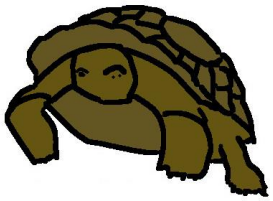
Long-term secure signatures for the IoT

Andreas Hülsing

PQCRYPTO
ICT-645622



Hash-based Signature Schemes

[Mer89]

Long-term secure

- Only needs secure hash function
- Post-quantum
- Possibility of hash combiners

IoT compatible?

- Only needs secure hash function

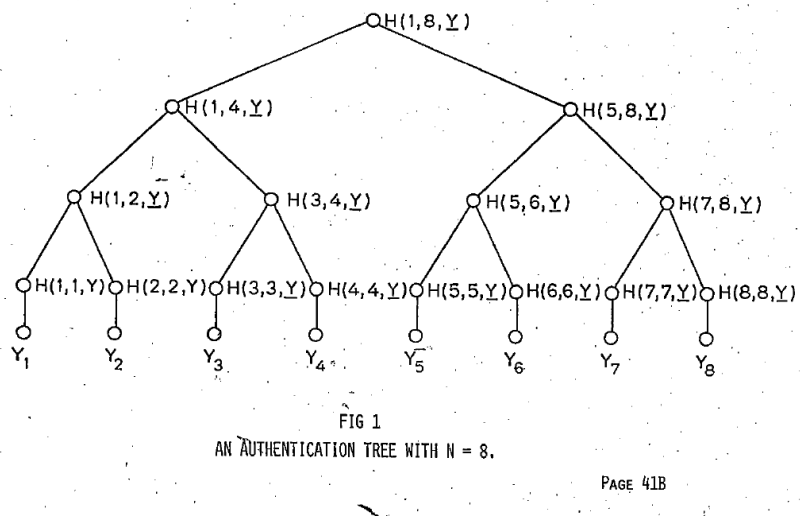
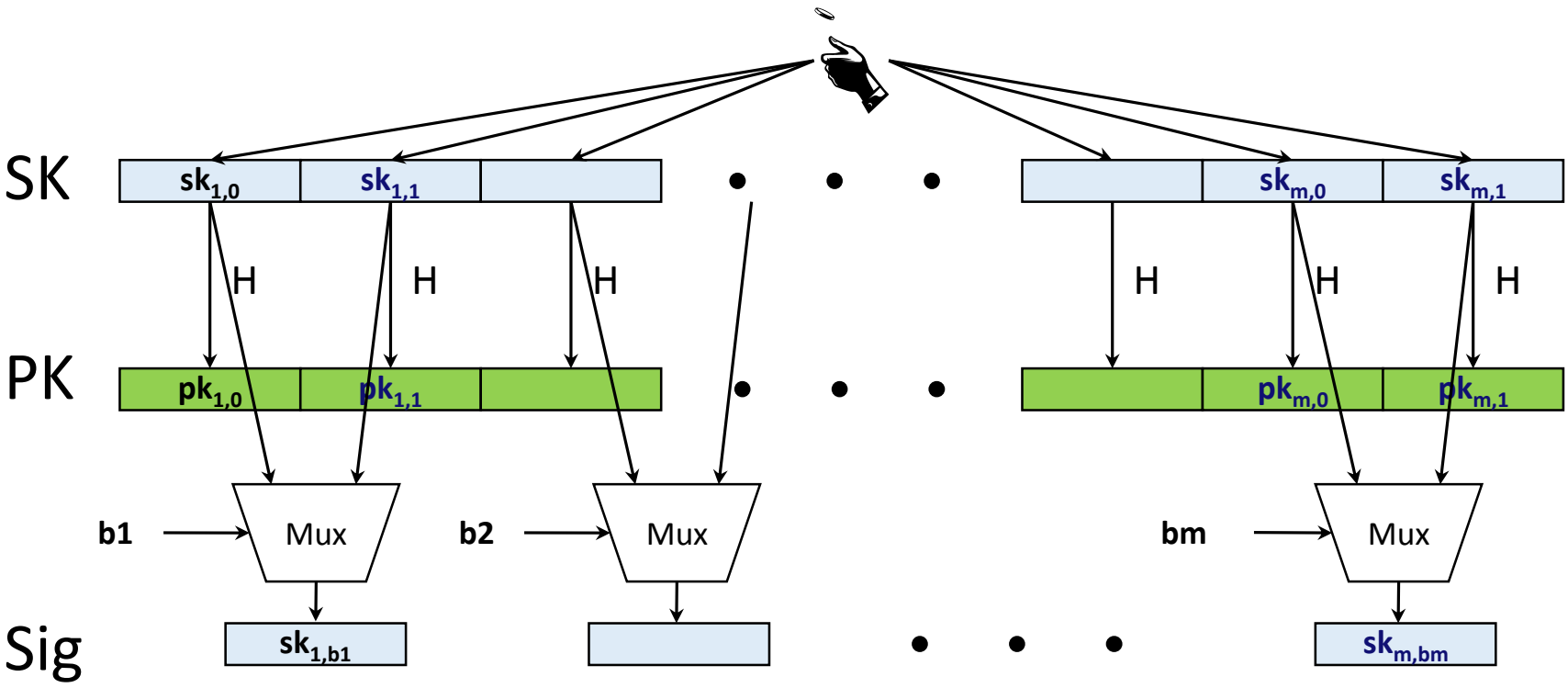


