Are these lattices isomorphic? A quest for finer invariants

Guilhem Mureau*[1]

[1]Institut de Mathématiques de Bordeaux – Inria Bordeaux – France

Résumé

In its decisional form, the module-Lattice Isomorphism Problem (decision module-LIP) has received first attention in an article by C. Ling et. al. (Asiacrypt 2024). The authors gave a polynomial-time algorithm to distinguish spinor genera within the genus of a quadratic binary O_F-lattice, assuming that O_F is a principal ideal domain. However, this algorithm would not impact cryptographic schemes based on decision module-LIP for lattices such as those employed in HAWK, i.e., for binary O_K-lattices equipped with a Hermitian form (with K a cyclotomic number field). Motivated by HAWK's framework, we investigate a concept that serves as an analogue of the spinor genus for Hermitian lattices, called special genus. This notion was studied by Shimura who provided a complete set of invariants for describing special genera. Building on this result, we propose an algorithm to determine whether two Hermitian lattices belong to the same special genus. Specifically for HAWK's lattice and siblings, our algorithm runs in classical polynomial-time. Nevertheless we provide numerical evidence suggesting that the ability to distinguish special genera does not, in practice, constitute a significative advantage for solving decision module-LIP.

*Intervenant