University of Windsor

SAC2022

Invited Talk: Efficient key recovery attacks on SIDH

Wouter Castryck

I will discuss a key recovery attack, jointly discovered with Thomas Decru, on the Supersingular Isogeny Diffie-Hellman problem. It uses isogenies between abelian surfaces. If the endomorphism ring of the starting curve is known, the attack runs in polynomial time and effectively breaks the NIST submissions SIKEp434, SIKEp503, SIKEp610 and SIKEp751 in a matter of hours on a single core. We will also discuss some recent improvements which speed up the attack by a significant factor; most notably, these improvements include a "direct evaluation" approach due to Maino-Martindale, Oudompheng, Petit and Wesolowski. To conclude, we will also discuss the case where the endomorphism ring of the starting curve is unknown. In this case, our algorithm runs in sub-exponential time (as does the independent method by Maino-Martindale), but this has been superseded by a beautiful trick due to Robert, involving abelian eightfolds (!).