ICFO



Un camino eficiente hacia claves cuanticas seguras

Las entropias de Renyi, centrales en las pruebas de seguridad modernas de distribucion cuantica de claves, han sido tradicionalmente dificiles de optimizar desde el punto de vista computacional. Investigadores del ICFO han presentado ahora, en un articulo de PRX Quantum, un metodo para calcularlas de forma eficiente y fiable, lo que permite obtener pruebas de seguridad mas estables.

September 14, 2026

Corria el ano 1984 cuando Bennett y Brassard disenaron el primer protocolo de distribucion cuantica de claves (QKD, por sus siglas en ingles), el BB84, dando asi origen al campo de la criptografia cuantica. Mas de cuarenta anos despues, los investigadores han llevado a cabo numerosos experimentos, ampliado los marcos teoricos y desarrollado una gran variedad de nuevos protocolos QKD. La idea fundamental, sin embargo, sigue intacta: Alicia y Bob, dos usuarios honestos que desean comunicarse de forma segura, intercambian y miden estados cuanticos para obtener una clave secreta, confiando unicamente en las leyes de la fisica

cuantica para protegerse de Eva, la espia mas inteligente y maliciosa de todas.
Para evaluar si un protocolo QKD es seguro, es esencial acotar la cantidad de informacion que Eva puede llegar a obtener de los estados cuanticos intercambiados. Esto se ha calculado tradicionalmente mediante la llamada entropia de von Neumann, pero la mayoria de las pruebas de seguridad modernas ahora utilizan una **entropia** mas general llamada **Renyi** , una familia de entropias que tiene en cuenta cuan optimas son las medidas elegidas. Introduciendo un paso adicional de optimizacion sobre este conjunto, los investigadores pueden aproximarse todavia mas a la clave que Alicia y Bob obtienen en realidad.
Esta optimizacion, sin embargo, es computacionalmente dificil de resolver. Los enfoques actualmente disponibles se basan en algoritmos ad hoc que son lentos, numericamente inestables o aplicables solo a casos particulares. Al menos, esa era la situacion hasta que **Mariana Navarro,** investigadora del ICFO que esta realizando un doctorado industrial en Luxquanta, una spin-off del ICFO que ofrece soluciones de criptografia cuantica para empresas y redes de telecomunicaciones, encontro una forma de sortear estas dificultade computacionales. Bajo la supervision del**Dr. Carlos Pascual Garcia**, antiguo investigador del ICFO y ahora jefe de Teoria Cuantica en Luxquanta, junto con Andres Gonzalez Lorente Pablo Parellada y el Dr. Mateus Araujo de la Universidad de Valladolid, y utilizando metodo numericos ya consolidados (concretamente, la optimizacion conica), el equipo h desarrollado**un metodo practico y fiable para calcular entropias de Renyi.**
Publicado recientemente en PRX Quantum, su metodo basado en optimizacion conica permite abordar de forma eficiente varios protocolos QKD, desde el historico BB84 hasta un protocolo mas exigente de variables continuas con modulacion discreta, el cual involucra a sistemas cuanticos mas grandes y restricciones experimentales mas complejas.
i¿½Al principio, nos sorprendio la velocidad de nuestra estrategiai¿½, recuerda Mar ana Navarro, primera autora del articulo. En la prueba numerica para el BB84 con cubits, por ejemplo, el metodo conico resolvio la optimizacion en una fraccion de segundo, mien ras que implementaciones comparables tardaban decenas de segundos. i¿½Ademas, **nuestro metodo no solo es mas rapido, sino tambien mas sistematico y numericamente preciso que los enfoques anteriores**i¿½, anad
. El siguiente paso natural seria calcular tasas de clave segura para protocolos mas complejo , como el BB84 con estados senuelo (decoy-state) y el QKD independiente del dispositivo de medicion. Pero, segun Carlos Pascual Garcia, uno de los investigadores senior del estudio, la optimizacion conica tiene tambien el potencial de permitir comparaciones mas justas entre disenos de protocolos alternativos, estudiar con precision las perdidas en el canal o la eficiencia de los detectores en un experimento, y ofrecer informacion practica sobre a que distancia pueden estar Alicia y Bob manteniendo al mismo tiempo la seguridad.
i¿½Hace cuarenta anos, ni siquiera Bennett y Brassard habrian podido imaginar como ser a hoy la criptografia cuanticai¿½, reflexiona el investigador. i¿½El futuro es incierto, y s lo el tiempo dira el impacto que tendra nuestro estudio. Pero me alegra poder decir

ue ya estamos persiguiendo estos objetivos mas amplios, y los resultados preliminares s n muy prometedor

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

Agradecimientos:
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.