XMSS: Extended Hash-Based Signatures

(draft-irtf-cfrg-xmss-hash-based-signatures)

A. Hülsing, D. Butin, S.-L. Gazdag, A. Mohaisen

Hash-based Signature Schemes

[Mer89]

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

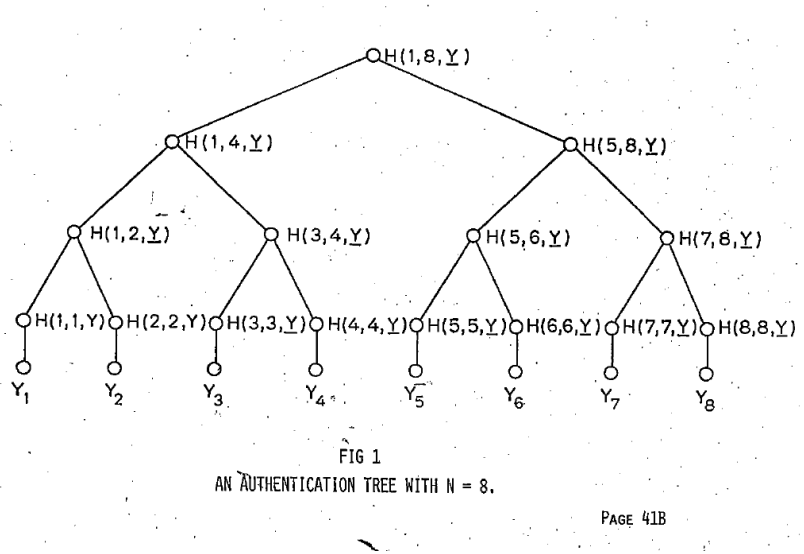
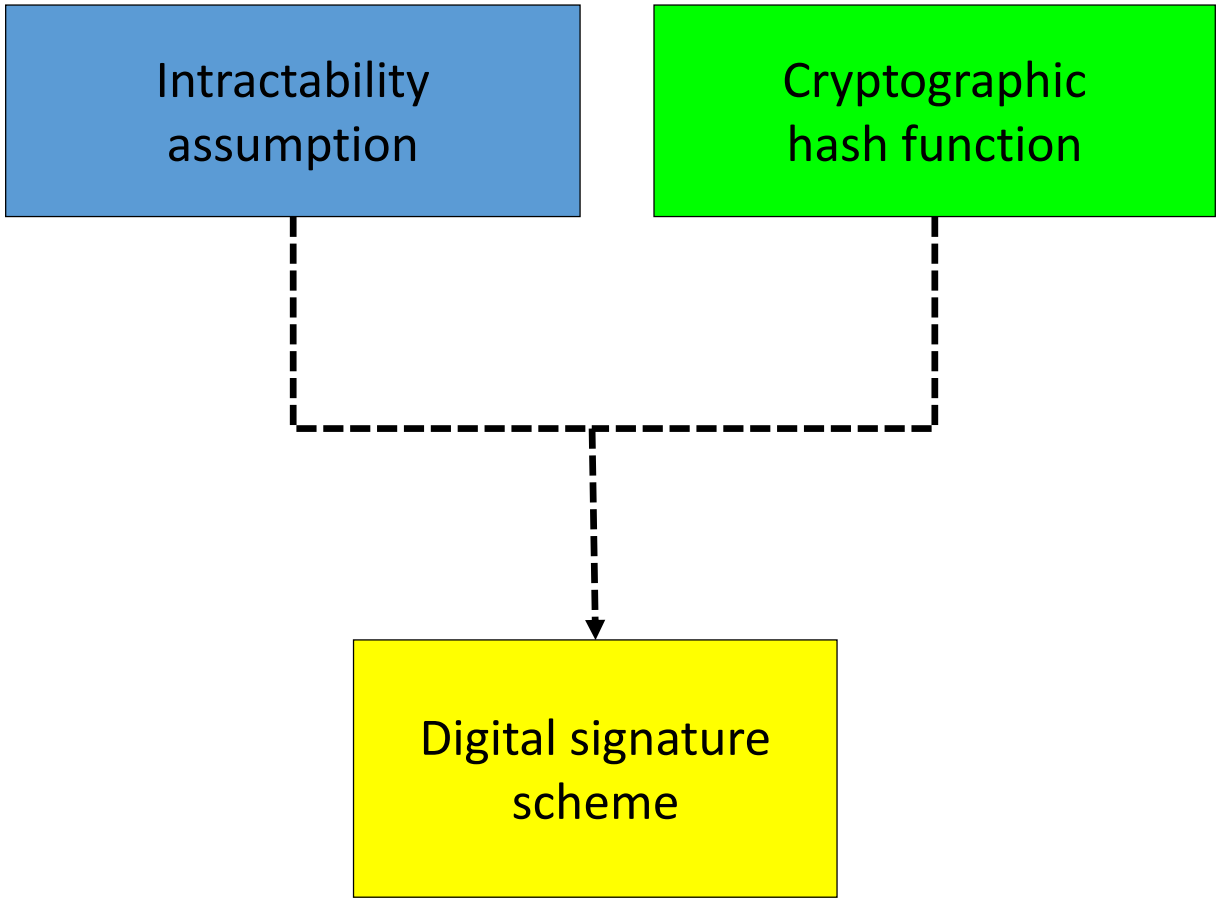


