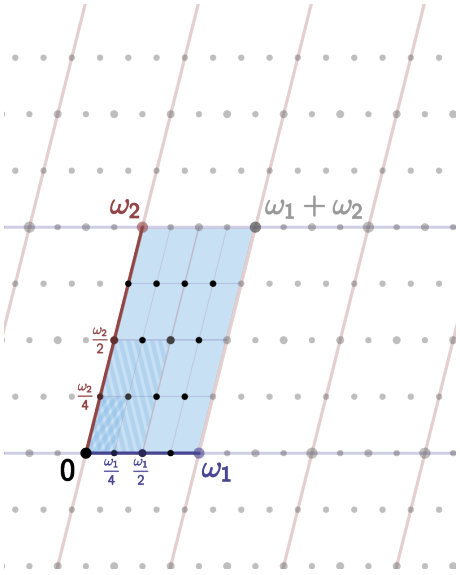
Distance to the F_p subgraph



Two elliptic curves are *isogenous* if there is an algebraic map (an *isogeny*) between them; computing an isogeny of degree ℓ has a cost proportional to ℓ. For a fixed prime p, the *supersingular* elliptic curves in characteristic p form a graph, called the *supersingular isogeny graphs*. This graph plays a central role in isogeny based cryptographic, through schemes such as SQIsign.

All supersingular elliptic curves for a fixed characteristic p can be defined over $\mathbb{F}_{p^2}$, i.e. over an extension of degree 2 of $\mathbb{F}_p$. However, a smaller set can already defined over the base field $\mathbb{F}_p$. These form a distinguished $\mathbb{F}_p$ *subgraph* with extra structure, tied to class groups of imaginary quadratic orders. This subgraph plays an important role in attacks against the *supersingular isogeny problem*, the problem underlying isogeny based cryptography.

The goal of this thesis is to analyze this subgraph in relation to the whole graph. More specifically:

- prove a bound X such that every $E/\mathbb{F}_{p^2}$ admits an isogeny of degree at most X to a curve defined over $\mathbb{F}_p$;
- study how tight this bound is, and whether it can be made explicit;
- explore variants: fixed small degree ℓ steps (as in CSIDH), bounding the number of steps instead of the degree, or average- rather than worst-case distance.

Some interest in number theory and algebraic geometry is required.

Practicalities

Promotor:	Frederik Vercauteren
Daily supervisor:	Milan Boutros milan.boutros@esat.kuleuven.be office B01.21
Nature of the work:	40% literature, 50% theoretical work, 10% software
Number of students:	1

 © 2026 – 2027 COSIC