genua A Bundesdruckerei Company

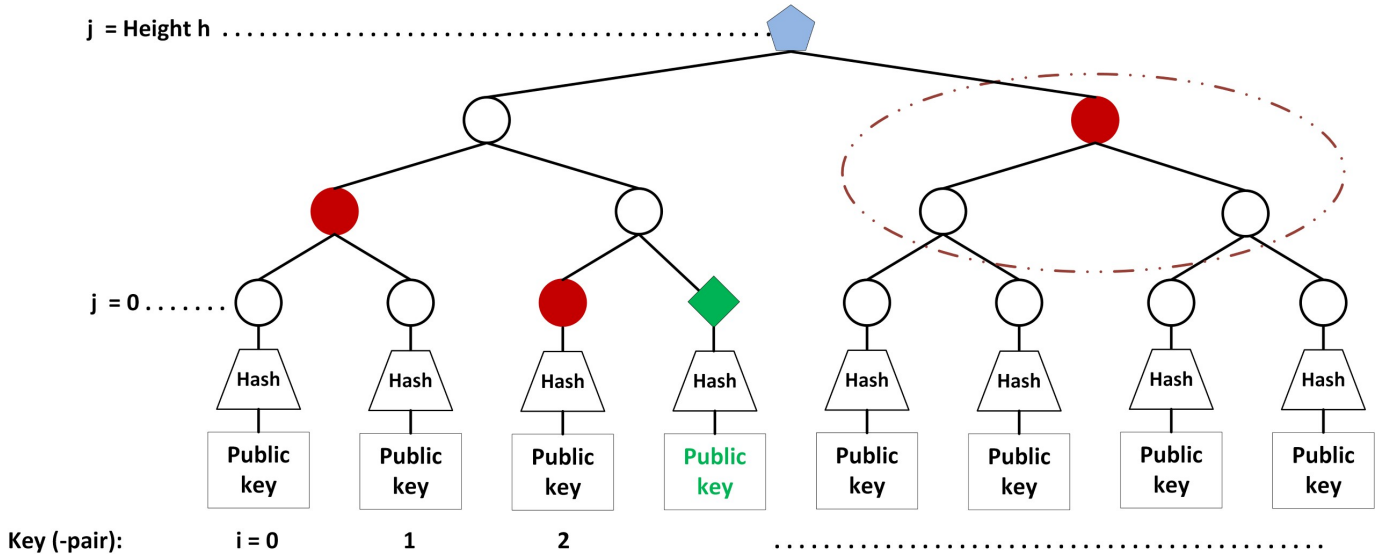
Hash-based Signatures in Practice

Starting the transition to post-quantum cryptography

Stefan-Lukas Gazdag
PQCrypto – 2017-06-26

Hash-based Signatures

- Well understood
- Post-quantum
- All we need: secure cryptographic hash function

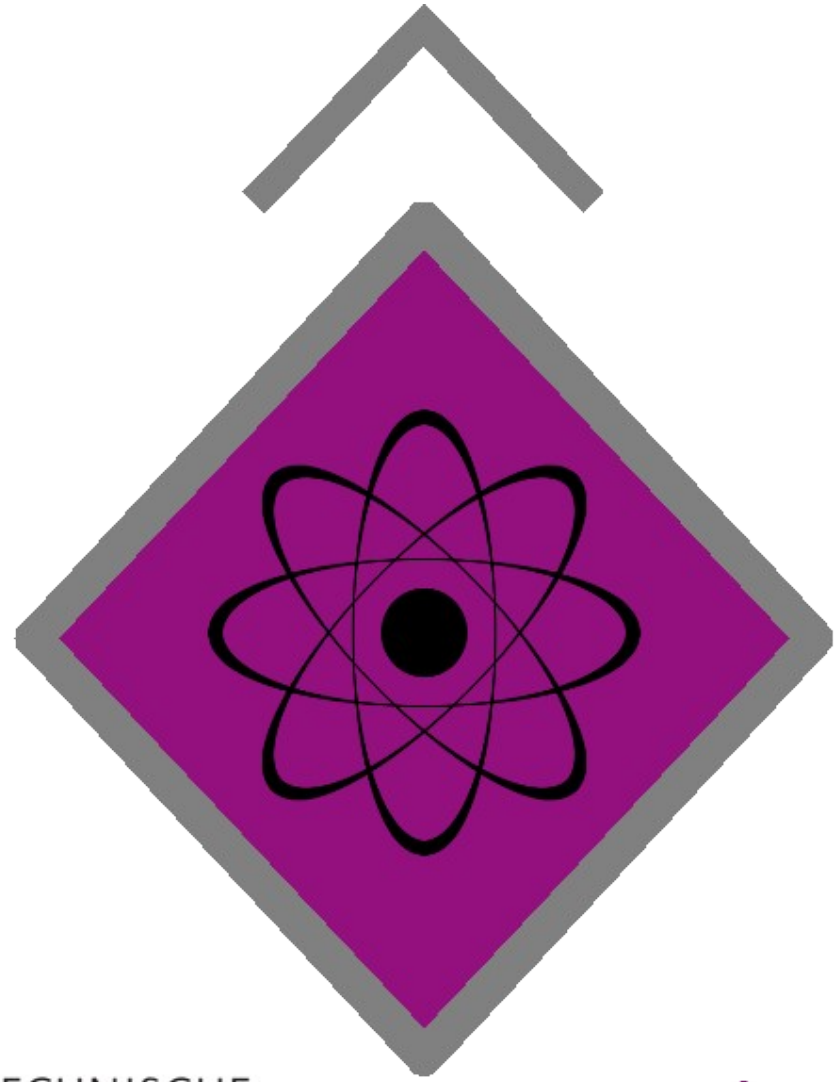


Hash-based Signatures

genua A Bundesdruckerei Company

- Well understood
- Post-quantum
- All we need: secure cryptographic hash function

