Departamento de Matemática
Universidade de Aveiro

CIDMA CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

Seminário do Grupo de Álgebra e Geometria

Isogeny graphs and isogeny cryptography

Enric Florit

Resumo

Public key cryptography is essential for all modern-day communications, and a handful of protocols are deployed across all devices that we use everyday. Notably, these protocols are vulnerable to (hopefully) theoretical quantum-computer cryptanalysis. Several replacements have been proposed, aiming for so-said post-quantum resistance.

In this talk, I will introduce isogeny graphs, a combinatorial device that allows us to adapt elliptic curve crpytography to the post-quantum world. In particular I will mention the SIDH protocol, which was to be one of NIST's promising standards — until it was broken, by use of isogenies and classical computers, a little over a year ago. Time allowing, I will also mention other proposals that remain safe against all kinds of attacks.

Sala Sousa Pinto, 20 de novembro de 2023, 14:00

This seminar is partly supported by the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UIDB/04106/2020.

fct Fundação para a Ciência e a Tecnologia

REPÚBLICA PORTUGUESA