Call for fast short-input hash functions

A. Hülsing
Hash-based signatures

• Post-quantum signature schemes
• Security only relies on security of hash function
• Most confidence inspiring candidate right now
• Stateful (XMSS) & stateless (SPHINCS)
Stateful (XMSS)

• Fast
• Not to big (Sig: 2-3 kB, PK: 512 bit)
• Internet Drafts currently in last call
  • See https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/
  • Comment!

• Stateful...
Stateless (SPHINCS)

@128 bit post-quantum security

• 10ms per sig (optimized)
• 41 kB signatures
• Ok, but could be better!
Costs for SPHINCS (XMSS similar)

- Uses hash functions
  - $F: \{0,1\}^n \rightarrow \{0,1\}^n$
  - $H: \{0,1\}^{2n} \rightarrow \{0,1\}^n$
  - Only (second-) preimage resistance needed, no collision resistance!

For one signature:

- **451456** calls to $F$
- **91251** calls to $H$

All other operations are negligible.
We call for fast F and H

• Speed-up for SPHINCS (and XMSS)
• Trade-offs allow to use improved speed to reduce signature size

• First proposal in SPHINCS paper:
  • SPHINCS F and H: Sponge using ChaCha permutation
• Further proposals needed
• Cryptanalysis needed
Thank you!
Questions?