A hidden shift quantum attack on unbalanced SIDH

Péter Kutas[1], Simon-Philipp Merz[2], Christophe Petit[1], Charlotte Weitkämper[1]

University of Birmingham, UK
Royal Holloway, University of London, UK

Rump session, ANTS, 01.07.2020.

Motivation

- Childs-Jao-Soukharev: subexponential attack against cryptosystem based on ordinary elliptic curves
- Exploits the class group action, can be adapted to CSIDH
- De Feo-Jao in the original SIDH paper: "no reasonable variant of this strategy would apply to supersingular elliptic curves"

Result

- SIDH problem : given two elliptic curves E_1 and E_2, ϕ secret isogeny of degree N_1; if given the image of generators of $E_1[N_2]$ under ϕ, find ϕ
- When N_1 and N_2 are unbalanced, hidden shift attack which is somewhat analogous to CJS attack
- So far not better than previous attacks but fundamentally different