Title: Supersingular and superspecial isogeny cryptography.

Enric Florit (Universitat de Barcelona)

Abstract:
Public key cryptography is extensively used in essentially all systems that need some connection to the internet. As development of quantum computers gets more advanced, a real threat to cryptography appears, since algorithms that break RSA and cryptosystems based on discrete logarithms have been known for long.

This has motivated the introduction of post-quantum cryptography. Isogeny-based cryptography is the attempt to adapt elliptic curve cryptography to this new model. In this talk, I will explain the basics of the protocol SIDH.

Remarkably, SIDH was about to be standardised by NIST, until a polynomial-time attack was proposed in august that erased all possibility. Hence, after seeing why SIDH worked, we will also see why it was broken (and how they are trying to fix it).