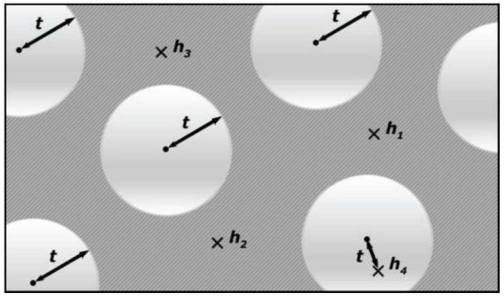
Recent Developments in Quantum Safe Crypto:

Hash-based Signatures

Andreas Hülsing

Trapdoor- / Identification Scheme-based (PQ-)Signatures



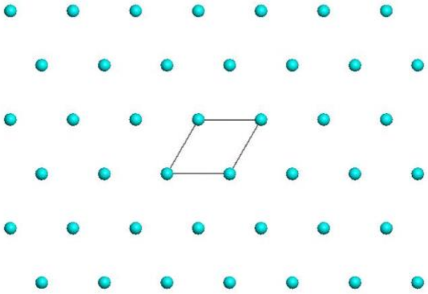
Lattice, MQ, Coding

- Signature and/or key sizes
- Runtimes
- Secure parameters

$$y_1 = x_1^2 + x_1x_2 + x_1x_4 + x_3$$

$$y_2 = x_3^2 + x_2x_3 + x_2x_4 + x_1 + 1$$

$$y_3 = \ldots$$



Hash-based Signature Schemes

[Mer89]

- Post quantum
- Only secure hash function
- Security well understood
- Fast

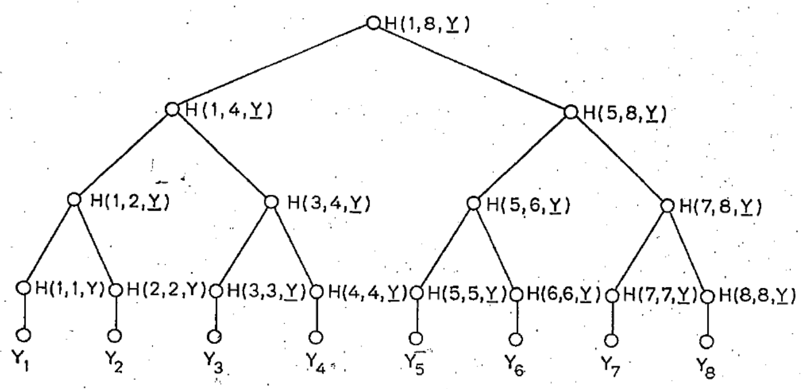
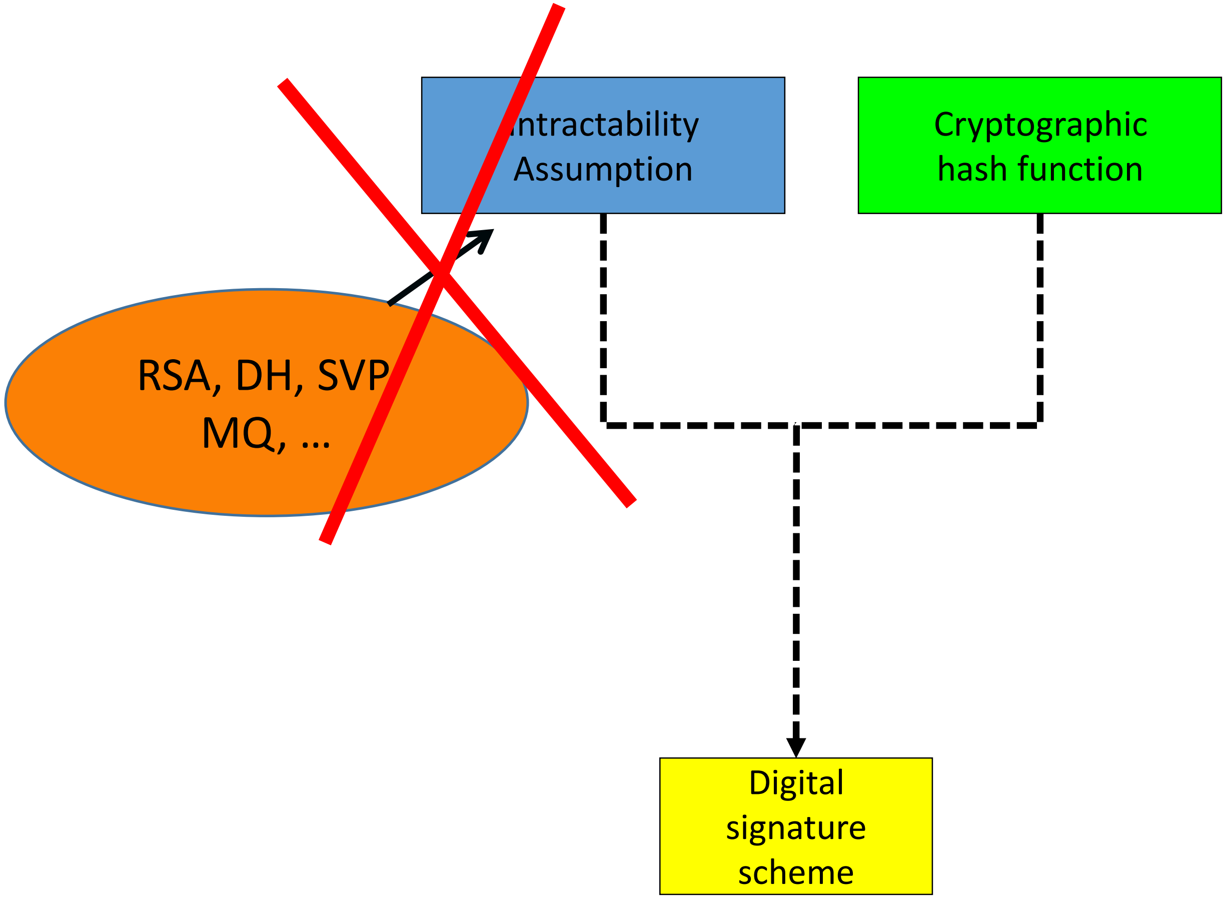


