Crittografia a base d'isogenie Luca De Feo

Le isogenie sono morfismi di varietà abeliane. La loro teoria algoritmica è sviluppata da oltre 30 anni, motivata in parte dall'algoritmo di Schoof–Elkies–Atkin per il conteggio di punti, algoritmo fondamentale in crittografia ellittica.

I progressi algoritmici hanno portato negli ultimi 20 anni allo sviluppo di una nuova branca della crittografia, detta a base d'isogenie. L'ogetto centrale centrale di questa disciplina non è più una curva ellittica isolata, bensì un grafo di curve ellittiche legate da isogenie. I grafi d'isogenie esibiscono diverse strutture combinatorie interessanti —foreste, grafi di Cayeley, grafi espansori—, e offrono dei problemi computazionalmente difficili come la ricerca di cammini. Su queste basi, siamo oggi in misura di costruire un vasto spettro di primitive crittografiche: cifratura e firma digitale resistenti agli attacchi quantistici, crittografia a orologeria, sistemi a soglia, ecc.

Questo mini-corso darà un'introduzione alla teoria delle isogenie di curve ellittiche su corpi finiti, e spiegherà come la crittografia è costruita a partire da esse.