FIG 1
AN AUTHENTICATION TREE WITH N = 8.

PAGE 41B

Lamport-Diffie OTS [Lam79]

Message M = b1,…,bm, OWF H * = n bit



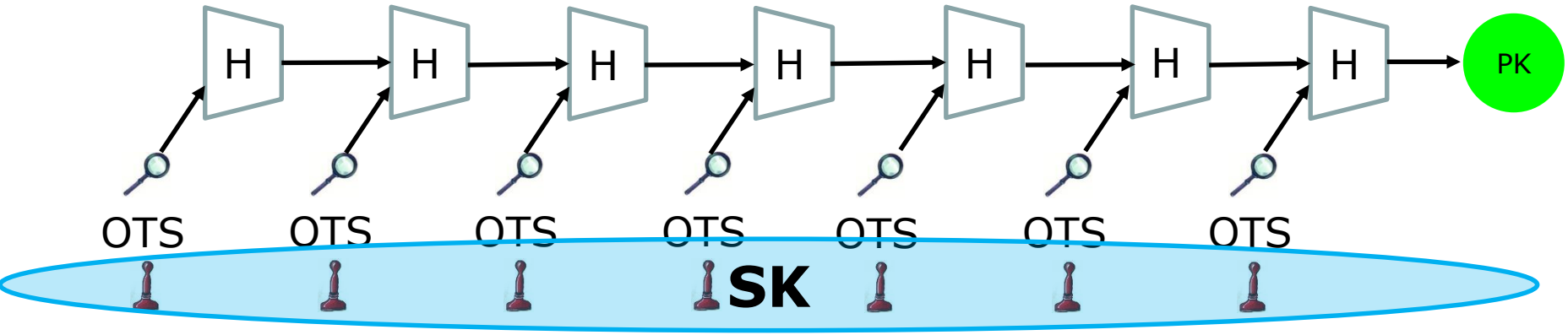
One-time signatures

- Can only be used once
- Basic building block
- Secret keys can be generated pseudorandomly

WOTS^{+} [Hue13]

