draft-irtf-cfrg-hash-to-curve

IETF 106 – CFRG – Singapore

Major Updates

Removed Icart

Promoted Simplified SWU for (Weierstrass) AB == 0 case

Shallue-van de Woestijne parameterization now applies to all curves (previously applied only to $p = 1 \bmod 3$)

Minor Updates

Add guidance for curve mapping functions

Add guidance for alternate `hash_to_base` functions

Clarify domain separation requirements*

Clarify and specify output point sign to align with `draft-irtf-cfrg-vrf`

Add optimized and constant-time square root computations

Add Z selection code

* Thanks to Chris Patton and Benjamin Lipp!

Status and Next Steps

Pending work items

- Add test vectors (derived from proof of concept Sage code)
- Finish ongoing implementations

Start RGLC?