Postdoctoral Position in Lattice Cryptography and Quantum Algorithms

Research context

Learning with Errors (LWE) and its variants underpin a wide range of cryptographic constructions. Additional structure can enable new functionality and improve efficiency, while raising fundamental questions about security and the applicability of existing algorithms and hardness reductions. This position will explore these questions from two complementary perspectives: exploiting ring and module structure in quantum lattice algorithms, and understanding the hardness foundations and cryptographic uses of a variant of LWE called decomposed LWE.

Quantum algorithms for module lattices

This direction asks whether the algebraic structure of module lattices can be used to improve quantum algorithms for lattice problems. One starting point is the connection between Module-LWE and structured extrapolated dihedral coset problems (EDCP). The research will examine how algorithmic techniques developed for unstructured EDCP extend to this setting, and whether module structure can yield an advantage in suitable parameter regimes.

A complementary approach will investigate quantum filtering, which has yielded algorithms for quantum variants of LWE and certain short integer solution (SIS) instances beyond the EDCP framework. Subsequent developments in quantum decoding and the study of quantum LWE states offer further tools for investigating lattice problems. Topics include investigating the algebraic structure of ring and module lattices to improve the decoding, LWE state preparation, and oblivious sampling procedures, and studying whether these can be exploited to design more efficient quantum algorithms for lattice problems in the structured setting. The project may also study implications for the module version of the inhomogeneous short integer solution problem (Module-ISIS), using reductions involving quantum LWE variants.

Hardness and applications of decomposed LWE

This research direction will examine the hardness foundations of decomposed LWE, with particular emphasis on the choice of secret and error distributions. Topics include reductions between distributional variants and their quantitative losses, as well as the obstacles posed by the public decomposition and correlations across samples. The connection with succinct LWE offers an additional route for establishing hardness guarantees in suitable parameter regimes.

On the construction side, the project will investigate how these insights can support new cryptographic functionality or improve the efficiency and security of existing schemes. Potential applications include key-homomorphic computation, succinct randomized encodings, broadcast encryption, registered attribute-based encryption, distributed policy encryption, and group key agreement. A central goal is to connect advances in the underlying hardness assumptions with concrete improvements in constructions, while carefully accounting for correctness and parameter requirements.

Organization

Candidates should hold a PhD in cryptography, quantum computing, or a closely related field. This position is part of the PEPR Quantique PQ-TLS project, which aims to develop secure and efficient post-quantum cryptographic primitives. The expected start date is 01/01/2027, and the position is funded for one year. The selected candidate will join the CAPSULE team at the Inria Centre at the University of Rennes and will be supervised by Dr Yixin Shen, a researcher at Inria Rennes.