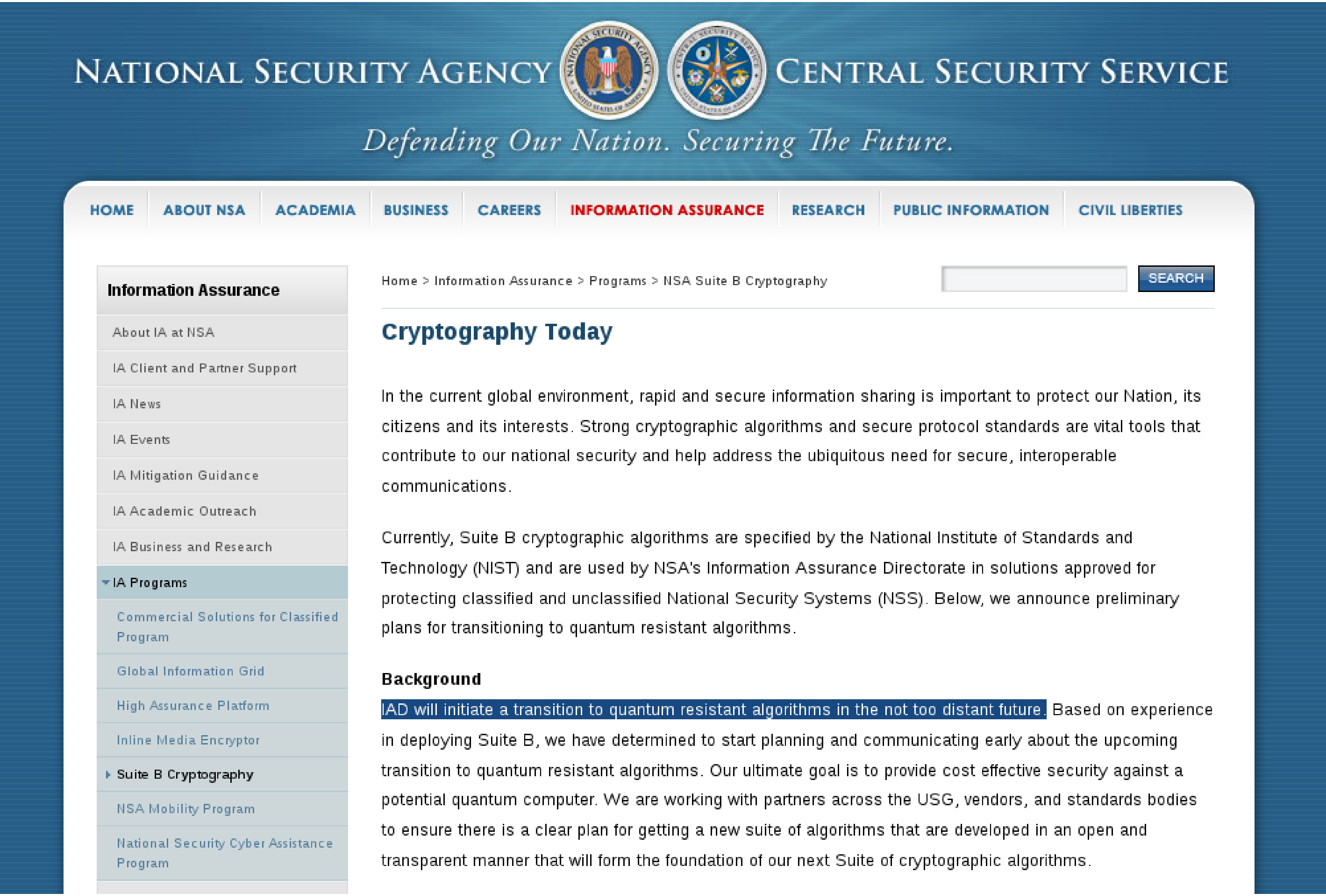
Hash-based Signatures@CFRG

Andreas Hülsing



Home > Information Assurance > Programs > NSA Suite B Cryptography

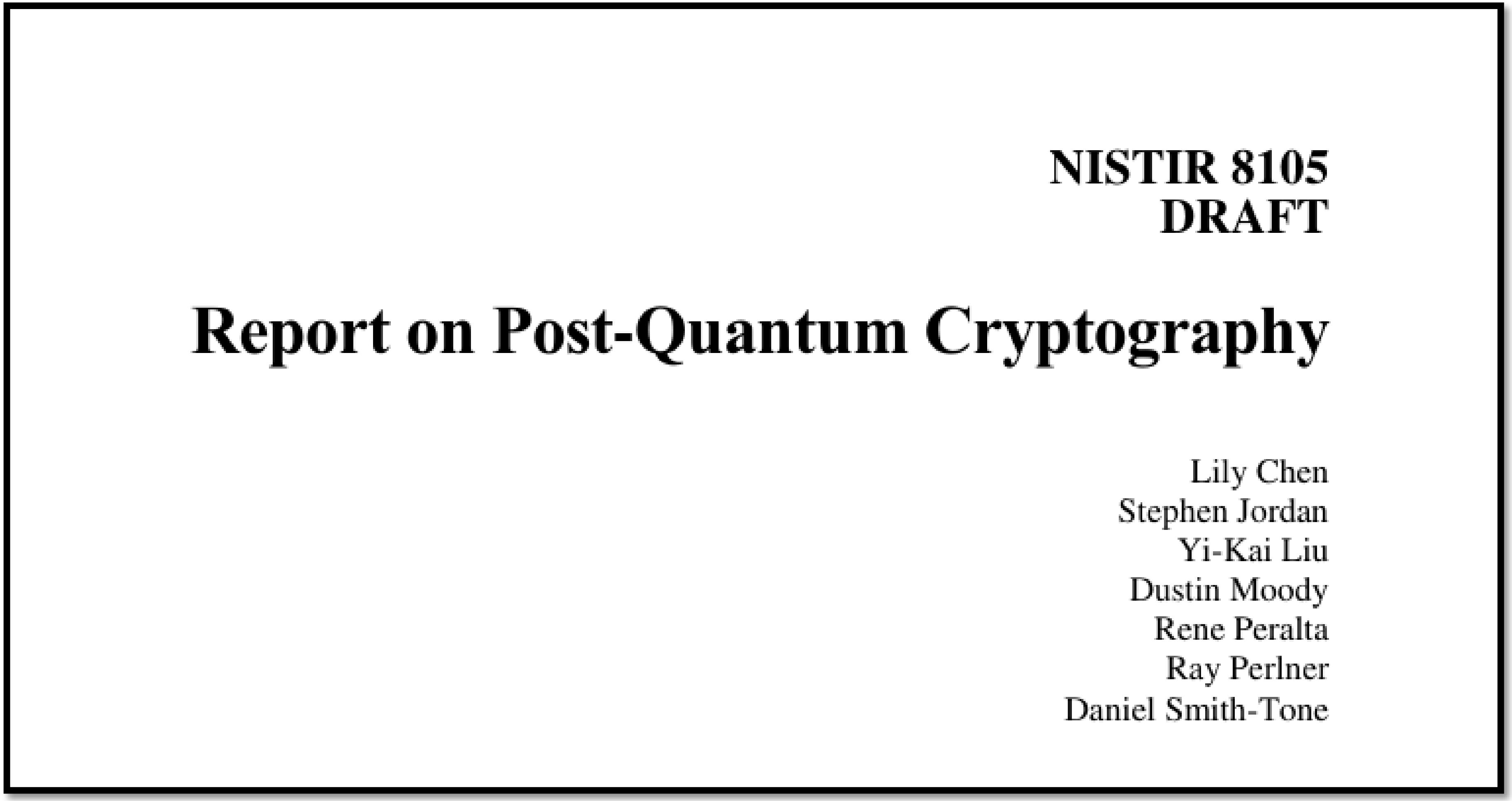
Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

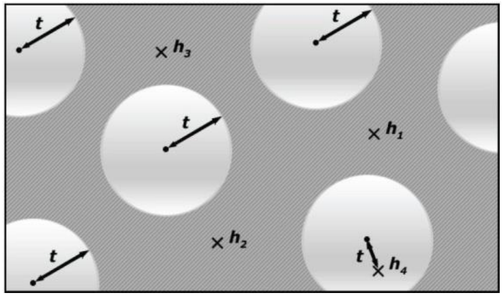


NISTIR 8105
DRAFT

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

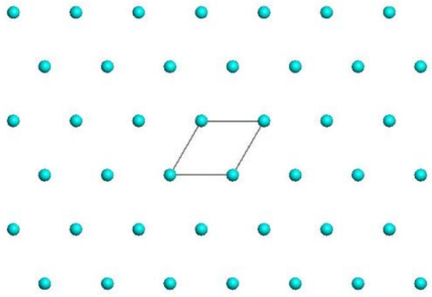
Trapdoor- / Identification Scheme-based (PQ-)Signatures