FIG 1

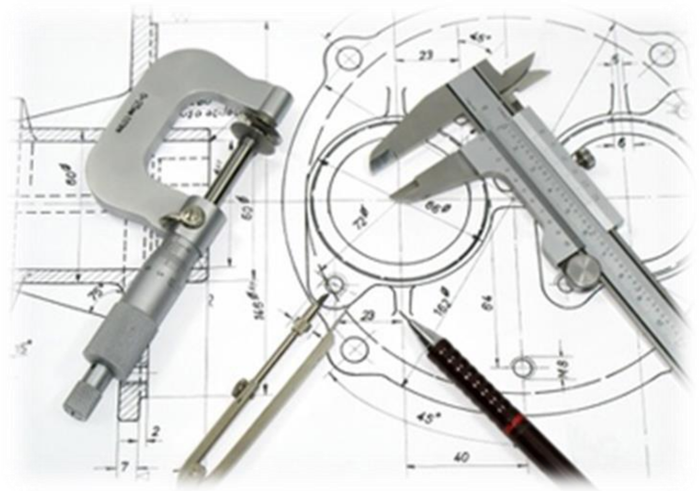
AN AUTHENTICATION TREE WITH N = 8.

PAGE 41B

RSA – DSA – EC-DSA…

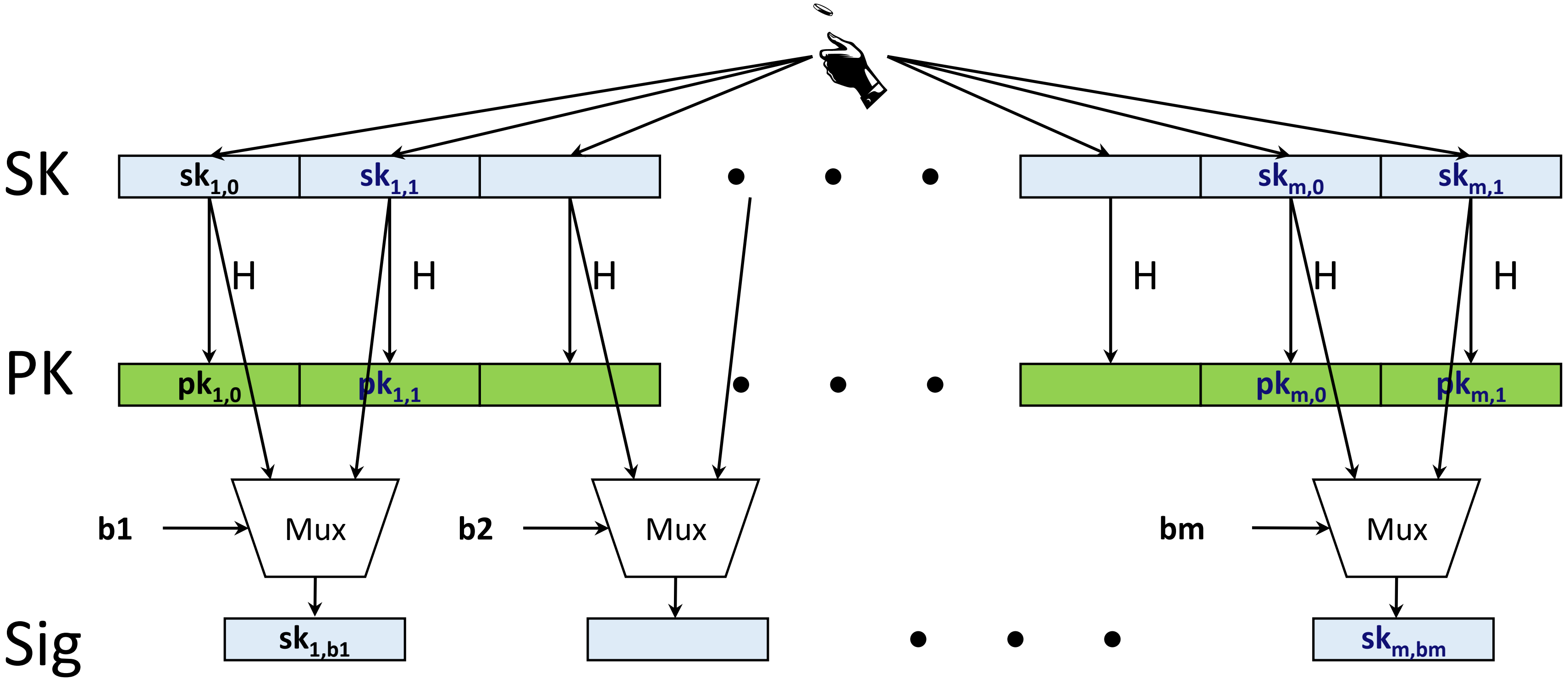


Basic Construction

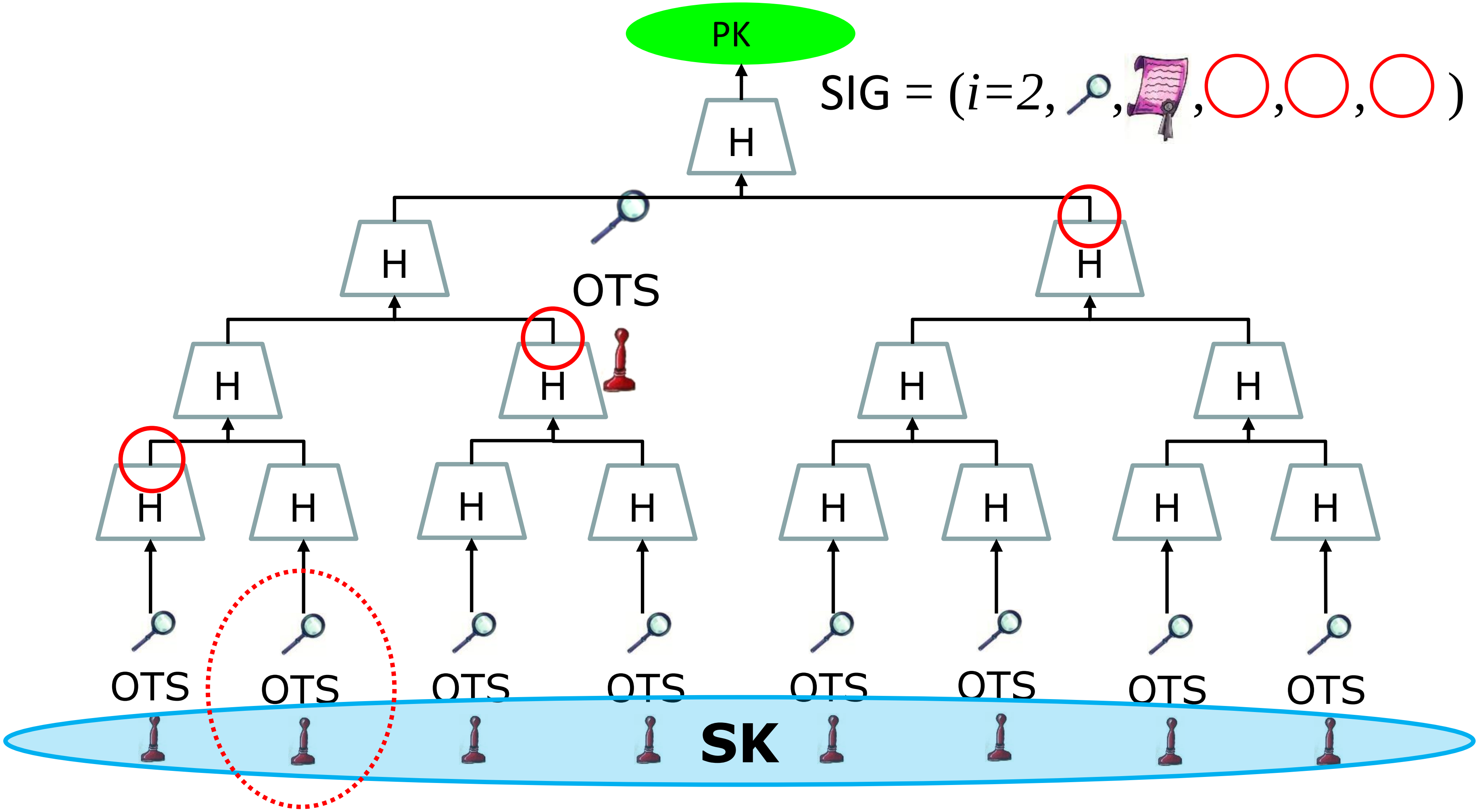


Lamport-Diffie OTS [Lam79]

