Quantum Key Distribution: new advances in security and practicality

Quantum key distribution (QKD) is a method for two parties, Alice and Bob, to generate a shared secret key that is secure against eavesdropping, based on the principles of quantum physics. Recent research at ICFO has focused on continuous variable QKD (CV-QKD), which uses readily available optical components and existing telecom infrastructure.

February 13, 2025

CV-QKD offers advantages over discrete variable QKD (DVQKD), including simpler and more affordable implementation, and scalability, especially for metropolitan distances. However, security proofs for CV-QKD have been mostly limited to Gaussian modulation, which is challenging to implement. Discrete-modulated CV-QKD (DM CV-QKD), where Alice uses a small set of coherent states, is more practical but has lacked robust security analysis.
In their publication, ICFO researchers **Carlos Pascual-Garcia**, **Dr. Stefan Bauml**, **Dr. Rotem Liss** , led by **ICREA Prof. Antonio Acin**, in collaboration with Universidad de Valladolid, address this challenge by providing a security proof for a DM CV-QKD protocol using four coherent

states and heterodyne measurements. This protocol uses a generalized entropy accumulation theorem (GEAT) to establish security against general attacks. The GEAT is a formalism that allows a quantitative interpretation of sequential processes, such as a series of rounds in a QKD protocol. This approach, reported in Physical Review A, allows to place a lower bound on the amount of key obtainable by Alice and Bob, even in the presence of an adversary with unlimited quantum resources.

This new security proof is enhanced by a numerical algorithm based on conic optimization. Said method allows a fast, reliable assessment of the security of the protocol, providing on demand estimations of secret keys. Furthermore, the use of the GEAT allowed the researchers to avoid the virtual tomography required by prior works, which simplifies the security proof and improves finite-size secret key rates. In particular, the study found that positive key rates are achievable for block sizes of around 108 laser signals at metropolitan distances. This is a significant improvement over previous results, which required block sizes of 1011 signals or more, as well as more involved numerical methodologies.

These findings have several important implications, including a reduction in the block sizes required to generate meaningful secret key rates, and the derivation of numerical tools for practical implementations. The results show that it is possible to achieve the highest security standards in QKD under conditions that are experimentally accessible.

The researchers note limitations related to the GEAT, such as restrictions on the signal generation frequency, which will be addressed in future research by using the recent marginal entropy accumulation theorem. Future work will also explore more advanced security techniques based on Renyi entropies, which yield higher secret key generation rates. The study's findings represent a significant step forward in the development of practical and secure CV-QKD systems with implications for the future of secure quantum communication networks.

Reference:

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

Acknowledgements:

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.