FIG 1

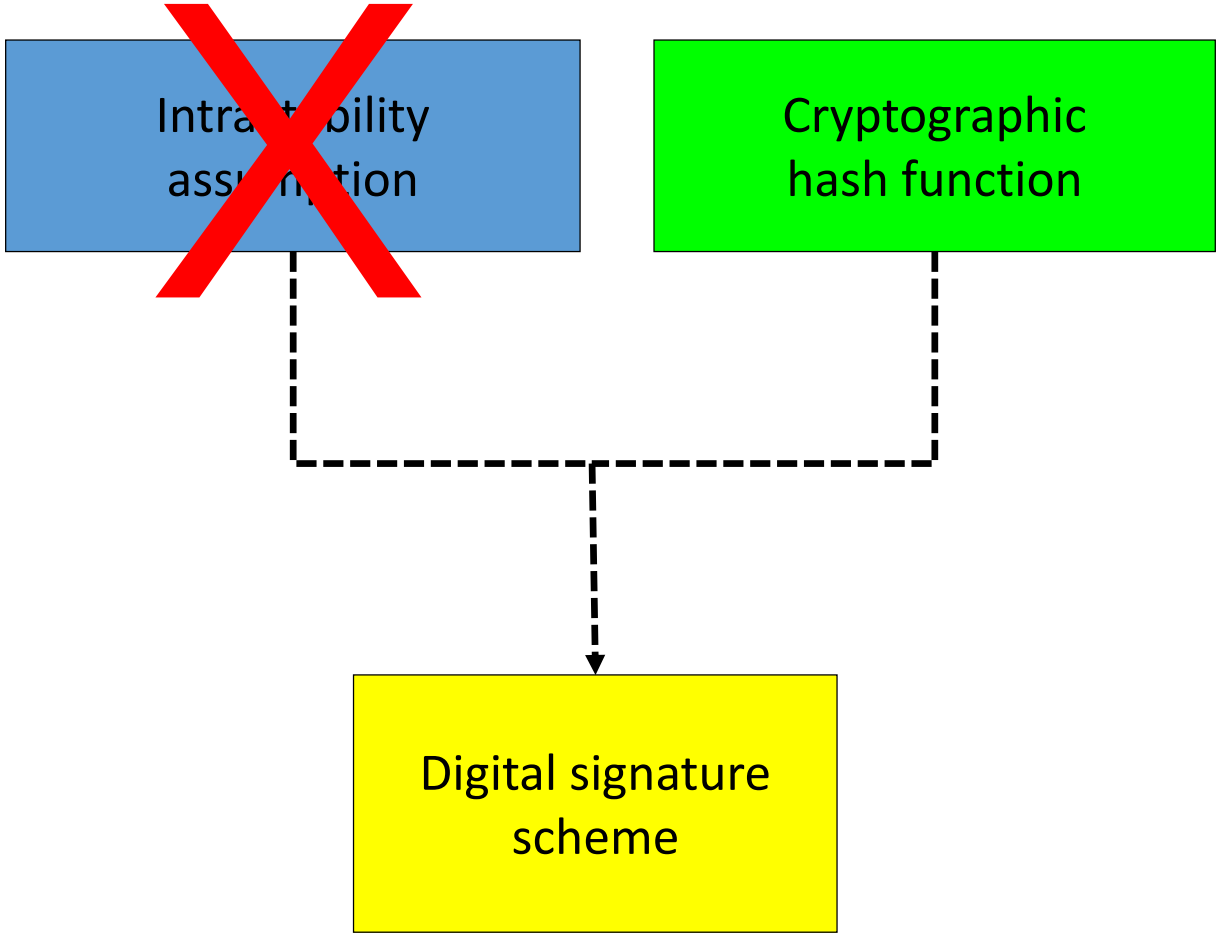
AN AUTHENTICATION TREE WITH N = 8.

PAGE 41B

Security


Intractability assumption
Cryptographic hash function
Digital signature scheme

Security


Intra bility
ass tion
Cryptographic
hash function
Digital signature
scheme

Post-Quantum Security

n-bit hash function

Grover‘96:

Preimage finding $\boldsymbol{O(2^n)} \rightarrow \boldsymbol{O(2^{\frac{n}{2}})}$

Brassard et al. 1998:

Collision finding $\boldsymbol{O(2^{\frac{n}{2}})} \rightarrow \boldsymbol{O(2^{\frac{n}{3}})}$

Aaronson & Shi’04:

Quantum collision finding $\boldsymbol{2^{\frac{n}{3}}}$ is lower bound

Advanced Applications

- Forward Secure Signatures
  - Security of old signatures after key compromise

- Delegatable / Proxy Signatures
  - Securely delegate signing rights

→ Require specific pseudorandom key gen

Design Choices

- Follow literature as close as possible
- Full collision-resilience
- Classical and post-quantum secure parameters
- Prepared for stateless schemes (SPHINCS)

Schemes in the Draft

- Winternitz One Time Signature ($WOTS^{+}$)
- Extended Merkle (tree) signature scheme (XMSS)
- Multi-tree XMSS (XMSS^MT)

Conclusion

- Draft is out

  https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/

We want your feedback!