High-speed high-security signatures

D. J. Bernstein
University of Illinois at Chicago

Niels Duif
Technische Universiteit Eindhoven

Tanja Lange
Technische Universiteit Eindhoven

Peter Schwabe
National Taiwan University

Bo-Yin Yang
Academia Sinica

Fast signature verification.

Intel Nehalem/Westmere CPUs:
280880 cycles for verification.
(Official eBATS measurement.)

Fast signature verification.

Intel Nehalem/Westmere CPUs:
280880 cycles for verification.
(Official eBATS measurement.)

Even faster batch verification.

$<$ 134000 cycles/signature
to verify 64 signatures of
64 messages under 64 public keys.
4×2.4GHz: 71000 verif/second!

Fast signature verification.
Intel Nehalem/Westmere CPUs:
280880 cycles for verification.
(Official eBATS measurement.)

Even faster batch verification.
$<$ 134000 cycles/signature
to verify 64 signatures of
64 messages under 64 public keys.
4×2.4GHz: 71000 verif/second!

Very fast signing.
88328 cycles for signing.
(Official eBATS measurement.)
4×2.4GHz: 108000 signs/second!

Fast key generation.

Almost as fast as signing.

Fast key generation.
Almost as fast as signing.

High security level.
$> 2^{128}$ operations for
all attacks known
(without quantum computers).

Fast key generation.
Almost as fast as signing.

High security level.
$> 2^{128}$ operations for
all attacks known
(without quantum computers).

Small signatures.
64 bytes for signature.
No hidden slowdowns.

Fast key generation.
Almost as fast as signing.

High security level.
$> 2^{128}$ operations for
all attacks known
(without quantum computers).

Small signatures.
64 bytes for signature.
No hidden slowdowns.

Small keys.
32 bytes for public key.
No hidden slowdowns.

No secret array indices.

No information flow from secret data to addresses.

$\Rightarrow$ No cache-timing attacks.

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.

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.

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.

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 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.

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.

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 session keys.
Signing is deterministic.

Software uses the
NaCl/SUPERCOP API:
`crypto_sign_keypair`,
`crypto_sign`,
`crypto_sign_open`.

Available now in SUPERCOP:
`bench.cr.yp.to/supercop.html`

Will also be in NaCl:
`nacl.cr.yp.to`

Public domain—
use it any way you want!

Paper is online:
`ed25519.cr.yp.to`