Lattice, MQ, Coding

- Signature and/or key sizes
- Runtimes
- Quantum 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

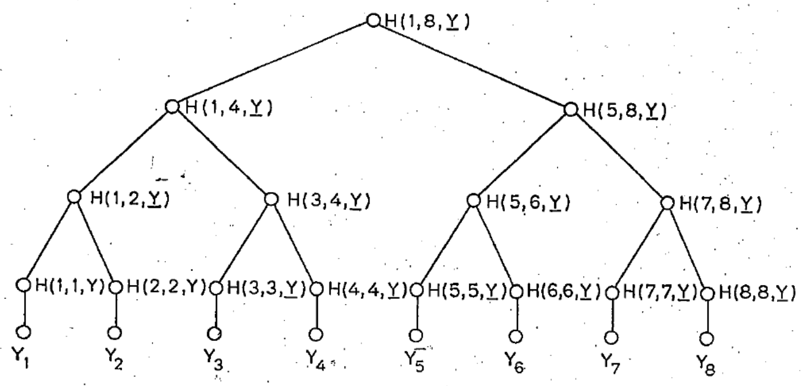
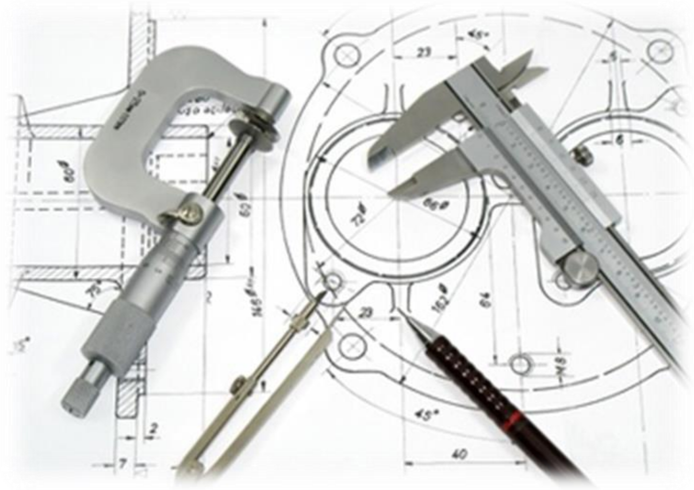


FIG 1

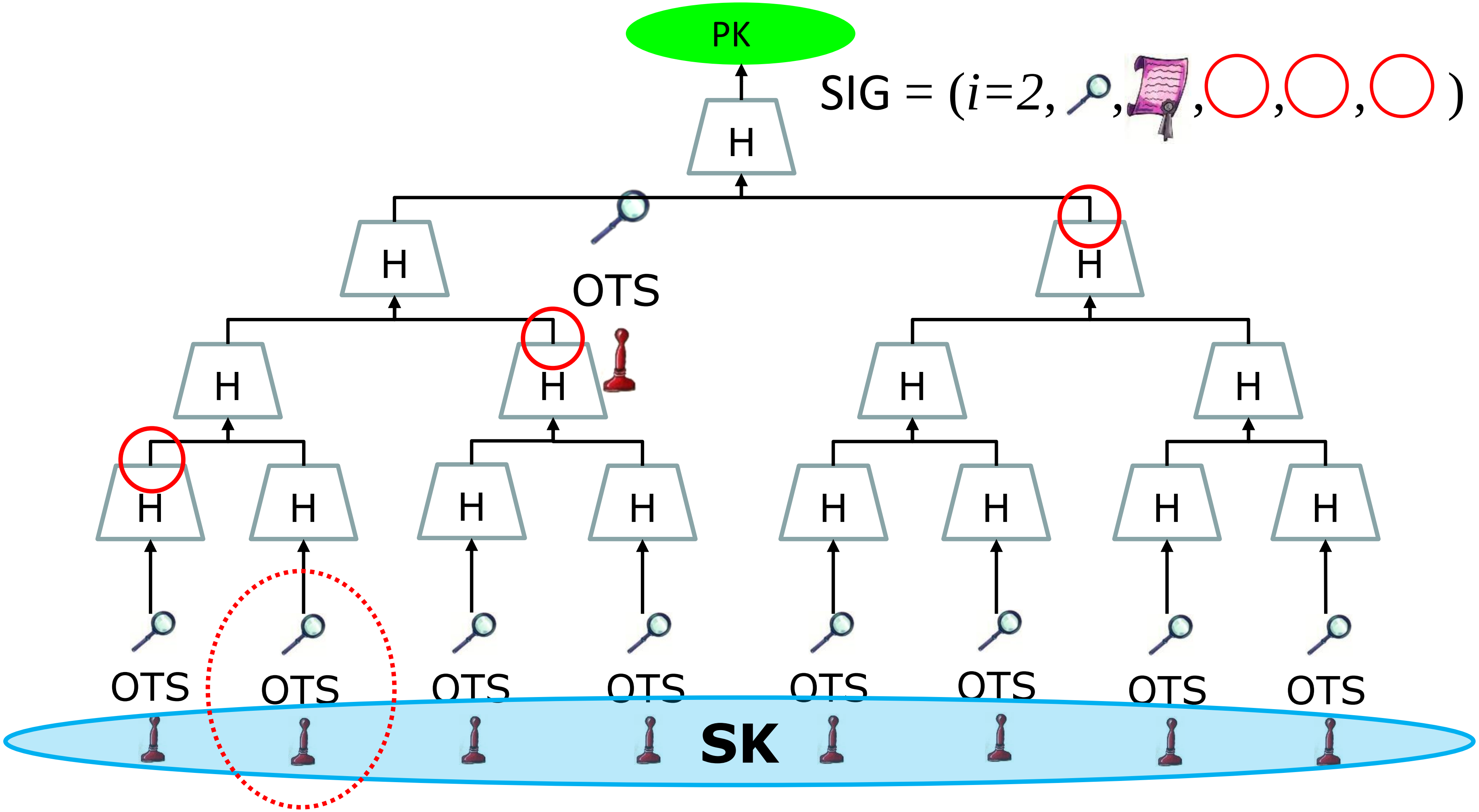
AN AUTHENTICATION TREE WITH N = 8.