But: peculiarities like statefulness
(private key has to be updated)



TECHNISCHE UNIVERSITÄT DARMSTADT

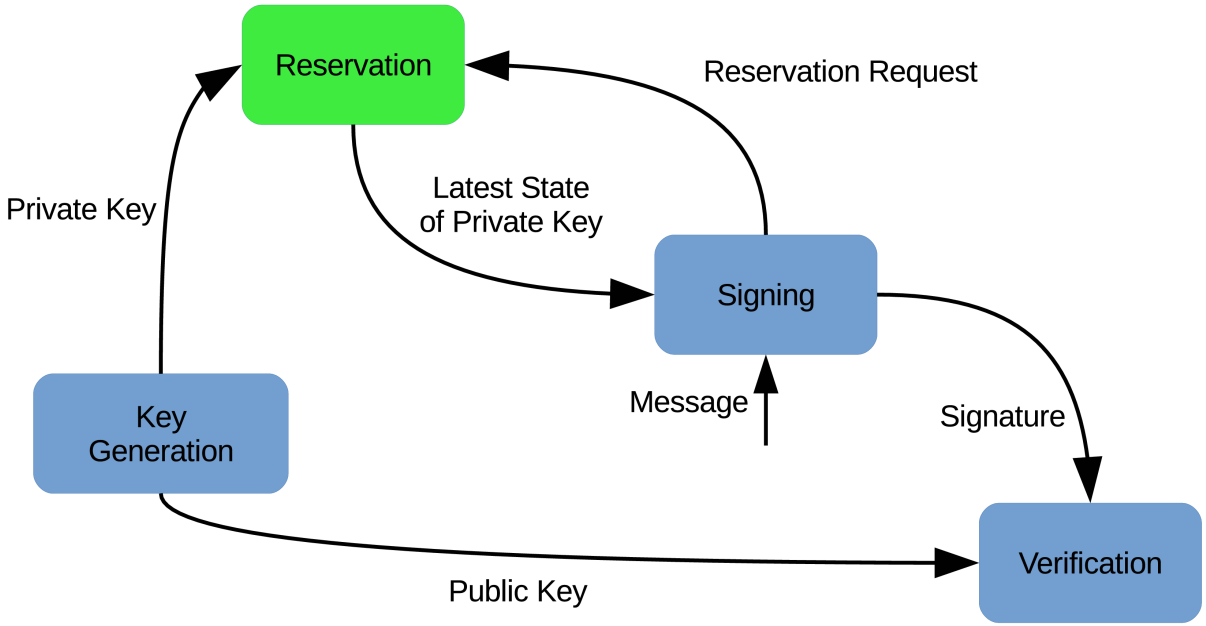
genua A Bundesdruckerei Company

genua A Bundesdruckerei Company

McGrew et al.:

State Management for Hash-Based Signatures

http://eprint.iacr.org/2016/357



Standardization

genua A Bundesdruckerei Company

Crypto Forum Research Group
Internet-Draft
Intended status: Informational
Expires: September 6, 2017

D. McGrew
M. Curcio
S. Fluhrer
Cisco Systems
March 5, 2017

Hash-Based Signatures
draft-mcgrew-hash-sigs-06

Abstract

This note describes a digital signature system based on cryptographic hash functions, following the seminal work in this area of Lamport, Diffie, Winternitz, and Merkle, as adapted by Leighton and Micali in 1995. It specifies a one-time signature scheme and a general signature scheme. These systems provide asymmetric authentication without using large integer mathematics and can achieve a high security level. They are suitable for compact implementations, are relatively simple to implement, and naturally resist side-channel attacks. Unlike most other signature systems, hash-based signatures would still be secure even if it proves feasible for an attacker to build a quantum computer.

Standardization

genua A Bundesdruckerei Company

Crypto Forum Research Group
Internet-Draft
Intended status: Informational
Expires: October 1, 2017

A. Huelsing
TU Eindhoven
D. Butin
TU Darmstadt
S. Gazdag
genua GmbH
A. Mohaisen
SUNY Buffalo

March 30, 2017

XMSS: Extended Hash-Based Signatures
draft-irtf-cfrg-xmss-hash-based-signatures-09

Abstract

This note describes the eXtended Merkle Signature Scheme (XMSS), a hash-based digital signature system. It follows existing descriptions in scientific literature. The note specifies the WOTS+ one-time signature scheme, a single-tree (XMSS) and a multi-tree variant (XMSS^MT) of XMSS. Both variants use WOTS+ as a main building block. XMSS provides cryptographic digital signatures without relying on the conjectured hardness of mathematical problems. Instead, it is proven that it only relies on the properties of cryptographic hash functions. XMSS provides strong security guarantees and is even secure when the collision resistance of the underlying hash function is broken. It is suitable for compact implementations, relatively simple to implement, and naturally resists side-channel attacks. Unlike most other signature systems, hash-based signatures can withstand attacks using quantum computers.

Conclusion

- First official standards available soon
- Safe deployment / good performance feasible for some use cases NOW!
- First genua products featuring post-quantum update signatures available by the end of this year

- First official standards available soon
- Safe deployment / good performance feasible for some use cases NOW!
- First genua products featuring post-quantum update signatures available by the end of this year

Start the transition now!

www.square-up.org

stefan-lukas_gazdag@genua.de