Contribution ID: **9** Type: **not specified**

Algebraic lattices in cryptography

Monday, June 28, 2021 4:00 PM (45 minutes)

Finding short vectors in a lattice of large dimension is a problem that is believed to be hard to solve even with a quantum computer. For this reason, it has been used in the past 20 years to construct a lot of post-quantum cryptographic protocols (i.e., protocols which we hope are secure even against a quantum computer).
In order to improve efficiency of the cryptographic protocols, we often use lattices that have some extra algebraic structure (for instance, lattices that are also ideals of a number field).

The objective of this talk is to review recent algorithms that have been developed to compute short vectors in these algebraically structured lattices. We will see that thanks to the extra algebraic structure, it is sometimes slightly easier to find short vectors in these lattices than in the non-structured lattices.

Presenter: Dr PELLET-MARY, Alice (Université de Bordeaux)