Message M = b1,…,bm, OWF H $\boxed{\quad * \quad}$ = n bit



Merkle’s Hash-based Signatures



XMSS: Extended Hash-Based Signatures

draft-irtf-cfrg-xmss-hash-based-signatures-01

XMSS

Tree: Uses bitmasks

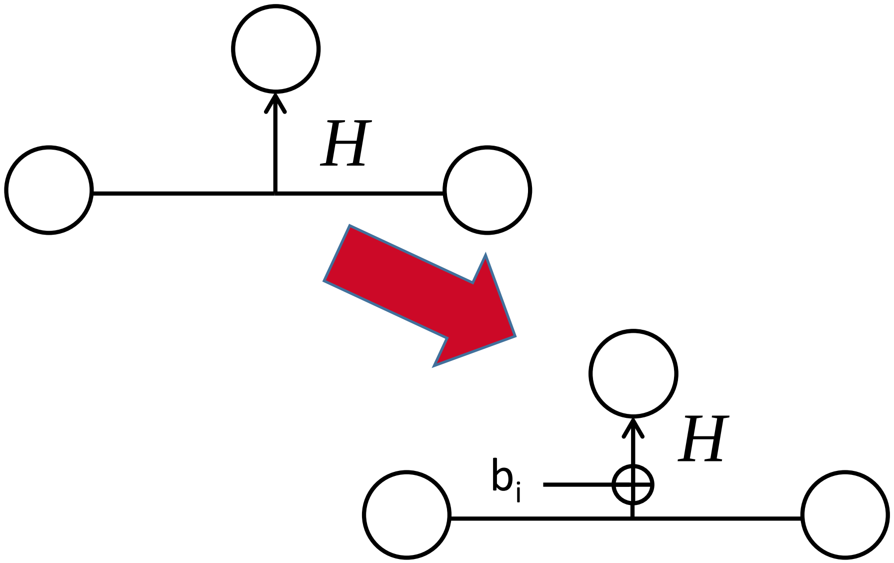
Leafs: Use binary tree with bitmasks

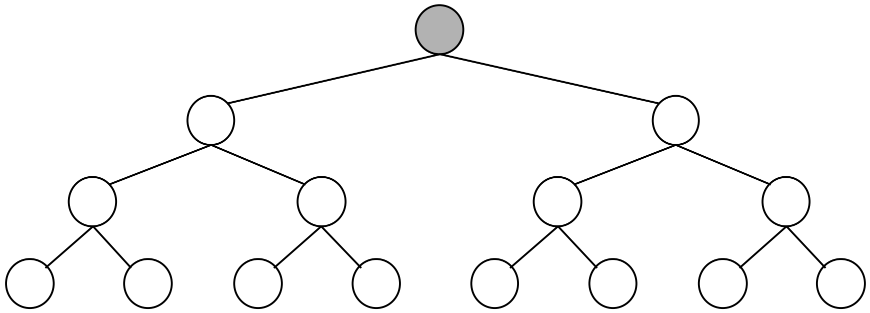
OTS: WOTS$^+$

Mesage digest: Randomized hashing

Collision-resilient

-> signature size halved



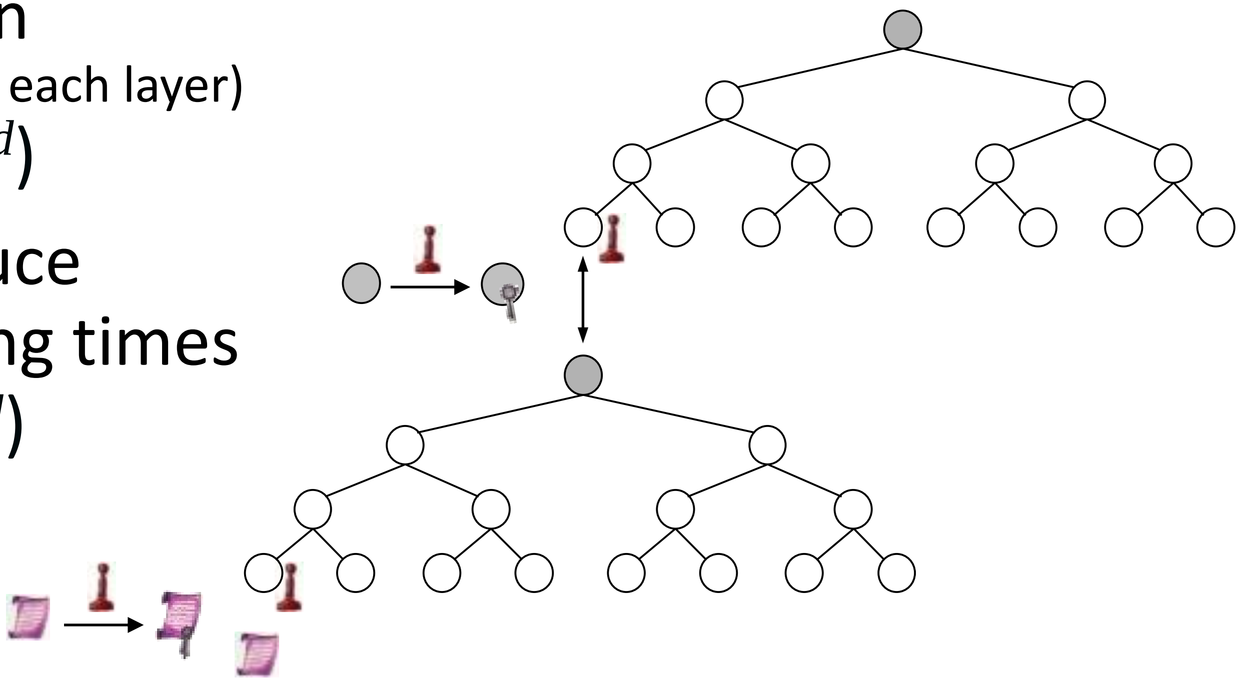


Multi-Tree XMSS

Uses multiple layers of trees

-> Key generation
(= Building first tree on each layer)
$\Theta(2^h) \rightarrow \Theta(d*2^{h/d})$

-> Allows to reduce worst-case signing times
$\Theta(\mathrm{h}/2) \rightarrow \Theta(h/2d)$



Since v01: Multi-target-attack-resilience

Issue:
XMSS with 256bit hash $\nRightarrow$ 256bit security

Reason:

Multi-target-attacks

Solution:

Use different key & bitmask for each hash invocation

Keys & bitmasks must be public!

