CRYPTO
Part of Fox-IT

Quantum Security Deep Dive

Sander Dorigo
Security Architect @ Fox-IT
15 februari 2023

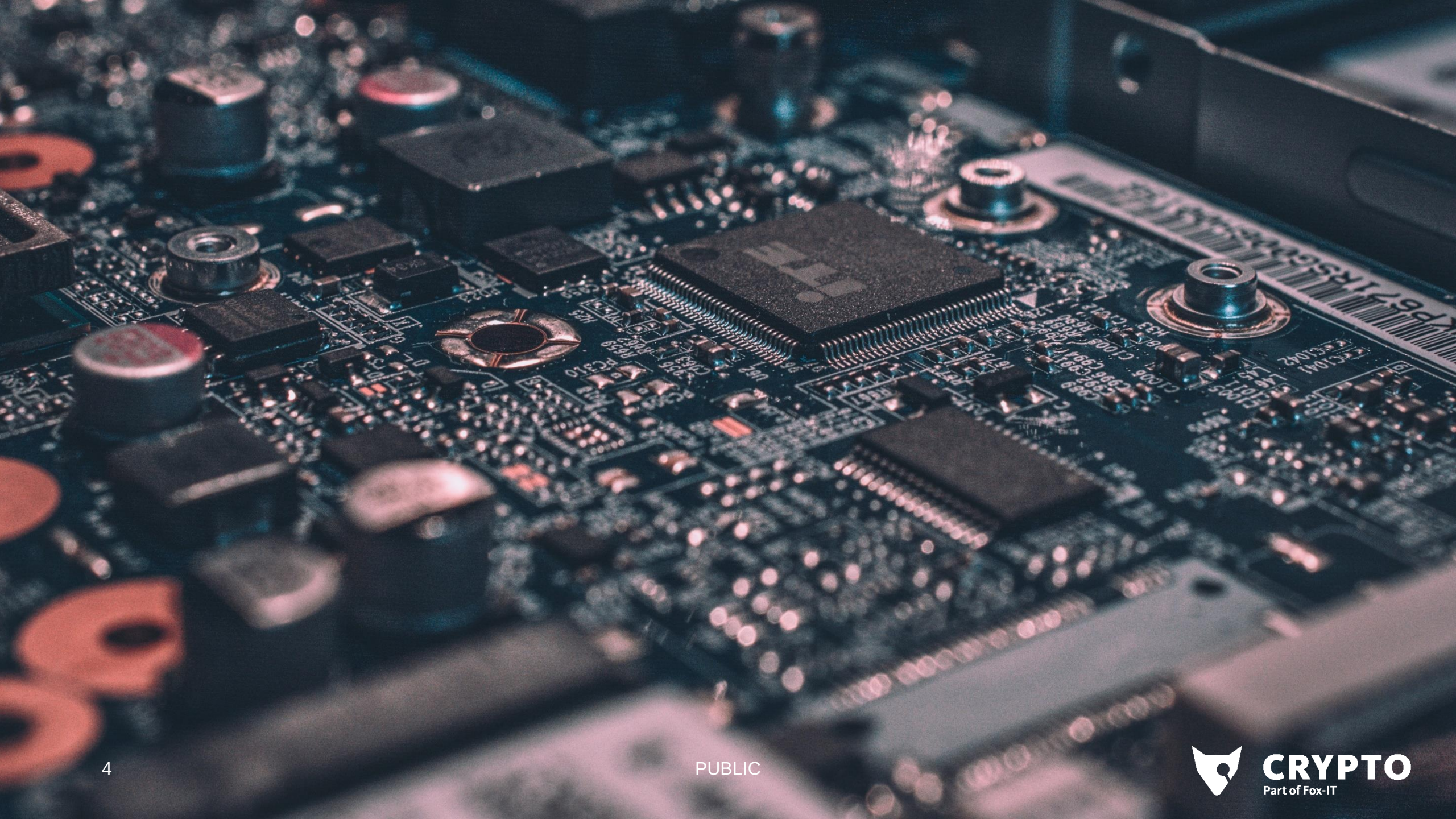
PUBLIC

PUBLIC

CRYPTO
Part of Fox-IT

PUBLIC

CRYPTO
Part of Fox-IT



PUBLIC

CRYPTO
Part of Fox-IT

Veranderingen in algoritmes

Nu

- RSA
- Diffie–Hellman
- ECC Diffie–Hellman
- ~ AES

Straks?

