Speaker: Wouter Castryck
Title: An efficient break of the supersingular isogeny Diffie-Hellman protocol

Abstract. Finding an explicit isogeny between two given isogenous elliptic curves over a finite field is considered a hard problem, even for quantum computers. In 2011 this led Jao and De Feo to propose a key exchange protocol that became known as SIDH, shorthand for Supersingular Isogeny Diffie-Hellman. The security of SIDH does not rely on a pure isogeny problem, due to certain "auxiliary" elliptic curve points that are exchanged during the protocol (for constructive reasons). In this talk I will discuss a break of SIDH that was discovered in collaboration with Thomas Decru. The attack uses isogenies between abelian surfaces and exploits the aforementioned auxiliary points, so it does not break the pure isogeny problem. I will also discuss improvements of this attack due to Maino et al. and Robert, as well as a countermeasure by Fouotsa et al., along with breaks of this countermeasure in some special cases.