Solution: PRG + Seed in PK

Security:

- Not really standard model.
- Natural but new assumption („Generating the public values using a PRG, the scheme does not get less secure if seed is published.“),
- Or ROM
- Scientific paper with details and proof out soon

Preview v02

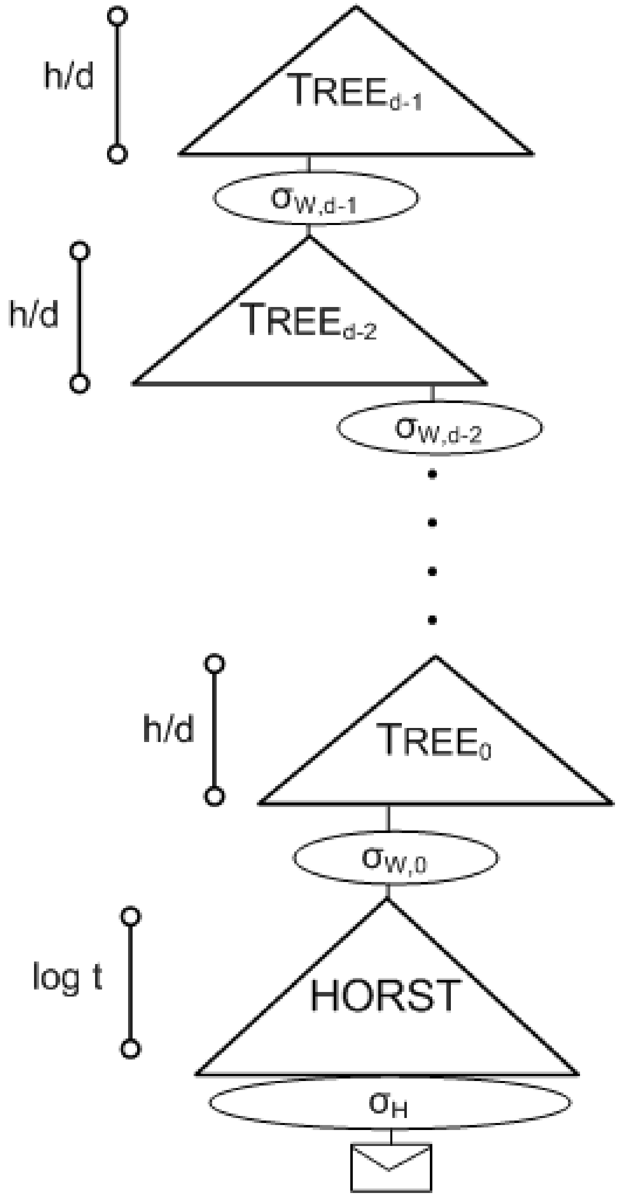
- Improved hash address format
- More precise description (endianess)
- Test vectors
- Public domain code (ref & fast)

SPHINCS: practical stateless hash-based signatures

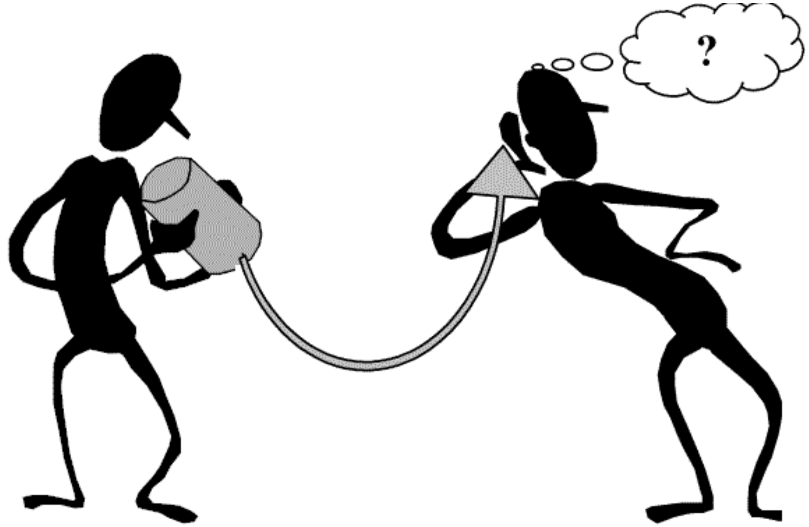
joint work with Daniel J. Bernstein, Daira Hopwood, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, Zooko Wilcox O'Hearn

SPHINCS

- Stateless Scheme
- XMSS^{MT} + HORST + (pseudo-)random index
- Collision-resilient
- Deterministic signing
- SPHINCS-256:
  - 128-bit post-quantum secure
  - Hundrest of signatures / sec
  - 41 kb signature
  - 1 kb keys



Thank you!
Questions?



For references & further literature see
https://huelsing.wordpress.com/hash-based-signature-schemes/literature/