Hash to curve update

Armando Faz-Hernández, Sam Scott, Nick Sullivan, Riad S. Wahby, Christopher A. Wood

IETF 105 - CFRG - 25 July 2019
Hash to curve: Roadmap

Three big pieces:

1. hash_to_base
   Arbitrary string $\rightarrow$ Element of finite field $\mathbb{F}$

2. map_to_curve
   Element of $\mathbb{F} \rightarrow$ Point on E over base field $\mathbb{F}$

3. clear_cofactor
   Point on E $\rightarrow$ Point in prime-order subgroup $G$

Goal: *constant-time* hashing for any E. *(No hash-and-check!)*
**hash_to_base** (string $\rightarrow \mathbb{F}$)

parameterized by field $\mathbb{F}$ and a hash function $H$

- Explicit security requirements
  - ensure collision resistance, uniform distribution over $\mathbb{F}$

- Build from HKDF
  - security even if $H$ is not perfect

- “Prehash for free”
  - only need to hash long input string once

- Domain separation guidelines
  - helps with protocol composition (but: not a panacea!)
map_to_curve (\(\mathbb{F} \rightarrow \) point on E)

- Specify how to choose sign of resulting point
  - Interoperability without needing to specify how to compute \(\sqrt{x}\)

- Explicitly handle exceptional cases
  - map_to_curve functions are defined over all of \(\mathbb{F}\)

- Removed SWU in favor of (generalized) Simplified SWU
  - faster, handles all of the same curves (but: IPR worries?)

- Unified Elligator 2 for Montgomery and Edwards
  - faster for Edwards, plus cross-curve interoperability

- New map for pairing-friendly (and other) curves [WB19]
Hash-to-curve suites

specs for widely-used curves, right now comprising:
- NIST curves (P-256, P-384, P-521)
- RFC7748 (*25519 / *448)
- secp256k1
- BLS12-381

-04 includes constant-time*, optimized pseudocode for P-256, *25519, *448
- *assuming, of course, that all primitives are constant time!
- future drafts will provide pseudocode for all suites

Planned additions:
- other curves (e.g., from pairings I-D)
- flowchart to identify params for curves that are not covered (?)
Open questions and discussion

➔ What other suites are needed?
   ◆ supersingular curves with \( j \in \{0, 1728\} \) (use CSIDH p511?)

➔ IPR concerns
   ◆ Icart, Simplified SWU may have patent entanglements
   ◆ Proposal: use Shallue and van de Woestijne as IPR fallback.
     Performance / implementation complexity are same as SWU,
     and SvdW covers Icart, Simplified SWU, and more.

➔ Others?
   ◆ email: draft-irtf-cfrg-hash-to-curve@ietf.org
   ◆ GitHub: https://github.com/cfrg/draft-irtf-cfrg-hash-to-curve/