Alternative
Elliptic Curve Representations

draft-ietf-lwig-curve-representations-03

René Struik
Struik Security Consultancy
E-mail: rstruik.ext@gmail.com

IETF 104 – Prague, Czech Republic, March 26, 2019
Background

History:
– Initial document presented on March 21, 2018 @ IETF-101
– Adopted as WG doc after IETF-102 meeting Montreal, July 2018
– Full details on curve-related material prior to IETF-103

Background:
– NIST curves and CFRG curves use different curve models, thereby seemingly precluding code reuse
– Draft shows how curve models are related, by showing how one can switch between curve models via alternative representations
– Draft illustrates how to reuse existing code for NIST prime curves to implement CFRG curves (e.g., combine P-256 curve + Curve25519)
– Draft also illustrates how to use this to reuse existing standards
– Draft illustrates how to implement Edwards curve via Montgomery ladder, thereby allowing also code reuse amongst just CFRG curves
Current Status

What is in current WG draft?

– Incorporates worked-out examples
  ♦ Implementations:
    – co-factor Diffie-Hellman (X25519) via Weierstrass curve;
    – EdDSA signing via Montgomery ladder for Curve25519;
  ♦ Specifications:
    – NIST-compliant specification co-factor Diffie-Hellman (ECDH) for CFRG curves (usable with §4.2 of draft-selander-ace-cose-ecdh-13)
    – ECDSA signatures using Weierstrass form of Curve25519 and SHA256 (“ECDSA25519” – used with draft-ietf-6lo-ap-nd-11)
    – Includes self-contained treatment of group laws, field arithmetic, data representations and conversions, and detailed examples

Rev03 vs. rev02:

– Detailed examples, with formats, for all Curve25519 family members
– Expanded security considerations and IANA considerations
Next Steps

Readiness Draft:
– **Document is ready** (of course, more eyes on this always welcome)

Document Review Status:
– Early suggestions by Nikolas Rösener, Phillip Hallam-Baker
– Detailed crypto panel review by Stanislav Smyshlyaev
  (included verification of all curve parameters and mappings)
– **Still ongoing**: check examples in Appendix K (Stanislav Smyshlyaev)
  (I provided Sage code routines to make this less burdensome)

Implementations:
  See [https://community.nxp.com/docs/DOC-330199](https://community.nxp.com/docs/DOC-330199) (mentions 10x speed-up with *existing* ECC HW)
[3] ECDSA25519 specified with draft-ietf-6lo-ap-nd-11