- Shorter signatures
- Size-speed trade-off

Chain-based OTS

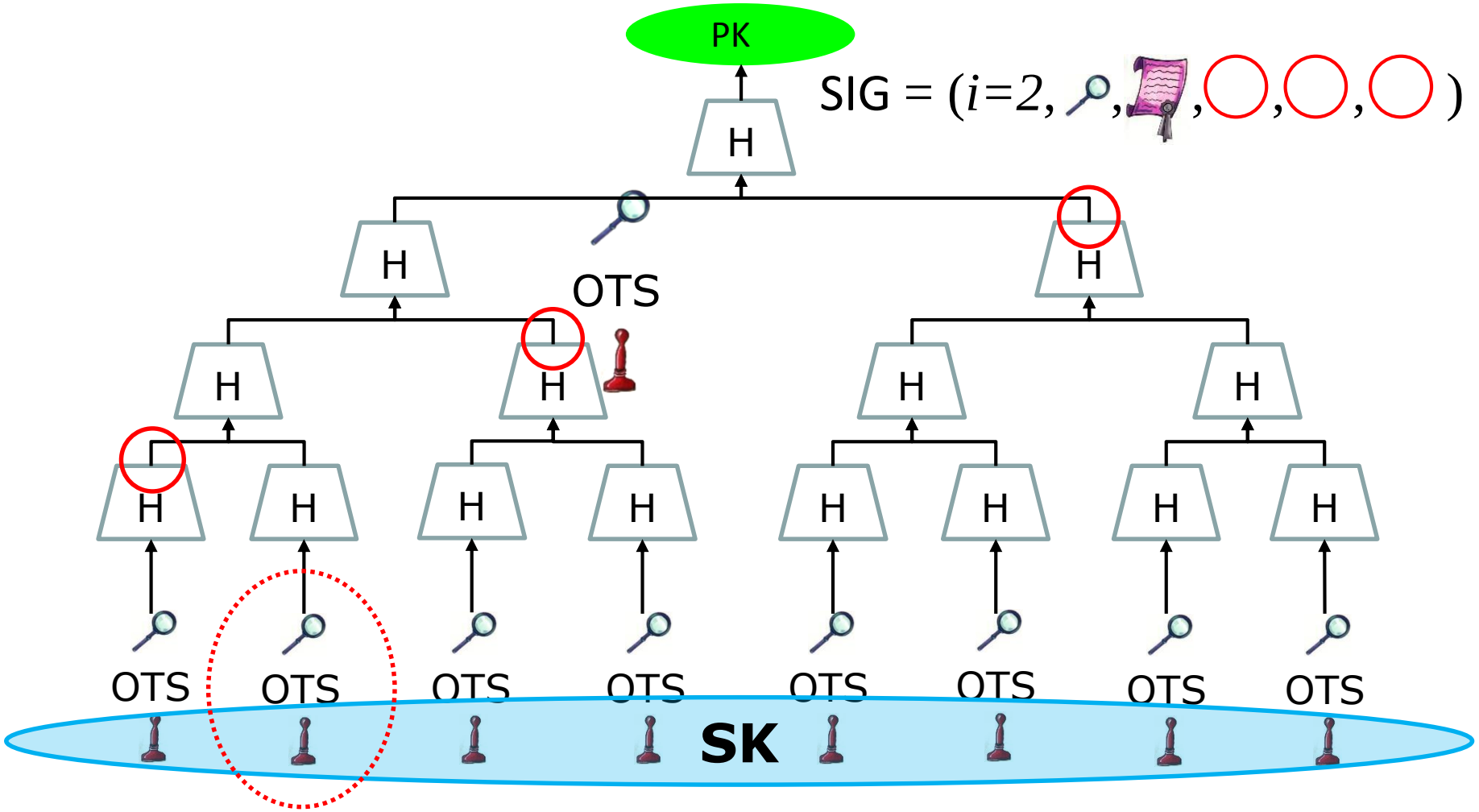


Chain-based OTS [NY89]

- Extremely fast signing via „pebbeling“
- Extremely fast verification of sequential signatures
- Small keys
- Small sigs (for sequential signatures)
- Extremely useful in combination with aggregator
- Stateful

See e.g. Dahmen, Krauss. Short Hash-Based Signatures for Wireless Sensor Networks. CANS 2009.

Merkle's signature scheme



Merkle‘s signature scheme

- Fast signing via „tree traversal algorithms“
- Extremely fast verification
- Small keys
- Medium size sigs
- Stateful

Latest: XMSS-T

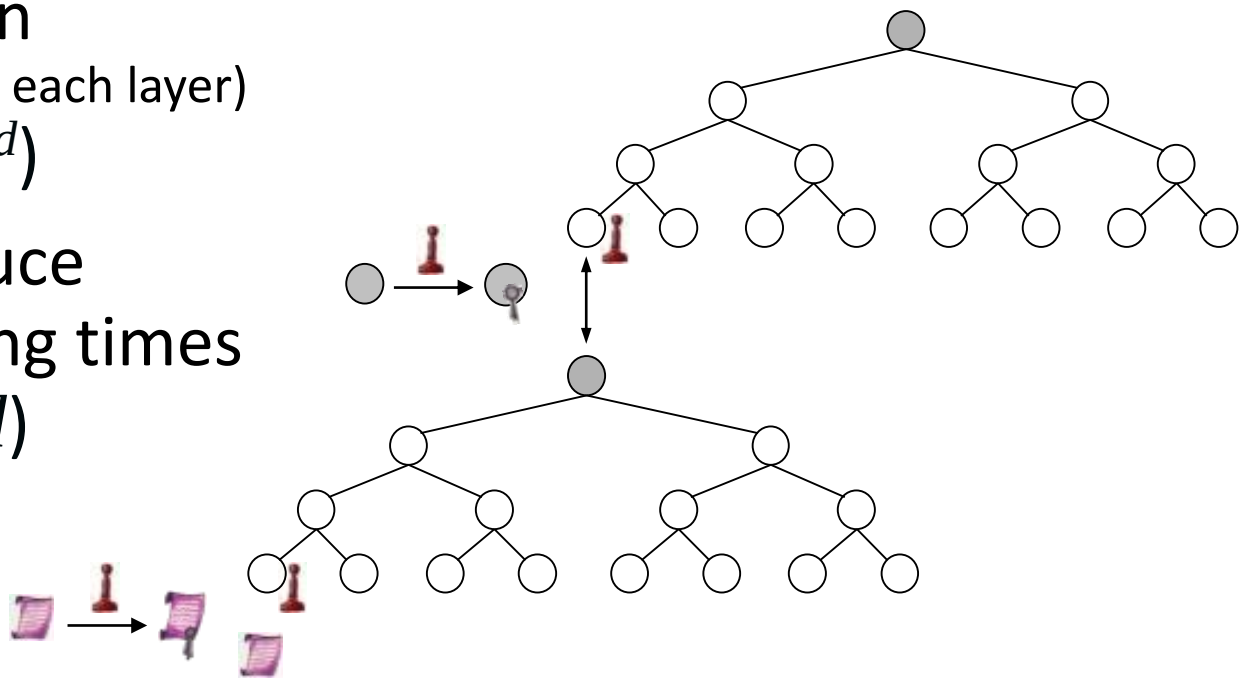
(Hülsing, Rijneveld, Song. Mitigating Multi-Target Attacks in Hash-based Signatures. PKC ‘16)

