(Tweet)NaCl

Daniel J. Bernstein, Tanja Lange, Peter Schwabe

December 29, 2013

30C3, Hamburg

(Tweet)NaCl

NaCl http://nacl.cr.yp.to

- Networking and Cryptography library
- Contributions by Matthew Dempsky, Adam Langley, Niels Duif, Bo-Yin Yang, Emilia Käsper
- Paper: http://cryptojedi.org/papers/#coolnacl
- For wider audience
  http://nacl.cr.yp.to/securing-communication.pdf

TweetNaCl http://tweetnacl.cr.yp.to

- All NaCl functions used by applications in 100 tweets
- Joint work with Wesley Janssen
- http://twitter.com/tweetnacl
- Paper: http://cryptojedi.org/papers/#tweetnacl

(Tweet)NaCl – Functionality

- High-level, easy-to-use API
- Core functionality: Public-key authenticated encryption:

```
c = crypto_box(m,n,pk,sk)
m = crypto_box_open(c,n,pk,sk)
```

- Similarly high-level API for signatures:

```
sm = crypto_sign(m, sk)
m = crypto_sign_open(sm, pk)
```

- Various lower-level functionalities (scalar multiplication, secret-key authenticated encryption, stream encryption hashing)

(Tweet)NaCl – Security

- All primitives have ≥ 128 bits of security against known attacks
- Very conservative choice of primitives
- No timing leaks from secret branch predictions
- No timing leaks from secret load/store addresses
- No padding oracles
- Centralized randomness generation from the OS
- No unnecessary randomness

(Tweet)NaCl – Speed

NaCl

- Exceptionally high speed, e.g. on AMD Phenom II X6 1100T CPU:
  - > 80000 public-key authenticated encryption/second
  - > 80000 public-key verify-and-decrypt/second
  - > 70000 signatures/second
  - > 180000 signature verifications/second
  - Various speedups for multiple packets to the same public key; batch verification of signatures...

(Tweet)NaCl – Speed

NaCl

- Exceptionally high speed, e.g. on AMD Phenom II X6 1100T CPU:
  - > 80000 public-key authenticated encryption/second
  - > 80000 public-key verify-and-decrypt/second
  - > 70000 signatures/second
  - > 180000 signature verifications/second
  - Various speedups for multiple packets to the same public key; batch verification of signatures...

TweetNaCl

- Slower (e.g., $\approx 15\times$ for Curve25519); still fast enough for many applications
- Very small code base (human auditible!)
- Very easy to integrate (one `.c` file, one `.h` file)

(Tweet)NaCl – the future

Plans for 2014

- Next release of NaCl will have full PIC support, Ed25519 signatures, NEON optimizations.
- Port to AVR microcontrollers, joint work with Michael Hutter (for a preview see `http://cryptojedi.org/crypto/#avrnacl`)
- A cool logo for NaCl (ideas, suggestions...?)

Plans for 201[4-9]

- Full implementation of the networking part of NaCl
- Protection against larger class of side channels