

High-speed high-security signatures

Peter Schwabe

National Taiwan University



Joint work with Daniel J. Bernstein, Niels Duif,
Tanja Lange and Bo-Yin Yang

September 19, 2011

ECC 2011 Rump Session

Ed25519 speed

- ▶ 128-bit-secure elliptic-curve signatures

Ed25519 speed

- ▶ 128-bit-secure elliptic-curve signatures
- ▶ Fast signature verification: 273364 cycles on Intel Nehalem/Westmere (eBATS benchmark)

Ed25519 speed

- ▶ 128-bit-secure elliptic-curve signatures
- ▶ Fast signature verification: 273364 cycles on Intel Nehalem/Westmere (eBATS benchmark)
- ▶ Even faster batch verification: 134000 cycles/signature to verify 64 signatures of 64 messages under 64 public keys
4 × 2.4GHz: 71000 verifications/second!

Ed25519 speed

- ▶ 128-bit-secure elliptic-curve signatures
- ▶ Fast signature verification: 273364 cycles on Intel Nehalem/Westmere (eBATS benchmark)
- ▶ Even faster batch verification: 134000 cycles/signature to verify 64 signatures of 64 messages under 64 public keys
4 × 2.4GHz: 71000 verifications/second!
- ▶ Very fast signing: 87548 cycles (eBATS benchmark)
4 × 2.4GHz: 108000 signs/second

Ed25519 speed

- ▶ 128-bit-secure elliptic-curve signatures
- ▶ Fast signature verification: 273364 cycles on Intel Nehalem/Westmere (eBATS benchmark)
- ▶ Even faster batch verification: 134000 cycles/signature to verify 64 signatures of 64 messages under 64 public keys
4 × 2.4GHz: 71000 verifications/second!
- ▶ Very fast signing: 87548 cycles (eBATS benchmark)
4 × 2.4GHz: 108000 signs/second
- ▶ Fast key-pair generation: Almost as fast as signing

- ▶ 128-bit-secure elliptic-curve signatures
- ▶ Fast signature verification: 273364 cycles on Intel Nehalem/Westmere (eBATS benchmark)
- ▶ Even faster batch verification: 134000 cycles/signature to verify 64 signatures of 64 messages under 64 public keys
4 × 2.4GHz: 71000 verifications/second!
- ▶ Very fast signing: 87548 cycles (eBATS benchmark)
4 × 2.4GHz: 108000 signs/second
- ▶ Fast key-pair generation: Almost as fast as signing
- ▶ Signatures have only 64 bytes (no hidden slowdowns)

- ▶ 128-bit-secure elliptic-curve signatures
- ▶ Fast signature verification: 273364 cycles on Intel Nehalem/Westmere (eBATS benchmark)
- ▶ Even faster batch verification: 134000 cycles/signature to verify 64 signatures of 64 messages under 64 public keys
4 × 2.4GHz: 71000 verifications/second!
- ▶ Very fast signing: 87548 cycles (eBATS benchmark)
4 × 2.4GHz: 108000 signs/second
- ▶ Fast key-pair generation: Almost as fast as signing
- ▶ Signatures have only 64 bytes (no hidden slowdowns)
- ▶ Public keys have only 32 bytes (no hidden slowdowns)

- ▶ No secret array indices, no information flow from secret data to addresses \Rightarrow no cache-timing attacks
- ▶ No secret branch conditions, no information flow from secret data to branch unit
- ▶ Collision resilience, hash collisions do not break this signature system
- ▶ Elimination of Sony-style stupidity, signing is deterministic

- ▶ No secret array indices, no information flow from secret data to addresses \Rightarrow no cache-timing attacks
- ▶ No secret branch conditions, no information flow from secret data to branch unit
- ▶ Collision resilience, hash collisions do not break this signature system
- ▶ Elimination of Soly-style stupidity, signing is deterministic

**CONDITIONALLY
ACCEPTED**

- ▶ No secret array indices, no information flow from secret data to addresses \Rightarrow no cache-timing attacks
- ▶ No secret branch conditions, no information flow from secret data to branch unit
- ▶ Collision resilience, hash collisions do not break this signature system
- ▶ Elimination of Sony-style stupidity, signing is deterministic

- ▶ No secret array indices, no information flow from secret data to addresses \Rightarrow no cache-timing attacks
- ▶ No secret branch conditions, no information flow from secret data to branch unit
- ▶ Collision resilience, hash collisions do not break this signature system
- ▶ Foolproof session keys, signing is deterministic

- ▶ No secret array indices, no information flow from secret data to addresses \Rightarrow no cache-timing attacks
- ▶ No secret branch conditions, no information flow from secret data to branch unit
- ▶ Collision resilience, hash collisions do not break this signature system
- ▶ Foolproof secret keys, signing is deterministic

ACCEPTED

- ▶ Software uses NaCl/SUPERCOP API
- ▶ Included in SUPERCOP <http://bench.cr.yp.to/supercop.html>
- ▶ Will also be in NaCl <http://nacl.cr.yp.to/>
- ▶ Public domain – use it any way you want!

<http://ed25519.cr.yp.to>