Distribucio de Claus Quantica: nous avencos en seguretat i practicitat

La distribucio de claus quantica (QKD, per les seves sigles en angles) es un metode mitjancant el qual dues parts, Alice i Bob, poden generar una clau secreta compartida que es segura contra intercepcions, basant-se en els principis de la fisica quantica. Investigacions recents a l'ICFO s'han centrat en la QKD de variables continues (CV-QKD), que utilitza components optics facilment disponibles i la infraestructura de telecomunicacions ja existent.

February 13, 2025

La CV-QKD presenta avantatges respecte a la QKD de variables discretes (DV-QKD), com ara una implementacio mes senzilla i assequible, a mes de ser escalable, especialment per a distancies metropolitanes. No obstant aixo, les proves de seguretat per a la CV-QKD han estat majoritariament limitades a la modulacio gaussiana, la implementacio de la qual es complexa. La CV-QKD de modulacio discreta (DM CV-QKD), en que Alice utilitza un petit conjunt d'estats coherents, es mes practica, pero encara no compta amb una analisi de

seguretat solida.

En la seva publicacio, els investigadors de l'ICFO **Carlos Pascual-Garcia**, el **Dr. Stefan Bauml** i el **Dr. Rotem Liss**, liderats pel **Prof. ICREA Antonio Acin**, en col·laboracio amb la Universitat d Valladolid, aborden aquest repte proporcionant una prova de seguretat per a un protocol d DM CV-QKD que utilitza quatre estats coherents i mesures heterodines. Aquest protoco empra un teorema generalitzat d'acumulacio d'entropia (GEAT, per les seves sigles en angles per establir seguretat contra atacs generals. El GEAT es un formalisme que permet un interpretacio quantitativa de processos seqüencials, com ara una serie de rondes en n protocol QKD. Aquest enfocament, presentat a Physical Review A, permet establir un limit inferior en la quantitat de clau que Alice i Bob poden obtenir, fins i tot en presencia d'un adversari amb recursos quantics il·limitats

Aquesta nova prova de seguretat es veu reforcada per un algoritme numeric basat e optimitzacio conica. Aquest metode permet una avaluacio rapida i fiable de la seguretat de protocol, proporcionant estimacions de claus secretes sota demanda. A mes, l'us del GEA va permetre als investigadors evitar la tomografia virtual requerida en treballs anteriors, cos que simplifica la prova de seguretat i millora les taxes de claus secretes en escenaris de mid finita. En particular, l'estudi va demostrar que es possible assolir taxes de clau positives per blocs d'aproximadament 10^7 senyals laser en distancies metropolitanes. Aixo representa un millora significativa en comparacio amb resultats previs, que requerien blocs de 10^{11} seny ls o mes, aixi com metodologies numeriques mes complex

s. Aquests descobriments tenen diverses implicacions importants, inclosa la reduccio de la mida del bloc requerit per generar taxes de clau secreta significatives, aixi com el desenvolupament d'eines numeriques per a implementacions practiques. Els result ts demostren que es possible assolir els estandards mes alts de seguretat en QKD en condicions experimentalment accessibl

s. Els investigadors assenyalen certes limitacions relacionades amb el GEAT, com ra restriccions en la freqüencia de generacio de senyals, que seran abordades en fut res investigacions mitjancant l'us del recent teorema d'acumulacio d'entropia marginal. ixi mateix, els treballs futurs exploraran tecniques de seguretat mes avancades basades en les entropies de Renyi, que permeten majors taxes de generacio de claus secretes.

Els descobriments de l'estudi representen un avenc significatiu en el desenvolupamen de sistemes de CV-QKD practics i segurs, amb implicacions importants per al futur de les xa xes de comunicacio quantica seg

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

Agraiments:
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.