

Hashing into Elliptic Curves

Jean-Sébastien Coron
University of Luxembourg

Outline

- 1 Hashing into Elliptic Curves
 - Motivation
 - Classical Techniques

- 2 Icart's Function

Introduction

- Hashing into Elliptic Curves
 - Boneh-Franklin IBE: $Q_{id} = H_1(id)$ on the curve.
 - Password based authentication protocols (SPEKE, PAK).
- Boneh-Franklin: super-singular curve
 - Special curve with special operation: pairing.
 - Hashing is easy.
 - But larger parameters are required.
- How to hash into ordinary curves ?

Introduction

- Hashing into Elliptic Curves
 - Boneh-Franklin IBE: $Q_{id} = H_1(id)$ on the curve.
 - Password based authentication protocols (SPEKE, PAK).
- Boneh-Franklin: super-singular curve
 - Special curve with special operation: pairing.
 - Hashing is easy.
 - But larger parameters are required.
- How to hash into ordinary curves ?

Introduction

- Hashing into Elliptic Curves
 - Boneh-Franklin IBE: $Q_{id} = H_1(id)$ on the curve.
 - Password based authentication protocols (SPEKE, PAK).
- Boneh-Franklin: super-singular curve
 - Special curve with special operation: pairing.
 - Hashing is easy.
 - But larger parameters are required.
- How to hash into ordinary curves ?

SPEKE

- Simple Password Exponential Key Exchange (Jablon, 1996)
 - Let pw be a password shared by Alice and Bob
 - Let E be the subgroup of an elliptic curve of order q .
- Protocol
 - Alice sends $A = a.H(pw)$ to Bob, where $a \leftarrow \mathbb{Z}_q$
 - Bob sends $B = b.H(pw)$ to Alice, where $b \leftarrow \mathbb{Z}_q$
 - Alice computes $K = a.B = ab.H(pw)$
 - Bob computes $K = b.A = ab.H(pw)$

Try and Increment

- Elliptic curve:

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- Try and Increment:

Input: u an integer. We can take $u = H(m)$.

Output: Q , a point of $E_{a,b}(\mathbb{F}_p)$.

- 1 For $i = 0$ to $k - 1$
 - 1 Set $x = u + i$
 - 2 If $x^3 + ax + b$ is a quadratic residue in \mathbb{F}_p , then return $Q = (x, (x^3 + ax + b)^{1/2})$
 - 2 end For
 - 3 Return \perp
- Timing Attack

Try and Increment

- Elliptic curve:

$$E : y^2 = x^3 + ax + b \pmod p$$

- Try and Increment:

Input: u an integer. We can take $u = H(m)$.

Output: Q , a point of $E_{a,b}(\mathbb{F}_p)$.

- 1 For $i = 0$ to $k - 1$
 - 1 Set $x = u + i$
 - 2 If $x^3 + ax + b$ is a quadratic residue in \mathbb{F}_p , then return $Q = (x, (x^3 + ax + b)^{1/2})$
 - 2 end For
 - 3 Return \perp
- Timing Attack

Supersingular Elliptic Curve

- Supersingular curve:

$$E : y^2 = x^3 + 1 \pmod{p}$$

- with $p = 2 \pmod{3}$
- It has $p + 1$ points.
- Hashing into E :
 - Let $y = H(m)$
 - Let $x = (y^2 - 1)^{1/3}$
 - Return $P = (x, y)$
- p must be large because of MOV attack (at least 512 bits)

Supersingular Elliptic Curve

- Supersingular curve:

$$E : y^2 = x^3 + 1 \pmod{p}$$

- with $p = 2 \pmod{3}$
- It has $p + 1$ points.
- Hashing into E :
 - Let $y = H(m)$
 - Let $x = (y^2 - 1)^{1/3}$
 - Return $P = (x, y)$
- p must be large because of MOV attack (at least 512 bits)

Supersingular Elliptic Curve

- Supersingular curve:

$$E : y^2 = x^3 + 1 \pmod{p}$$

- with $p = 2 \pmod{3}$
- It has $p + 1$ points.
- Hashing into E :
 - Let $y = H(m)$
 - Let $x = (y^2 - 1)^{1/3}$
 - Return $P = (x, y)$
- p must be large because of MOV attack (at least 512 bits)

Hashing into Ordinary Curves

- Elliptic curve:

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- Icart's function
 - Published by Thomas Icart at CRYPTO 2009
 - Deterministic function into E
 - Requires $p \equiv 2 \pmod{3}$
 - Essentially one exponentiation in \mathbb{F}_p
- Shallue-Woestijne-Ulas algorithm
 - Deterministic algorithm into E (but requires a test)
 - Does not require $p \equiv 2 \pmod{3}$
 - Essentially one exponentiation in \mathbb{F}_p

Hashing into Ordinary Curves

- Elliptic curve:

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- Icart's function

- Published by Thomas Icart at CRYPTO 2009
- Deterministic function into E
- Requires $p \equiv 2 \pmod{3}$
- Essentially one exponentiation in \mathbb{F}_p

- Shallue-Woestijne-Ulas algorithm

- Deterministic algorithm into E (but requires a test)
- Does not require $p \equiv 2 \pmod{3}$
- Essentially one exponentiation in \mathbb{F}_p

Hashing into Ordinary Curves

- Elliptic curve:

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- Icart's function

- Published by Thomas Icart at CRYPTO 2009
- Deterministic function into E
- Requires $p \equiv 2 \pmod{3}$
- Essentially one exponentiation in \mathbb{F}_p

- Shallue-Woestijne-Ulas algorithm

- Deterministic algorithm into E (but requires a test)
- Does not require $p \equiv 2 \pmod{3}$
- Essentially one exponentiation in \mathbb{F}_p

Icart's Function

- Elliptic curve with $p = 2 \pmod 3$:

$$E_{a,b} : y^2 = x^3 + ax + b \pmod p$$

- Icart's function: (we can have $u = H(m)$)

$$\begin{aligned} f_{a,b} : \mathbb{F}_p &\mapsto E_{a,b} \\ u &\mapsto (x, y) \end{aligned}$$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{(2p-1)/3} + \frac{u^2}{3}$$

$$y = ux + v$$

$$v = \frac{3a - u^4}{6u}.$$

Icart's Function

- Elliptic curve with $p = 2 \pmod 3$:

$$E_{a,b} : y^2 = x^3 + ax + b \pmod p$$

- Icart's function: (we can have $u = H(m)$)

$$\begin{aligned} f_{a,b} : \mathbb{F}_p &\mapsto E_{a,b} \\ u &\mapsto (x, y) \end{aligned}$$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{(2p-1)/3} + \frac{u^2}{3}$$

$$y = ux + v$$

$$v = \frac{3a - u^4}{6u}.$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$
$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$

$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$
$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$
$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$

$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$

$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$

$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$
$$y = ux + v$$

Why it Works

- $E_{a,b} : y^2 = x^3 + ax + b \pmod p$
- Let $y = ux + v$ with u, v two parameters
- $u^2x^2 + 2uvx + v^2 = x^3 + ax + b$
- $x^3 - u^2x^2 + (a - 2uv)x + b - v^2 = 0$
- $(x - u^2/3)^3 + x(a - 2uv - u^4/3) = v^2 - b - u^6/27$
- We want: $a - 2uv - u^4/3 = 0$
 - We take $v = (3a - u^4)/(6u)$
- We get: $(x - u^2/3)^3 = v^2 - b - u^6/27$

$$x = \left(v^2 - b - \frac{u^6}{27} \right)^{1/3} + \frac{u^2}{3}$$
$$y = ux + v$$