

Distribucion Cuantica de Claves: nuevos avances en seguridad y practicidad

La distribucion cuantica de claves (QKD, por sus siglas en ingles) es un metodo mediante el cual dos partes, Alice y Bob, pueden generar una clave secreta compartida que es segura contra intercepciones, basandose en los principios de la fisica cuantica. Investigaciones recientes en el ICFO se han centrado en la QKD de variables continuas (CV-QKD), la cual emplea componentes opticos facilmente disponibles y la infraestructura de telecomunicaciones ya existente.

February 13, 2025

La CV-QKD presenta ventajas sobre la QKD de variables discretas (DV-QKD), como una implementacion mas sencilla y asequible, ademas de ser escalable, especialmente para distancias metropolitanas. Sin embargo, las pruebas de seguridad para la CV-QKD han estado mayormente limitadas a la modulacion gaussiana, cuya implementacion resulta compleja. La

CV-QKD de modulacion discreta (DM CV-QKD), en la que Alice usa un pequeno conjunto de estados coherentes, es mas practica, pero ha carecido de un analisis de seguridad solido. En su publicacion, los investigadores del ICFO **Carlos Pascual-Garcia**, el **Dr. Stefan Bauml** y el **Dr. Rotem Liss**, liderados por el **Prof. ICREA Antonio Acin**, en colaboracion con la Universidad de Valladolid, abordan este desafio proporcionando una prueba de seguridad para un protocolo de DM CV-QKD que utiliza cuatro estados coherentes y mediciones heterodinas. Este protocolo emplea un teorema generalizado de acumulacion de entropia (GEAT, por sus siglas en ingles) para establecer seguridad contra ataques generales. El GEAT es un formalismo que permite una interpretacion cuantitativa de procesos secuenciales, como una serie de rondas en un protocolo QKD. Este enfoque, presentado en Physical Review A, permite establecer un limite inferior en la cantidad de clave que Alice y Bob pueden obtener, incluso en presencia de un adversario con recursos cuanticos ilimitados.
Esta nueva prueba de seguridad se ve reforzada por un algoritmo numerico basado en optimizacion conica. Dicho metodo permite una evaluacion rapida y confiable de la seguridad del protocolo, proporcionando estimaciones de claves secretas bajo demanda. Ademas, el uso del GEAT permitio a los investigadores evitar la tomografia virtual requerida en trabajos anteriores, lo que simplifica la prueba de seguridad y mejora las tasas de claves secretas en escenarios de tamano finito. En particular, el estudio demostro que es posible alcanzar tasas de clave positivas para bloques de aproximadamente 10? senales laser en distancias metropolitanas. Esto representa una mejora significativa en comparacion con resultados previos, que requerian bloques de 10^{11} senales o mas, ademas de metodologi
s numericas mas compleja
. Estos hallazgos tienen varias implicaciones importantes, incluida la reduccion del tamano
e bloque requerido para generar tasas de clave secreta significativas, asi como el desarrollo
e herramientas numericas para implementaciones practicas. Los resultados demuestran que
s posible alcanzar los mas altos estandares de seguridad en QKD bajo condiciones accesibl
s experimentalment
. Los investigadores senalan ciertas limitaciones relacionadas con el GEAT, como restriccion
s en la frecuencia de generacion de senales, que seran abordadas en futuras investigacion
s mediante el uso del reciente teorema de acumulacion de entropia marginal. Asimismo, l
s trabajos futuros exploraran tecnicas de seguridad mas avanzadas basadas en las entropias
e Renyi, las cuales permiten mayores tasas de generacion de claves secretas. Los hallazgos d
l estudio representan un avance significativo en el desarrollo de sistemas de CV-Q
D practicos y seguros, con importantes implicaciones para el futuro de las redes
e comunicacion cuantica segura

Referencia:

Improved finite-size key rates for discrete-modulated continuous-variable quantum key distribution under coherent attacks. Carlos Pascual-Garcia, Stefan Bauml, Mateus Araujo,

Rotem Liss, and Antonio Acin. Phys. Rev. A 111, 022610 (2025)
DOI: https://doi.org/10.1103/PhysRevA.111.022610

Agradecimientos:
C.P.G thanks Marco Tulio Quintino for fruitful indications about numerical precision, and Yoann Pietri for suggestions about experimental aspects of CVQKD. We further thank Omar Fawzi, Min-Hsiu Hsieh, Lars Kamin, Florian Kanitschar, Bill Munro, Mizanur Rahaman, Gelo Noel Tabia, Ernest Tan, Toshihiko Sasaki and Shin-Ichiro Yamano for insightful discussions. This work was supported by the ERC (AdG CERQUTE, grant agreement No. 834266), the AXA Chair in Quantum Information Science, Gobierno de Espana (Severo Ochoa CEX2019-000910-S, NextGen Quantum Communications and FUNQIP), Fundacio Cellex, Fundacio Mir-Puig, the EU (QSNP and Quantera Veriqtas), the Generalitat de Catalunya (CERCA program and the postdoctoral fellowship programme Beatriu de Pinos), European Union's Horizon 2020 research and innovation programme under grant agreement No. 801370 (2019 BP 00097) within the Marie Sklodowska-Curie Programme. The research of M.A. was supported by the European Union- Next Generation UE/MICIU/Plan de Recuperacion, Transformacion y Resiliencia/Junta de Castilla y Leon, and by the Spanish Agencia Estatal de Investigacion, Grant No. RYC2023-044074-I.