From Code-Based Cryptography to Packing Bounds

Thomas Debris-Alazard

Inria, École Polytechnique, France

Pivotal results to argue the security of crypto-systems based on codes and lattices are the so-called worst-to-average case reductions. Regarding public-key cryptography based on codes, one of the aforementioned reductions can be stated as: from any algorithm decoding a random linear code one can derive an algorithm decoding any fixed code. A crucial tool to get such reduction is known as *code smoothing*. It refers to the fact when we start from a random codeword (of a fixed code) and then we add an error growing wider and wider, the distribution tends towards the uniform.

The first aim of this talk is to present the aforementioned code-based worst-to-average case reduction. Then we will mainly focus on code smoothing. As it will be shown, it is related to packing bounds, *i.e.*, finding upper bounds on code sizes with a given minimum distance. Our ultimate aim will be to present the most fruitful approach to provide such bounds: Delsarte's linear program derived from association scheme theory.

This talk is the result of joint works with André Chailloux, Léo Ducas, Nicolas Resch and Jean-Pierre Tillich