Multi-Tree XMSS [MMM02]

Uses multiple layers of trees

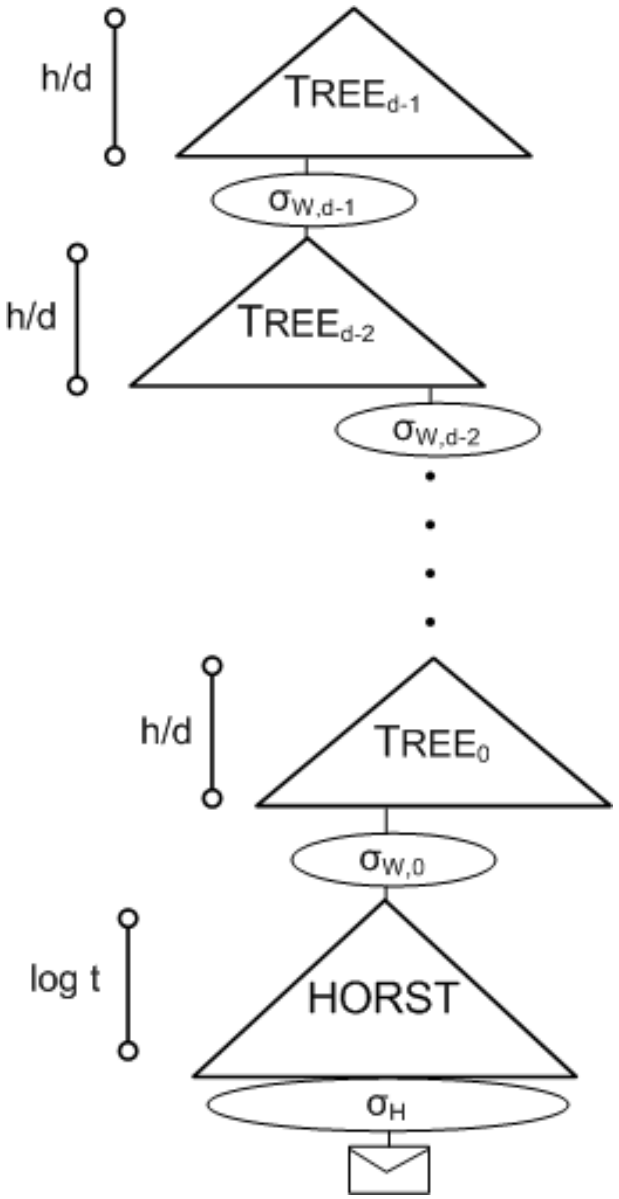
-> Key generation
(= Building first tree on each layer)
$\Theta(2^h) \rightarrow \Theta(d*2^{h/d})$

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



SPHINCS [BHH+15]

- 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



Performance on small devices

- STM32L100C development board: Cortex M3, 32MHz, 32-bit architecture, 256KB Flash, 16KB RAM

	KeyGen	Sign	Verify
XMSS^{MT}	278.80s	0.61s	0.16s
SPHINCS	0.88s	18.41s	0.51s

- Issue: SPHINCS sigs (41KB) don‘t fit single APDU

Future

- XMSS Internet Draft in IRSG poll
- At least two SPHINCS submissions for NIST
  - Faster / smaller signatures
- Several works on dedicated hash functions (Haraka, Siempira)

Thank you!
Questions?