# Applications to Cryptography of the Construction of Curves from Modular Invariants

Christelle Vincent

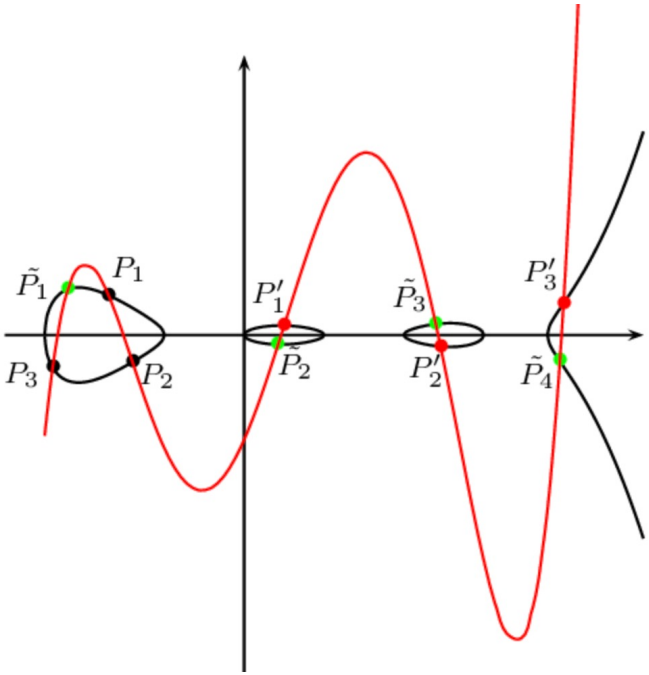
The UNIVERSITY of VERMONT

## Research question:

- Cryptography based on elliptic curves is currently widely deployed, thanks to their increased security
- Can curves of higher genus offer the same benefits?

## Problem and contributions:

- We currently do not have techniques to generate such curves
- Our work lays the computational and theoretical foundation to develop these techniques




The addition law on a curve of genus 3
Image by Costello and Lauter for *Group Law Computations on Jacobians of Hyperelliptic Curves*

## Scientific impact:

- Better bound on primes appearing in denominators of curve invariants
- Better understanding of modular formulae for invariants of curves of genus 3

## Broader impacts:

- Advances in fundamental research on curves of genus 3
- Conjecture which will allow efficient, provably correct computations

DMS-1802323
PI: Christelle Vincent
Christelle.Vincent@uvm.edu