Elliptic curves and isogenies in characteristic 2

Nicolas Sarkis*[1]

[1]INRIA Saclay – L'Institut National de Recherche en Informatique et e n Automatique (INRIA) – France

Résumé

Elliptic curves have been extensively used in cryptography for the past forty years. One reason for that is their efficient arithmetic, as well as having a group structure with no particular additional property. They also have good post-quantum aspects with isogeny-based cryptography, which are group homomorphisms with finite kernel.

In odd characteristic, they have been thoroughly studied, with several standard models such as twisted Edwards curves or Montgomery curves, optimized arithmetic and various isogeny formulas. Still, from a computational point of view, it would be natural to work with finite fields of characteristic 2, but elliptic curves in this context have to be studied differently. Notably, ordinary curves have interesting properties in this context such as having rational 2-torsion.

Some models in even characteristic are known to have efficient x-only arithmetic, but providing isogeny formulas has been less popular in the literature, which could be of interest for isogeny-based cryptography, especially the one based on ordinary graphs.

In this talk, we will introduce elliptic curves in characteristic 2, their particularities and x-only arithmetic, and then explain how to find isogeny formulas in this context. Joint work with Gustavo Banegas and Benjamin Smith.

*Intervenant