PUBLIC

NIST
CRYPTO
Part of Fox-IT

1: Klaar voor productie?

PUBLIC

CRYPTO
Part of Fox-IT

microsoft / PQCrypto-LWEKE Public

Watch 10 | Fork 33 | Star 8

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

master | PQCrypto-LWEKE / README.md | Go to file

patricklonga Add option to compile for s390x processors ✓ Latest commit 5540ce1 on Jun 15

4 contributors

206 lines (145 sloc) | 9.83 KB | Raw | Blame

FrodoKEM: Learning with Errors Key Encapsulation

This C library implements **FrodoKEM**, an IND-CCA secure key encapsulation (KEM) protocol based on the well-studied Learning with Errors (LWE) problem [1], which in turn has close connections to conjectured-hard problems on generic, "algebraically unstructured" lattices. This package also includes a Python reference implementation. **FrodoKEM** is conjectured to be secure against quantum computer attacks.

return value of randombytes() not checked #29

Closed [redacted] opened this issue on Jun 1 · 1 comment

[redacted] commented on Jun 1

For example during key generation:

PQCrypto-LWEKE/src/kem.c
Line 35 in 4210d53

```
35      randombytes(randomness, CRYPTO_BYTES + CRYPTO_BYTES + BYTES_SEED_A);
```

`randombytes()` can fail on Windows, which will go unnoticed and will lead to an insecure (possibly completely deterministic) key!

Additionally: the code in `randombytes.c` is not very well written for other reasons. On Linux, the code will simply deadlock if `\dev\urandom` is not available. And if you ever compile without either WINDOWS or NIX, then it defaults to returning `passed` instead of `failed`. But that last point doesn't actually matter, since the return value is not checked anyway...

