Dissertation Proposal: Generating random supersingular Elliptic Curves using modular polynomials

Simon Pohmann
Supervisor: Cristophe Petit

May 6, 2022

The motivation of my thesis is an open problem in isogeny-based cryptography, namely to find an algorithm that finds a random supersingular Elliptic Curve without revealing a l-isogeny path to that curve (starting from a canonical supersingular Elliptic Curve). Different approaches to solve this problem where explored in [Boo+22]. The focus of my dissertation should be to further study the idea presented in section 3, which is based on experimental evidence that there is a connection between an Elliptic Curve $E/\mathbb{F}_{p^2}$ being supersingular and having (multiple) fixed-degree isogenies to its conjugate $E^{(p)}$. In other words, an algorithm tries to find a random curve with isogenies of different fixed degrees[1], and hopes that this is then supersingular. Curves with the first property, i.e. having an n-isogeny $E \to E^{(p)}$ have previously been studied in e.g. [CS21].

The first main obstacle is that finding such a curve $E/\mathbb{F}_{p^2}$ with n_i-isogenies to $E^{(p)}$ is not easy if $n_1, ..., n_k$ are exponentially large (which they have to be in order to be secure). The current idea is to find a root of the greatest common divisor of $\Phi_{n_1}(x, x^p), ..., \Phi_{n_k}(x, x^p)$, but the normal methods to compute this run in time polynomial in the n_i.

The second obstacle is that it is not clear how the correlation between an n-isogeny $E \to E^{(p)}$ and E being supersingular behaves. Apart from experimental evidence, not much is known so far. Studying this part is not only important for making the above method work well, but also interesting from a pure math perspective.

Since this is a current research problem, it is not clear how much new progress I can make on the problems, but both my supervisor and myself believe that it will be possible to find something new and interesting. Especially the second part looks really promising to me.

[1] Currently, the main focus is on the situation that there are two isogenies of degrees $n_1 \neq n_2$

References

[Boo+22] Jeremy Booher et al. *Failing to hash into supersingular isogeny graphs*. Cryptology ePrint Archive, Report 2022/518. `https://ia.cr/2022/518`. 2022.

[CS21] Mathilde Chenu and Benjamin Smith. "Higher-degree supersingular group actions". In: *CoRR* abs/2107.08832 (2021).