# Hashing to Elliptic Curves

#### draft-sullivan-cfrg-hash-to-curve

Nick Sullivan (<u>nick@cloudflare.com</u>) Christopher A. Wood (<u>cawood@apple.com</u>)

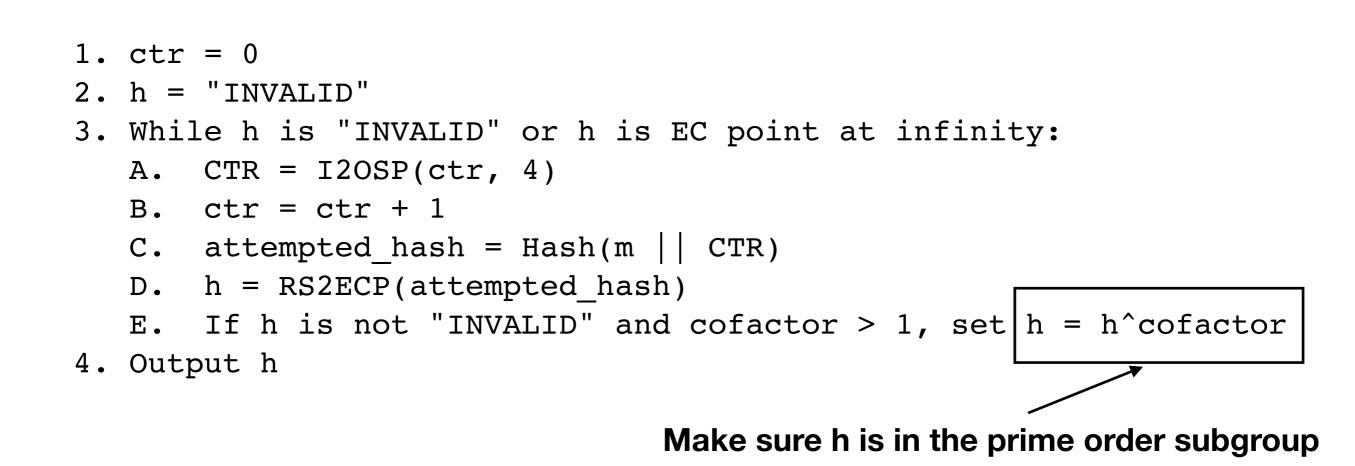
> CFRG IETF 101, March 2018, London

# 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 [<u>https://privacypass.github.io</u>]

# **Try-and-Increment**



# (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

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

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

#### lcart

$$\begin{split} t &= \mathsf{H}(\alpha) \\ v &= ((3A - t^4)/6t) \\ x &= (v^2 - b - (t^6/27))^{1/3} + (t^2/3) \\ y &= tx + v \\ \mathsf{Output}(x,y) \end{split}$$

# Elligator2

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

#### (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?

# Simplified SWU

 $t = H(\alpha)$  $x = -t^2$  $x_2 = (-b/a) \cdot (1 + (1/(t^2 + t)))$  $x_3 = t \cdot x_2$  $h_2 = f(x_2)$  $h_3 = f(x_3)$ Output $(x_2, h_2^{(q+1)/4})$  if  $h_2$  is square, else $(x_3, h_3^{(q+1)/4})$