👀 1

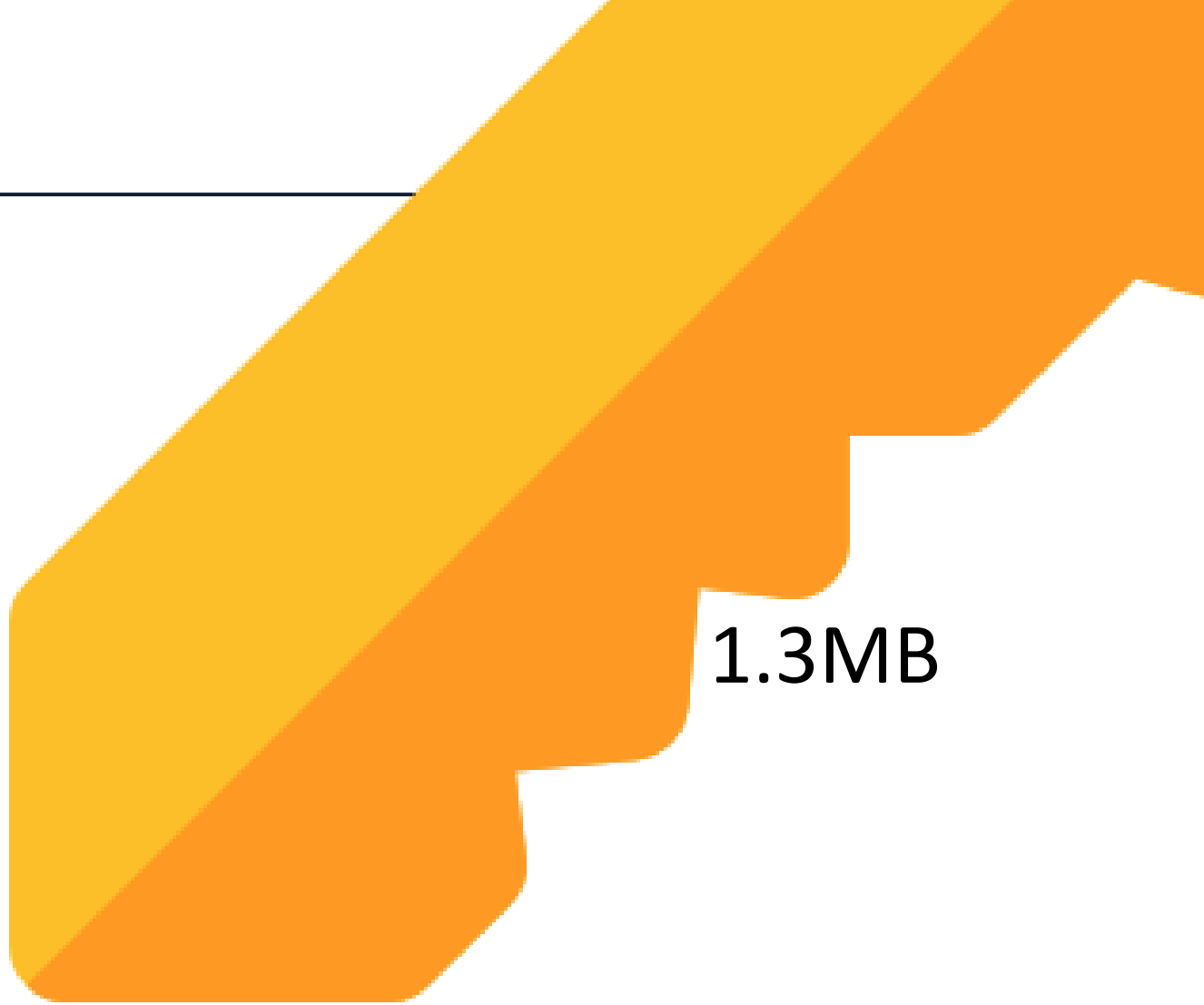
PUBLIC

2: Bijzondere sleutels

PUBLIC

CRYPTO
Part of Fox-IT

Bijzondere sleutels



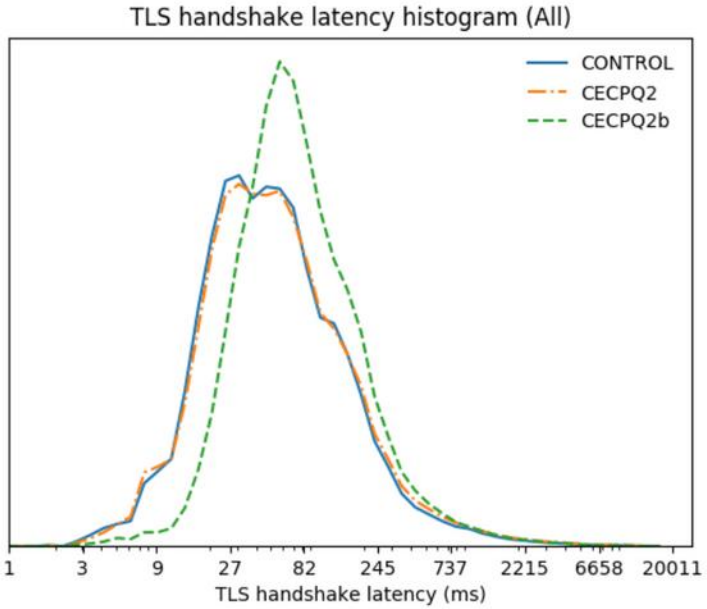
PUBLIC

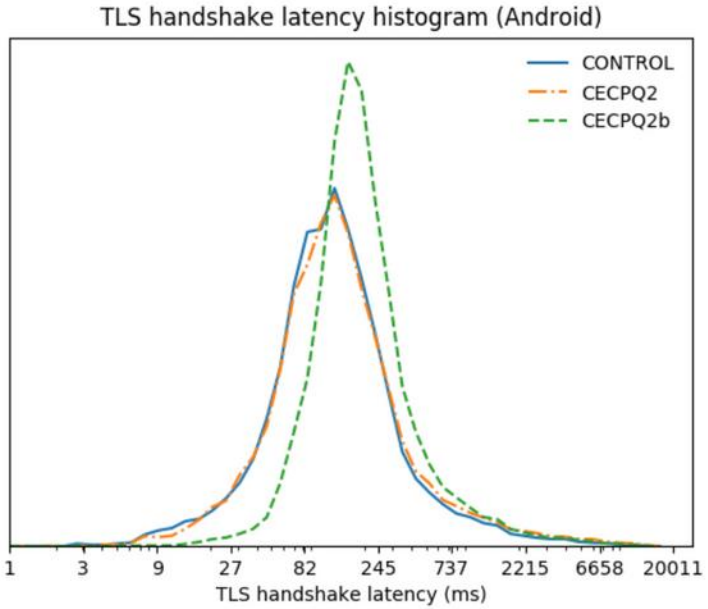
CRYPTO
Part of Fox-IT

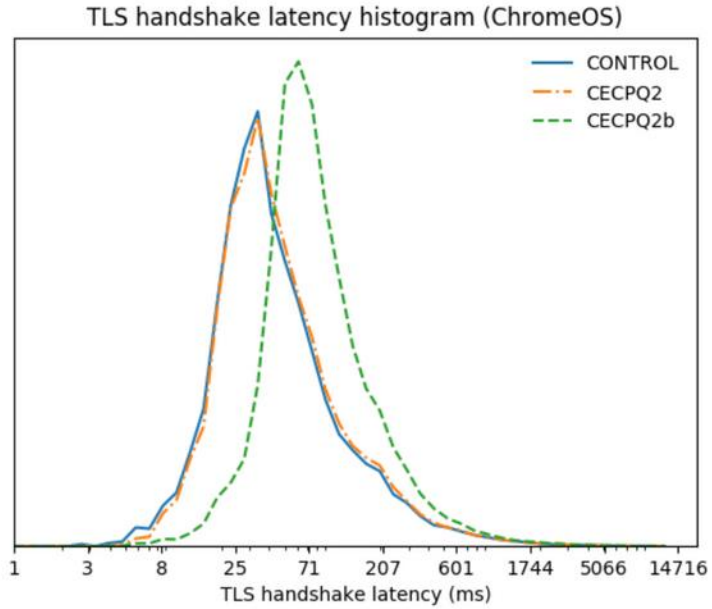
3: Hardware

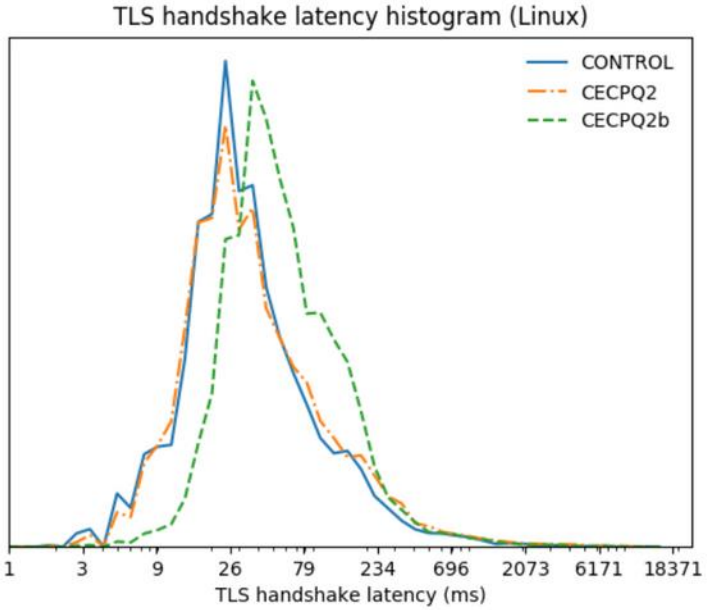
PUBLIC

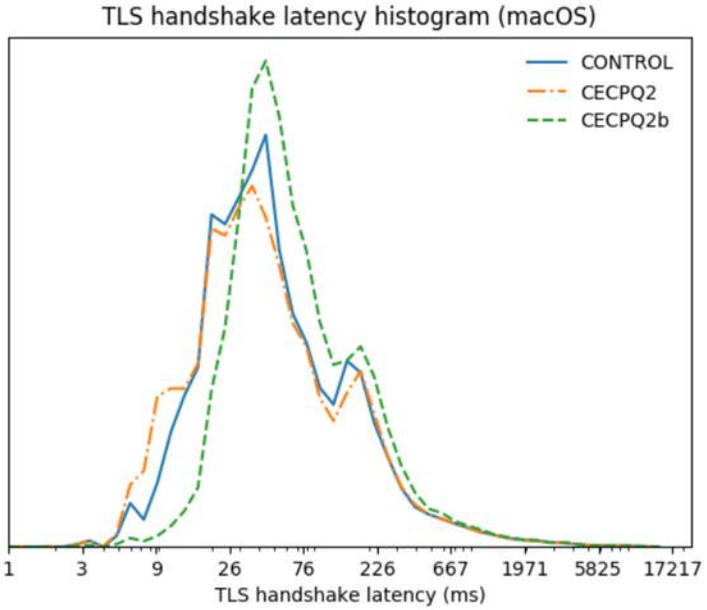
CRYPTO
Part of Fox-IT