PAGE 41B

Basic Construction



Merkle’s Hash-based Signatures



Situation at CFRG

Two drafts

1. **Hash-Based Signatures**
   draft-mcgrew-hash-sigs-03
   (Cisco)
2. **XMSS: Extended Hash-Based Signatures**
   draft-irtf-cfrg-xmss-hash-based-signatures-02
   (our draft)

Similarities

- Stateful schemes
- Multi-Layer support (virtually unlimited signatures)
- Internally using SHA2
- All hash calls randomized to mitigate multi-target attacks

Cisco Draft

- Based on Leighton-Micali construction

- Security entirely in random oracle model (heuristic)
  - Can easily lead to wrong security estimates
  - E.g. $H(R||M)$ vs. $H(M||R)$

XMSS Draft

- Based on XMSS
- Security of core construction in standard model
    - No heuristics
- Random oracle model for short public key
    - Replacing public data in PK with seed for PRG makes security only provable in ROM
- Accompanying paper with security proof and security analysis for quantum attacks

Resources for XMSS-Draft

Already available:

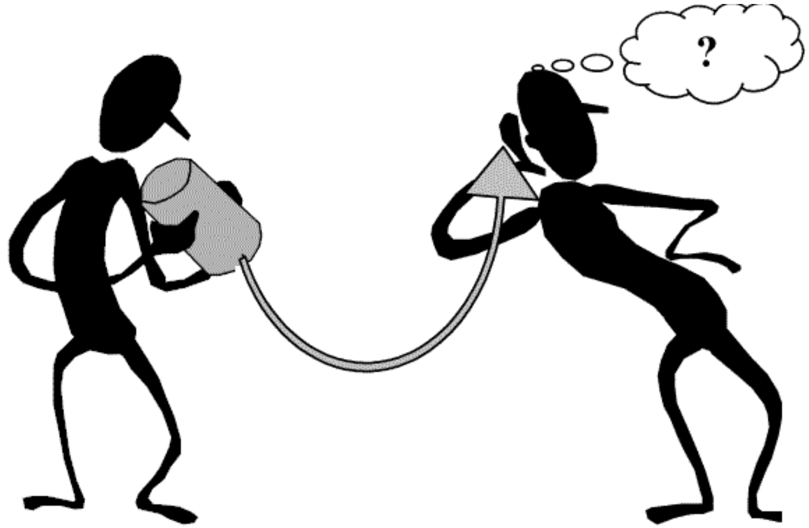
- Draft-v02
- Reference & fast implementation for v01 (only min. Differences for v02)
- Paper: „Mitigating Multi-Target Attacks in Hash-based Signatures.”

Coming soon:

- Draft-v03 (new address structure, updated security argument, new message compression)
- Reference & fast implementation for v03

(see http://huelsing.net)

Thank you!
Questions?



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