INTERNSHIP PROPOSAL

Laboratory name: Institut de Physique Théorique, CEA Saclay
CNRS identification code: UMR 3681 / Quobly Grenoble
Internship director's surname: Sangouard, Nicolas / Savin Valentin
e-mail: nicolas.sangouard@cea.fr Phone number:
Web page: https://quantum.paris/ https://quobly.io
Internship location: CEA Saclay, l'Orme des Merisiers, Bâtiment 774
Thesis possibility after internship: YES, already
Funding: YES If YES, which type of funding: CIFRE

Quantum cryptanalysis with silicon spin qubits

With Shor's algorithms, quantum computers are expected to compromise widely used classical cryptographic systems, such as RSA and elliptic-curve cryptography. The resources needed to execute these algorithms depend on (i) the decomposition of the algorithm into hardware-level subroutines, (ii) the underlying quantum hardware platform, and (iii) the fault-tolerant error-correction scheme used to protect quantum information.
Silicon spin qubits have recently emerged as a leading platform for scalable quantum computation. They combine fast gate operations, compatibility with mature semiconductor fabrication technologies, and the potential to shuttle qubits across a chip—an important asset for advanced error-correction and routing schemes.

The aim of this internship is to perform a detailed resource estimation for running Shor's algorithm to factor large RSA integers on a silicon-based quantum computer. More specifically, the student will i) model fault-tolerant implementations of Shor's algorithm using surface codes and lattice surgery, ii) Estimate the number of physical qubits and the computation time required to factor RSA numbers of cryptographic size with realistic noise sources for silicon spins, iii) benchmark these results against more advanced architectures that exploit qubit shuttling (e.g., transversal gates implementation and advanced codes such as quantum LDPC codes). The work will involve a combination of analytical reasoning, algorithmic decomposition, and numerical simulations.
This project will provide the student with solid training in quantum error correction, quantum algorithms, and architectures for fault-tolerant quantum computation—skills highly sought after in both academia and industry.

The internship is jointly hosted by:
CEA – Institut de Physique Théorique (Paris-Saclay): The student will join the Quantum Information group led by Nicolas Sangouard. The group is active in quantum computing architectures and fault-tolerance.
Quobly (Startup) : A leading French startup developing quantum processors based on silicon spin qubits. Supervision at Quobly will be ensured by Valentin Savin, an expert in quantum error correction and decoding.

Please, indicate which speciality(ies) seem(s) to be more adapted to the subject:

Condensed Matter Physics: YES Soft Matter and Biological Physics: NO
Quantum Physics: YES Theoretical Physics: YES