UNIVERSITÀ DI TRENTO
Dipartimento di Matematica

DOTTORATO

CYCLE 36th
ORAL DEFENCE OF THE PHD THESIS

Thursday 22nd February 2024 – at 11.00 am
Aula seminari – Dipartimento di Fisica
The event will take place in presence and online through the ZOOM platform.
To get the access codes please contact the secretary office

Marzio Mula

PhD Student in Mathematics

Graphs and pairings of elliptic curves

Abstract:

Most isogeny-based cryptosystems ultimately rely, for their security, on the problem of finding a secret isogeny between two elliptic curves (IsoPath). As cryptographic applications usually employ weaker variants of IsoPath for practical reasons, it is natural to ask whether these variants are equally hard from a computational perspective. For example, what happens if the endomorphism ring of one of the curves is known? Does the existence of suitable pairings affect the hardness of IsoPath? What happens if some non-trivial endomorphisms of the domain and codomain curves are known?

The first question leads to the well-known problem of hashing on the supersingular isogeny graph, i.e. the graph whose vertices are supersingular elliptic curves (up to isomorphism) and whose edges are isogenies of fixed degree. In the first part of the talk we show that none of the available hashing techniques are at the same time efficient and cryptographically secure, and we also point out a few alternative approaches. Furthermore, we leverage the classic Deuring correspondence between supersingular elliptic curves and quaternion orders to study a weaker variant of IsoPath.

We then address the latter questions, showing that, in the general case, finding distinct pairings compatible with a secret isogeny is no easier than solving IsoPath. In the presence of an orientation, on the other hand, we show that the existence of suitable self-pairings, together with a recent attack on the isogeny-based key-exchange SIDH, does lead to efficiently solving IsoPath in some cases.

Finally, we introduce a different graph of elliptic curves, which has not been considered before in isogeny-based cryptography and which does not arise, in fact, from isogenies: the Hessian graph. We give a (still partial) account of its remarkable regularity and discuss potential cryptographic applications.

Supervisors: Nadir Murru – Federico Pintore

CONTACTS
Staff di Dipartimento - Matematica
tel. 0461 281508-1625-1701-3786
phd.maths@unitn.it
www.maths.unitn.it