Multiplication polynomials for elliptic curves over finite local rings

Riccardo Invernizzi
KU Leuven, Belgium
riccardo.invernizzi@studend.kuleuven.be

For a given elliptic curve E over a finite local ring, we denote by E^∞ its subgroup at infinity. Every point $P \in E^\infty$ can be described solely in terms of its x-coordinate P_x, which can be therefore used to parameterize all its multiples nP. We refer to the coefficient of $(P_x)^i$ in the parameterization of $(nP)_x$ as the i-th multiplication polynomial.

We show that this coefficient is a degree-i rational polynomial without a constant term in n. We also prove that no primes greater than i may appear in the denominators of its terms. As a consequence, for every finite field $\mathbb{F}_q$ and any $k \in \mathbb{N}^*$, we prescribe the group structure of a generic elliptic curve defined over $\mathbb{F}_q[X]/(X^k)$, and we show that their ECDLP on E^∞ may be efficiently solved.

Joint work with Daniele Taufer (KU Leuven).