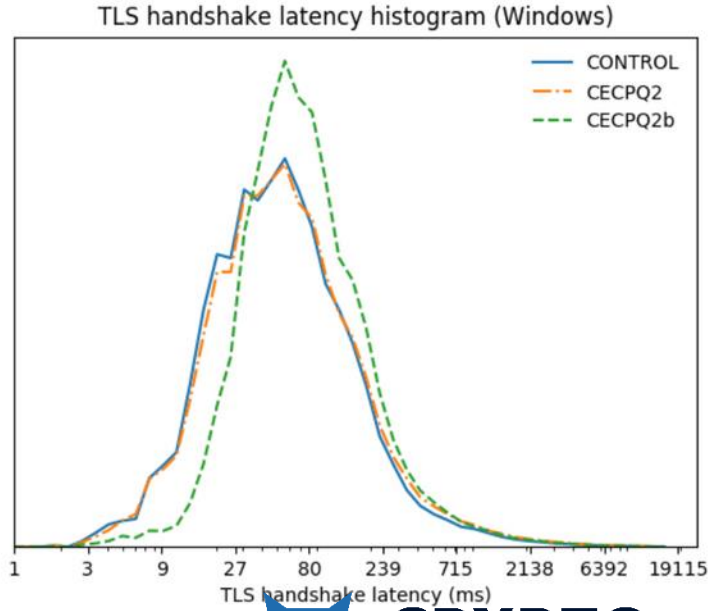








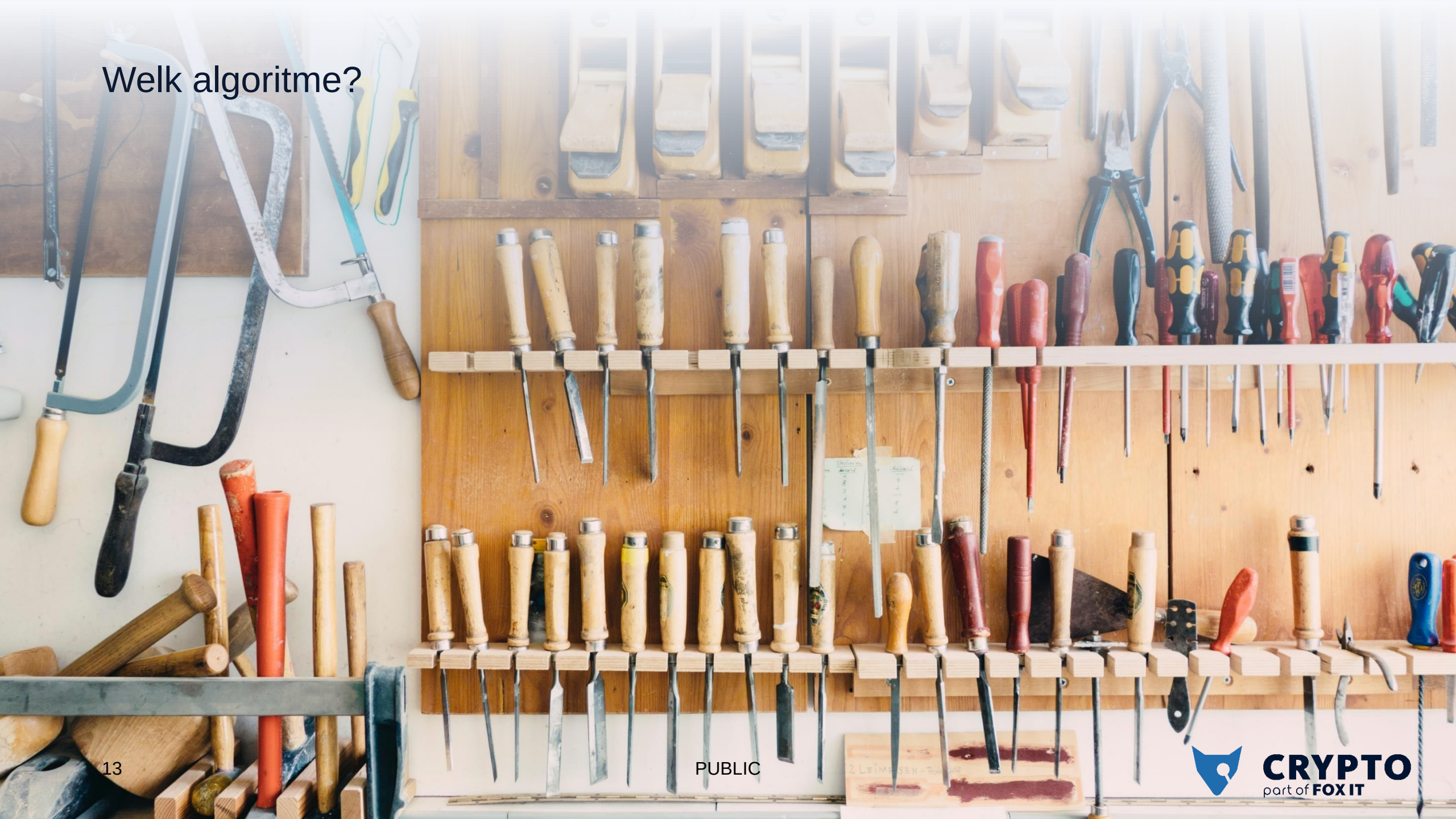




PUBLIC

CRYPTO part of FOX IT

Welk algoritme?



PUBLIC

CRYPTO part of FOX IT

Wat heb je nodig?

Key Encapsulation

Het versleutelen van een symmetrische sleutel

Digital signatures

Het authentiseren van digitale berichten

Public key encryption

Het versleutelen van (veel) data met behulp van een asymmetrische sleutel

(Authenticated) Key Exchange

Het afspreken van een te gebruiken (a)symmetrische sleutel. In-band of out-of-band

PUBLIC

Wat heb je nodig?

Key Encapsulation

- Lattice: FrodoKEM
- Code: BIKE

Digital signatures

Lattice: Dilithium, FALCON

Hash-based: SPHINC+, XMSS

Public key encryption

- Lattice: Kyber
- Code: Classic McEliece, HQC

(Authenticated) Key Exchange

- Lattice: Kyber
- Code: ClassicMcEliece, HQC
- *QKD*

Wat nu?

1. Migratiehandleiding post-quantum TNO / BZK
2. Onderzoek trade-offs door TNO / CWI / Fox-IT en anderen
3. NIST ronde 4
4. NIST PQ Digital Signature Schemes Standardization

Algoritme	CPU	RAM	Disk	Security	Side-channels	Etc ….
Kyber	++					
FrodoKEM						
XMSS			--			
Classic				+/-		?
HQC						
FALCON						

PUBLIC

TNO
CWI
Research institute for mathematics & computer science in the Netherlands
NIST
CRYPTO
Part of Fox-IT

