DRF: Thesis SL-DRF-21-0401

RESEARCH FIELD

Theoretical Physics / Theoretical physics

TITLE

Learning how to implement device-independent quantum key distribution using artificial intelligence

ABSTRACT

Quantum-assisted cryptography provides guarantees for secure communications that cannot be achieved with classical technologies. Yet, its security relies on the assumption that the devices used to produce a secret cryptographic key are trusted -- they carry out precisely the operations foreseen by the protocol. This assumption is hard to meet in practice and the security guarantees can be corrupted in case it is not perfectly satisfied, as demonstrated recently by hacking experiments. The aim of device-independent quantum key distribution (DIQKD) is to overcome this problem -- it provides security even when the devices are largely uncharacterised and treated like black boxes.

A major breakthrough in theoretical quantum information sciences is to lay the theoretical groundwork needed to realise the first proof-of-principle experiment reporting on DIQKD. Very recently, we successfully derived new security proofs in which the key rate is obtained directly from the statistics of measurement outcomes [1,2]. The aim of this proposal is to find the optical experiment leading the most favorable statistics for such a demonstraytion, using some machine learning technique.

[1] M. Ho, P. Sekatski, E.Y.-Z. Tan, R. Renner, J.-D. Bancal and N. Sangouard, Phys. Rev. Lett. 124, 230502 (2020)

[2] P. Sekatski, J.-D. Bancal, X. Valcarce, E.Y.-Z. Tan, R. Renner and N. Sangouard, arXiv:2009.01784 (2020)

LOCATION

Institut de Physique Théorique
Service de Physique Théorique
Place: Saclay

CONTACT PERSON

Jean-Daniel BANCAL
CEA
DRF/IPhT
IPhT, bat 774
CEA/Saclay
91191 Gif sur Yvette
Phone number: +33 1 69 08 66 30
Email: jean-daniel.bancal@ipht.fr

UNIVERSITY / GRADUATE SCHOOL

Paris-Saclay

Physique en Île-de-France (EDPIF)

THESIS SUPERVISOR

Nicolas Sangouard

CEA

DRF/IPhT

IPhT, bat 774

CEA/Saclay

91191 Gif sur Yvette