

**Pairings map  
elliptic curve problems  
to finite field problems**

**Elliptic curve arithmetic  
is slow**

**Finite field arithmetic  
is (very) fast**