ULB UNIVERSITÉ LIBRE DE BRUXELLES

Isogeny path problems for post-quantum cryptography

Abel Laval

March 27, 2025 - 14:30

Abstract

Quantum computers currently pose a threat to modern day communications security, which has incentivised cryptographers to look into quantum-safe alternatives. Among the potential candidates, we have isogeny-based cryptography whose security comes from the hardness of solving path-finding problems on isogeny graphs.

Isogenies are morphisms between elliptic curves (or more generally between abelian varieties). In this talk, we will define isogeny graphs and the related isogeny path-finding problem. Then we will show how this problem can be viewed in a quaternion algebra setting. Finally, we will see that this correspondence between the geometric and the arithmetic worlds allow us to build "efficient" crpytographic protocols.