Speaker: Jade Nardi
Title: Goppa-like AG codes from $C_{a,b}$ curves and the dimension of the square of their dual

Abstract. McEliece cryptosystem is one of the last code-based candidates for standardization of post-quantum cryptrographic to the NIST competition since the third round. It guarantees the smallest ciphertexts among all the candidates, but it suffers from the largest public keys. Over the past forty years, there were many attempts in replacing the family of binary Goppa codes by other structured families of codes in order to reduce the key size.

In this talk, we will introduce a new family of codes that can be used in this context, called Goppa-like AG codes. These codes generalize Goppa codes and can be constructed from any curve of genus $g \geq 0$. As subfield subcodes, they resist to the known structural attacks to AG codes.

Recently, Mora and Tillich established a bound for the dimension of the dual of Goppa codes, which for high rate Goppa codes is abnormally small compared to random codes. This makes high rate Goppa codes distinguishable from random ones, which does not threaten the McEliece cryptosystem but is likely to break the code-based CFS signature. As Mora and Tillich's bound relies on some properties of Reed-Solomon codes that they share with AG codes, notably their behaviour under componentwise product, it is natural to wonder how it applies to Goppa-like AG codes.

After studying Mora and Tillich's strategy to bound the dimension of the dual of classical Goppa codes, we will present how we generalize it to a family of Goppa-like AG codes from $C_{a,b}$ curves and we propose numerical experiments to measure how much our bound is sharp.

N.B. This talk is based on the preprint *Goppa-like AG codes from $C_{a,b}$ curves and their behaviour under squaring their dual*, with Sabira El Khalfaui, Mathieu Lhotel, on arXiv.