Hashing to Elliptic Curves

draft-sullivan-cfrg-hash-to-curve

Nick Sullivan (nick@cloudflare.com)
Christopher A. Wood (cawood@apple.com)

CFRG
IETF 101, March 2018, London

Background

Hashing to elliptic curves is common

- Simple Password Exponential Key Exchange [Jablon96]
- Password Authenticated Key Exchange [BMP00]
- Boneh-Lynn-Shacham signatures [BLS01]
- Verifiable Random Functions (VRFs) [draft-irtf-cfrg-vrf]
- Privacy Pass [https://privacypass.github.io]

Try-and-Increment

```
1. ctr = 0
2. h = "INVALID"
3. While h is "INVALID" or h is EC point at infinity:
   A.  CTR = I2OSP(ctr, 4)
   B.  ctr = ctr + 1
   C.  attempted_hash = Hash(m || CTR)
   D.  h = RS2ECP(attempted_hash)
   E.  If h is not "INVALID" and cofactor > 1, set h = h^cofactor
4. Output h
```

Make sure h is in the prime order subgroup

(Non-)Requirements

Requirements

- Constant-time
- …?

Non-requirements

- Invertible

Methods

Method	Requirement
Icart	q = 2 mod 3
SWU	None
Simplified SWU	q = 3 mod 4
Elligator2	q is large, has a point of order 2, and j-invariant != 1728

Interface & Notation

$$\mathsf{H2C}(\alpha) : \{0,1\}^+ \to E$$

$$\begin{aligned}
\alpha &= \text{arbitrary input} \\
q &= \text{prime order of base field} \\
u &= \text{point of order 2 (Elligator2)} \\
f(x) &= \text{curve equation} \\
\mathsf{H}(\alpha) &= \text{hash to prime order subgroup}
\end{aligned}$$

Icart

$$t = \mathsf{H}(\alpha)$$

$$v = ((3A - t^4)/6t)$$

$$x = (v^2 - b - (t^6/27))^{1/3} + (t^2/3)$$

$$y = tx + v$$

$$\mathsf{Output}(x, y)$$

Elligator2

$$r = \mathsf{H}(\alpha)$$
$$d = -A/(1 + ur^2)$$
$$e = f(d)^{(p-1)/2}$$
$$u = ed - (1 - e)A/u$$
$$\mathsf{Output}(u, f(u))$$

(Current) Recommendations

Curve	Method
P-256	Simplified SWU
P-384	Icart
Curve25519	Elligator2
Curve448	Elligator2

Open Tasks

- Complete cost analysis
- Add SWU details and implementation
- Include security reductions where possible
- Interface details: octet strings to integer point encodings
- Produce verifiable implementations
- Clarify mappings that are reversible — this is not always desirable!

Open Issues

- Always multiply by cofactor?

- How close to indistinguishable from random points is needed?

hash-to-curve - CFRG - IETF 101

Simplified SWU

$$t = \mathsf{H}(\alpha)$$

$$x = -t^2$$

$$x_2 = (-b/a) \cdot (1 + (1/(t^2 + t)))$$

$$x_3 = t \cdot x_2$$

$$h_2 = f(x_2)$$

$$h_3 = f(x_3)$$

$\mathsf{Output}(x_2, h_2^{(q+1)/4})$ if h_2 is square, else$(x_3, h_3^{(q+1)/4})$