ECC Cipher Suite Discussion (for Constrained Networks)

René Struik

Struik Security Consultancy

E-mail: rstruik.ext@gmail.com

Scheme Implementation Details (1)

Signature aspect:	**ECDSA256**	**Ed25519**	**ECDSA25519**
Curve model:	Weierstrass	twisted Edwards	Weierstrass
Curve:	P-256	Edwards25519	Wei25519
Hash function:	SHA256	SHA512	SHA256
Sign algorithm:	ECDSA	full-Schnorr	ECDSA
Public key size:	32 bytes	32 bytes	32 bytes
Signature size:	64 bytes	64 bytes	64 bytes
determinism:	nondeterministic	deterministic	nondeterministic

ECDH aspect:	**ECDH256**	**X25519**	**ECDH25519**
Curve model:	Weierstrass	Montgomery	Weierstrass
Public key:	compressed	x-coord only	compressed
DH algorithm:	co-factor ECDH	ECDH	co-factor ECDH
Validation checks:	strict	lenient	strict

ECDHOC suites:	**2-3**	**0-1**	**new (suggested)**

Scheme Implementation Details (2)

Cipher Suite 0-1: X25519 w/ Curve25519, Ed25519 signatures w/ Edwards25519
Cipher Suite 2-3: co-factor ECDH, ECDSA w/ SHA256, with P-256
Suggested suite Z: co-factor ECDH, ECDSA w/ SHA256, with Wei25519
(alternative for #5: A128GCM, SHA-256, X25519, ES256, P-256, A128GCM, SHA-256)

Properties of Suite Z:

Reuse of existing generic implementations NIST standards (incl. HW speed-ups)

Leverage FIPS 140-2 accreditation with NIST-compliant implementations (co-factor ECDH, ECDSA)

Common data formats and ordering conventions, common strict validation checks

Wei25519 can use Curve25519 code (so no write-off of code development cost)

No need for SHA256 *and* SHA512, no trivial fault attacks, extensible

Further Reading

FIPS 140-2, "Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program", US Dept of Commerce/NIST, Aug 28, 2020

FIPS 186-5 (draft), "Digital Signature Standard (DSS)", US Dept of Commerce/NIST, Oct 31, 2019

NIST SP 800-186 (draft), "Recommendations for Discrete Logarithm-Based Cryptography, Elliptic Curve Domain Parameters", US Dept of Commerce/NIST, Oct 31, 2019

draft-ietf-lwig-curve-representations-19 (137 pp, Dec 17, 2020)

slides-101-lwig-4-lwig-curve-representations-01 (March 21, 2018)

Curve Details

Curve aspect:	NIST P-256	Curve25519	Edwards25519
Curve model:	Weierstrass	Montgomery	twisted Edwards
Base point:	affine	x-coord only	affine
Internal coord:	Jacobian	x-projective	extended
Formulae:	Jacobian	Montgomery	Dawson
Wire format:	compressed	x-coord only	compressed
Bit/Octet ordering:	MSB, msb	LSB, msb	LSB, lsb

Implementation drawback:
different arithmetic, different point format, different bit/octet encoding

Lots of code to implement...
a) key agreement co-factor ECDH using NIST P-256 + Curve25519 (TLS1.3);
b) key agreement + sign/verify Curve25519 + Ed25519 (JOSE [RFC 8037]);
c) key agreement + sign/verify P-256 + ECDSA & Curve25519 + Ed25519