On the Randomness of Log-S-unit lattices

Afonso Li*[1]

[1]Institut de Mathématiques de Bordeaux – Université de Bordeaux, IMB (Institut de Mathématiques de Bordeaux) – France

Résumé

With the anticipated arrival of quantum computers promising more efficient computation and threatening existing cryptographic systems based on assumptions like integer factorization, the area of post-quantum cryptography has rapidly expanded.
One of the leading candidates for post-quantum cryptography utilizes mathematical structures called Euclidean lattices. These seemingly simple discrete structures within real vector spaces offer hard problems such as the shortest vector problem (SVP) and the closest vector problem (CVP). However, due to the large representation size of unstructured lattices, lattice-based cryptography turned towards structured lattices, an idea inspired by ideals or modules over the rings of integers of number fields. By doing so, the representation becomes more compact for cryptographic implementations. While offering significant efficiency gains, the algebraic structure introduces symmetries that can restrict their geometry and potentially introduce weaknesses. For instance, ideal lattices (i.e., lattices arising from ideals of number fields) present some weaknesses compared to random Euclidean lattices. One of the famous attacks/reductions is the reduction of ideal SVP to solving CVP in some precomputed lattice associated to the number field where the ideal lives. In this specific reduction, lattices known as Log-S-unit lattices play a crucial role.
In this talk, we will try to understand the geometry of these Log-S-unit lattices. We will see that they are strongly connected to an old hard problem in lattice cryptography called the inhomogeneous short integer solution (ISIS) problem. We will show that solving the CVP problem for some natural distributions of Log-S-unit lattices is at least as hard as the ISIS problem. By doing so, we gain a better understanding of the viability of the reduction of ideal SVP to CVP in Log-S-unit lattices.

*Intervenant