TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Facoltà di M.F.N.
Dipartimento di Matematica

Corso di Dottorato
15.02.2022 – 18.02.2022
Crittografia a base d'isogenie

Luca De Feo (I.B.M. Research Europe of Zurich)

Where: Conference Room 1201 - "Roberta Dal Passo"

Schedule:

15.02.2022 14:30 – 15:30 - Rome Time
16.02.2022 10:00 – 12:00 - Rome Time
17.02.2022 10:00 – 12:00 - Rome Time
18.02.2022 10:00 – 12:00 - Rome Time

Speaker: Luca De Feo (I.B.M. Research Europe of Zurich)

Organizing Committee: Giulio Codogni, Roberto Fringuelli, Claudio Onorati

Title: "Crittografia a base d'isogenie"

ABSTRACT: 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'oggetto 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.
In caso di interesse da parte degli studenti, si potranno calendarizzare delle lezioni aggiuntive di approfondimento a cura di Giulio Codogni e Michele Salvi.

Note: in presenza potranno partecipare un massimo di 40 persone previa esibizione del Super Green Pass. To attend the talks, it is compulsory to have the "Super Green Pass", or a valid COVID-19 Vaccination Card.