Implementation of an ECC with M-511

CS448 - Introduction to IT Security

Who? Yoann Kehler, Duong Ta

When? June 08, 2017

Outline

- What goals have we had?
- What have we done?
- What have we learned?

Term Project Goals

Term Project Goals

- understand the maths behind ECC

Term Project Goals

- understand the maths behind ECC
- implement a library with M-511 with:
  - key generation
  - encryption and decryption
  - signature and verification

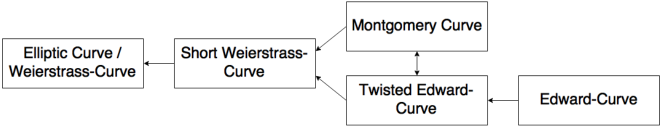
Term Project Goals

- understand the maths behind ECC
- implement a library with M-511 with:
  - key generation
  - encryption and decryption
  - signature and verification
- hike Jirisan

Put it into practice!

How to generate a curve?

variety of elliptic curves



Architecture of our Implementation

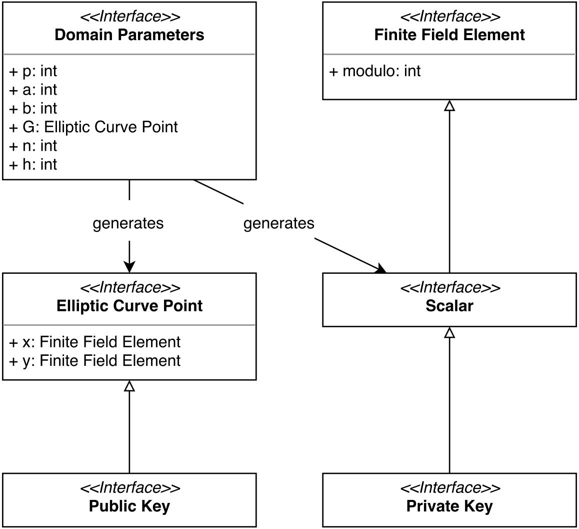
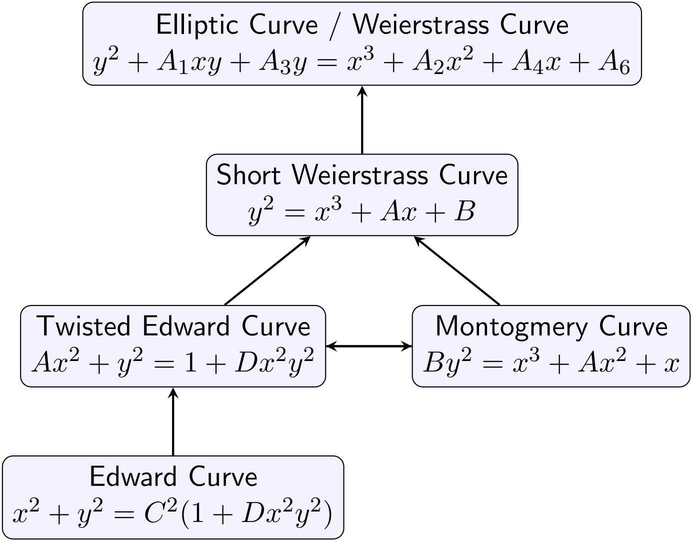


Figure: Class Diagram of our Implementation

Curve Shapes



Elliptic Curve / Weierstrass Curve

$y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6$

Short Weierstrass Curve

$y^2 = x^3 + Ax + B$

Twisted Edward Curve

$Ax^2 + y^2 = 1 + Dx^2y^2$

Montogmery Curve

$By^2 = x^3 + Ax^2 + x$

Edward Curve

$x^2 + y^2 = C^2(1 + Dx^2y^2)$

References I