Sandy2x: Fastest Curve25519 Implementation Ever

Tung Chou

Technische Universiteit Eindhoven, The Netherlands

Spetember 28, 2015

X25519 and Ed25519

X25519

- ECDH scheme
- public keys and shared secrets are points on the Montgomery curve

$$y^2 = x^3 + 486662x^2 + x$$

  over $\mathbb{F}_{2^{255}-19}$
- by Bernstein, 2006

Ed25519

- signature scheme
- public keys and (part of) signatures are points on the twisted Edwards curve

$$-x^2 + y^2 = 1 - 121665/121666x^2y^2$$

  over $\mathbb{F}_{2^{255}-19}$
- by Bernstein, Duif, Lange, Schwabe, and Yang, 2011

Performance results

	SB cycles	IB cycles	reference
X25519 public-key generation	54 346	52 169	**Sandy2x**
	61 828	57 612	[A. Moon]
	194 165	182 876	[Ed25519]
X25519 shared secret computation	156 995	159 128	**Sandy2x**
	194 036	182 708	[Ed25519]
Ed25519 public-key generation	57 164	54 901	**Sandy2x**
	63 712	59 332	[A. Moon]
	64 015	61 099	[Ed25519]
Ed25519 sign	63 526	59 949	**Sandy2x**
	67 692	62 624	[A. Moon]
	72 444	67 284	[Ed25519]
Ed25519 verification	205 741	198 406	**Sandy2x**
	227 628	204 376	[A. Moon]
	222 564	209 060	[Ed25519]

- Andrew Moon “floodyberry”, https://github.com/floodyberry/ed25519-donna

The Big multiplier and Small multiplier

The Big multiplier

- $64 \times 64 \rightarrow 128$-bit multiplications

The Small multiplier

- 2-way vectorized
- $32 \times 32 \rightarrow 64$-bit multiplications

The Big multiplier and Small multiplier

The Big multiplier

- $64 \times 64 \rightarrow 128$-bit multiplications

The Small multiplier

- 2-way vectorized
- $32 \times 32 \rightarrow 64$-bit multiplications

Paper and Code available at

- SAC 2015
- https://sites.google.com/a/crypto.tw/blueprint/