A computational framework for principally polarized abelian varieties

Etienne Piasecki*[1]

[1]Unité de Mathématiques Pures et Appliquées – Ecole Normale Supérieure de Lyon, Centre National de la Recherche Scientifique – France

Résumé

The higher dimensional notion generalizing elliptic curves are principally polarized abelian varieties (PPAVs). These objects have become increasingly important in isogeny-based cryptography due to the critical role they played in the breaking the SIDH key exchange mechanism. Since these breaks, many of recent advances in isogeny-based cryptography use PPAVs. However, they are difficult to work with and often a strong background in algebraic geometry is needed.
I will present a new computational framework for PPAVs that focuses on what can be computationally done with these objects. I will also present an instantiation of this framework and some applications.

This work aim to be accessible for someone with no prior background in algebraic geometry who wish to work with PPAVs. Participants new to the field are warmly welcomed to this talk.

This work is a collaboration with Maria Corte-Real Santos and Benjamin Wesolowski.

*Intervenant