EECS 498/598: Encrypted Systems
Winter 2022
Lecture 6: Elliptic Curves and Pairings

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Elliptic Curves

What is an elliptic curve?

Background: Groups of known order where DLOG + friends are hard!

- Diffie-Hellman

Only one family: $\mathbb{Z}_p^*$ e.g. $p=5$

$\{1, 2, 3, 4\}$

Problems with $\mathbb{Z}_p^*$:

(1) subexponential attacks
(2) large params
(3) slow operations

Elliptic Curves

1980s: Strange ideas in algebraic geometry!

- Lenstra factorization
- Koblitz, Miller
  Build cryptography from elliptic curves

1990s: Patents

2000s: patents expired

Elliptic Curves

Finite field: numbers mod p. can add/multiply

e.g. $p=5$ $\mathbb{F}_5 = \{0,1,2,3,4\}$

$3 \cdot 2 = 1 \mod 5$

Elliptic curve is equation w/ special form

$E = y^2 = x^3 + ax + b$ $a, b \in \mathbb{F}_p$ *non-degen

$E/\mathbb{F}_p$ ← over finite field $\mathbb{F}_p$

E.g. $y^2 = x^3 + x + 2$

Elliptic Curves

Set of points on $E/\mathbb{F}_p$

$$S = \{(x,y) \mid (x,y) \in \mathbb{F}_p \times \mathbb{F}_p,\ (x,y) \text{ satisfies eqn}\}$$

plug in result

Thm:

For a curve $E/\mathbb{F}_p$, $S \cup \{\mathcal{O}\}$ forms an (abelian) group! operation is "point addition".

Elliptic Curves

EC points ~ log p bits. To get n-bit security, group must only be 2n bits!

- DDH is hard (we think) in many classes

  Even non-DDH groups interesting...

Pairings

Let G_0, G_1, G_T be cyclic, order q.

$g_0 \in G_0$, $g_1 \in G_1$ are generators

A **pairing** is eff. computable f'n

$$e: G_0 \times G_1 \to G_T$$ "target" group

with properties

- Bilinear: let $u, u' \in G_0$ $v, v' \in G_1$

$$e(u \cdot u', v) = e(u, v) \cdot e(u', v)$$

- Non-degeneracy

$g_T := e(g_0, g_1)$ generates G_T

Pairings

"Symmetric": $G_0 = G_1$

"asymmetric": $G_0 \neq G_1$

Bilinearity implies

$\forall a, b \in \mathbb{Z}_q$

$$e(g_0^a, g_1^b) = e(g_0, g_1)^{ab} = e(g_0^b, g_1^a)$$

Boneh-Shoup Ch. 15