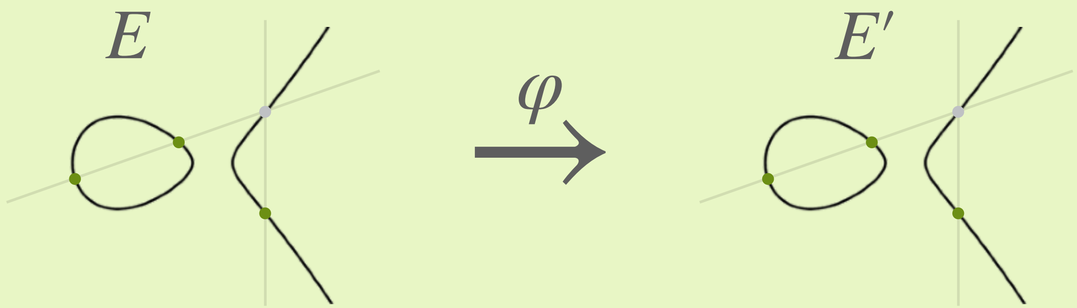
PART 1

SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



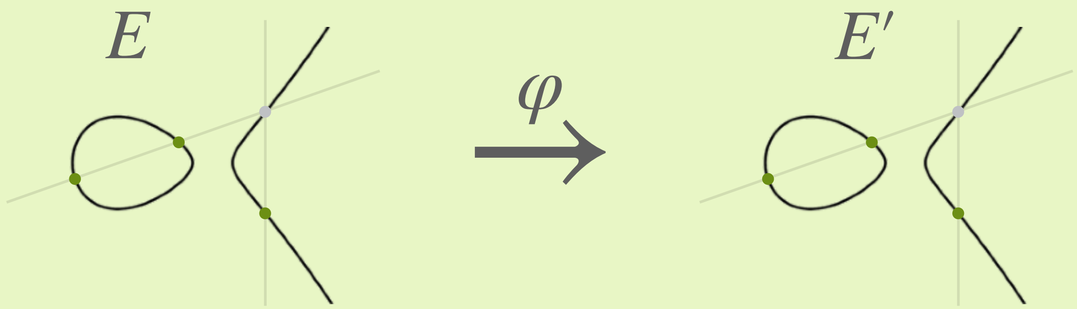
PART 1

SQIsign

WARNING!

- SQIsign is a **difficult** scheme, especially signing
- To keep this talk "down to earth", I will **simplify** a lot
- This will increase clarity and intuition by being **hand-wavy**, at the cost of rigor

isogenies



Isogeny

- "nice" map φ (group homomorphism) between elliptic curves $E \to E'$
- given by rational functions: a point $(x, y) \in E$ is mapped to $(f_1(x,y)/f_2(x,y) \ , \ g_1(x,y)/g_2(x,y))$
- size of $\ker \varphi$ is same as degree of φ!