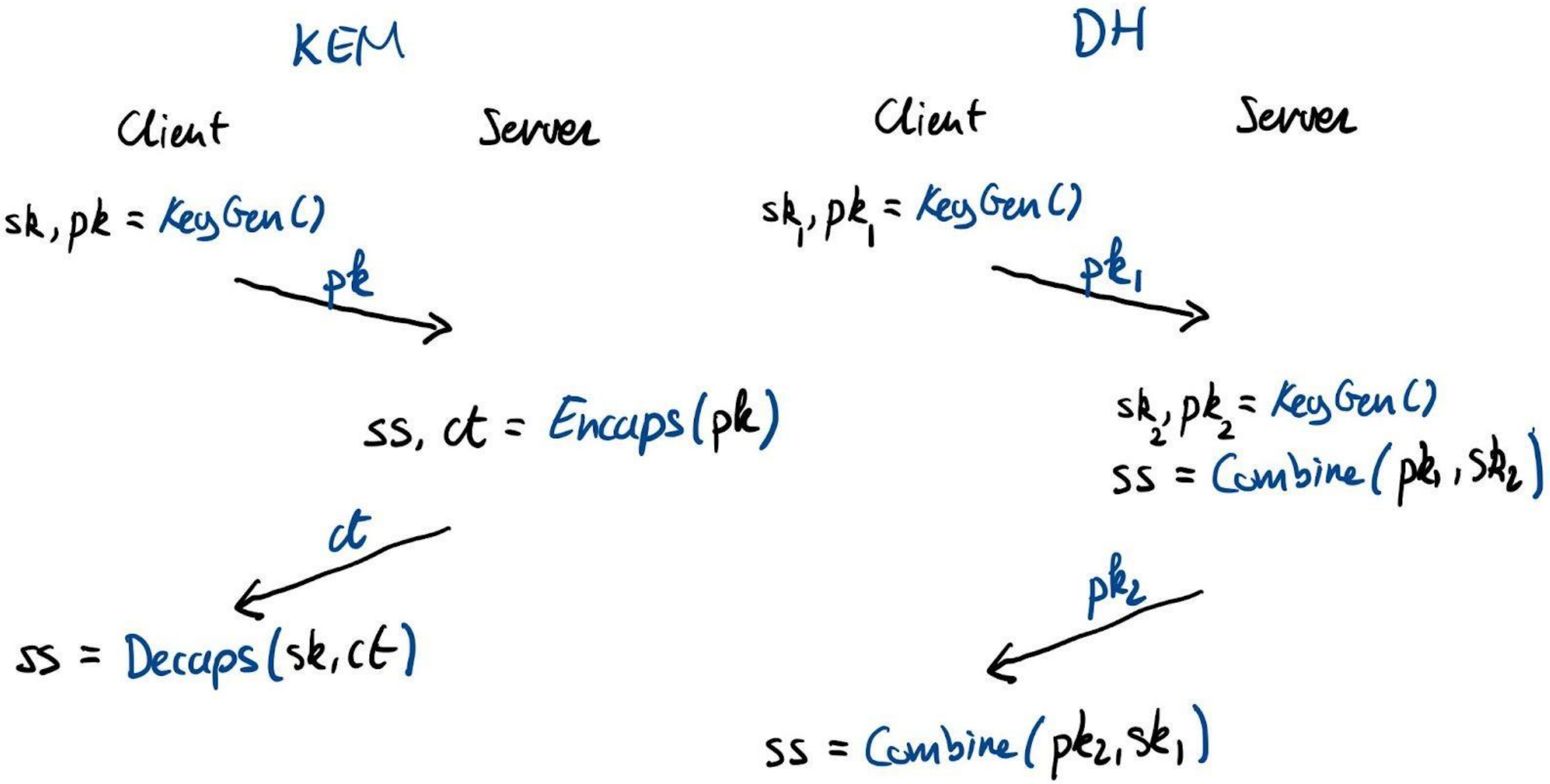
f0x.nl/pq

Question & Answers

Current state

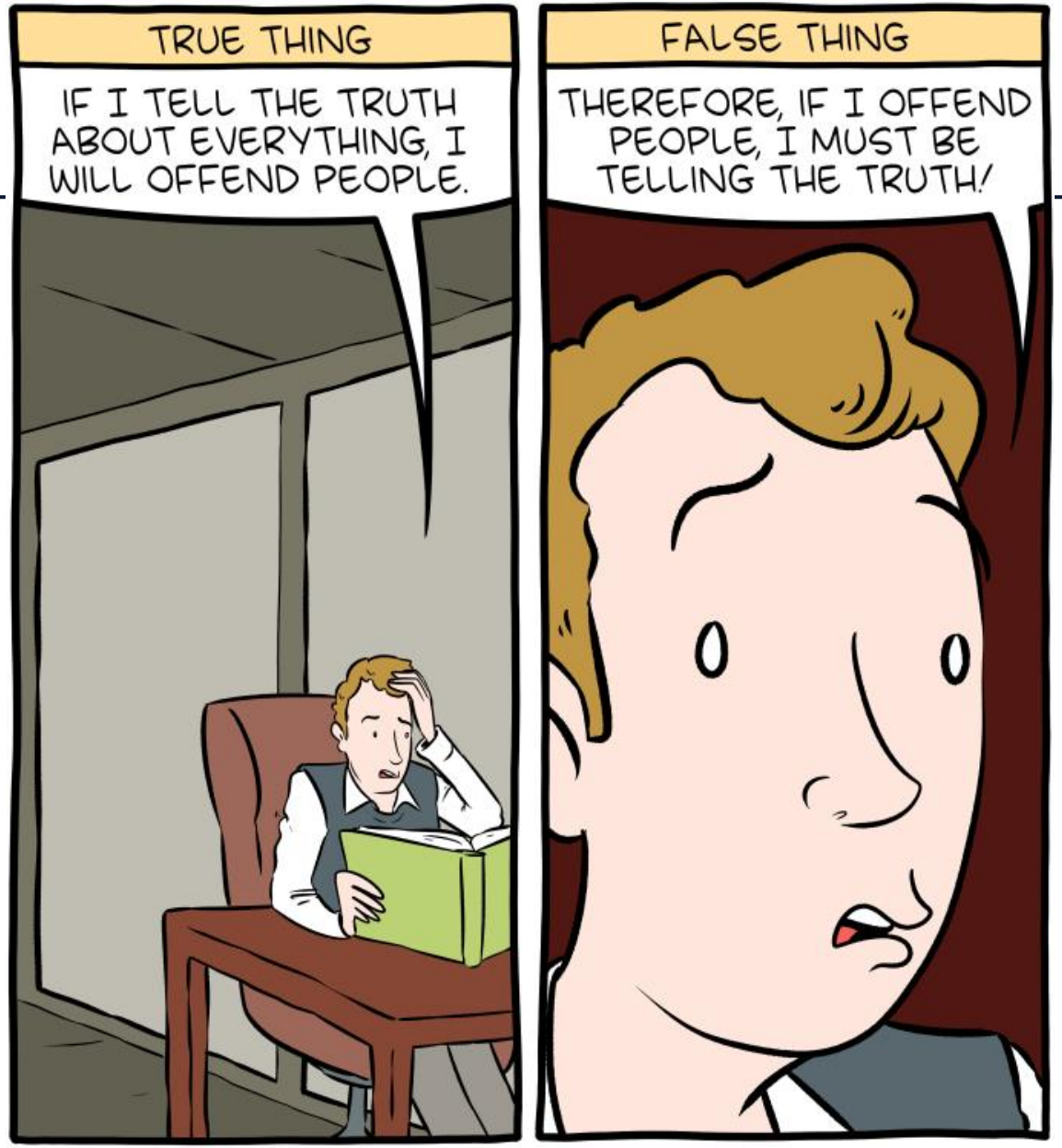
- Interactive versus non-interactive key agreement
- Stateful signatures
- Fast constant-time double-precision floating-point arithmetic

PUBLIC



PUBLIC

CRYPTO
Part of Fox-IT



Among scholars, this is known as the Daniel J. Bernstein Fallacy.

CRYPTO
Part of Fox-IT

Bijzondere processen

- Diffie Hellman?
- TLS requires public key encryption and a key derivation function for the key exchange (plus a signature algorithm for the PKI, if necessary)
  - Kan dus zonder DH. Zie werk van Thom Wiggers
  - Signal gebruikt 3XDH, nog geen goed alternatief voor

PUBLIC

f0x.nl/pq

Question & Answers