Research announcement: Practical Hash-based Signatures

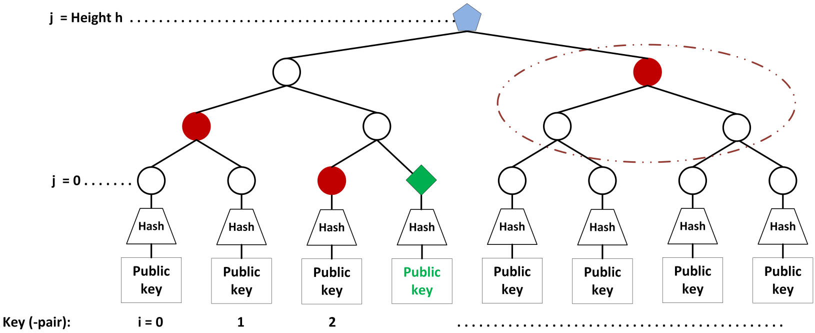
Stefan Gazdag, Andreas Hülsing, Denis Butin & Johannes Buchmann

genua

TU/e

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Hash-based signatures



- Complete binary tree structure, cryptographic hash function + one-time signature scheme (in practice: variant of Winternitz one-time signature)
- Initial scheme: Merkle, many improvements since
- Advanced variants (e.g. XMSS): multi-tree; second preimage resistance requirement instead of collision resistance; PRG one-time signature key generation; forward security

Advantages

- Minimal security requirements (only requires secure hash, no intractability assumption)
- Increasingly efficient
- Flexible — parameters allowing trade-offs (notably tree height and Winternitz parameter)
- Possible to instantiate with any secure cryptographic hash function

What is missing?

Well-understood theoretically, but obstacles to practical use:

- Internet-Draft for basic scheme exists (McGrew & Curcio 2014), but:
- . . . Need standard for advanced variants (multi-tree, collision-resistance not required) to take advantage of improved performance and security properties
- . . . Practical issues not tackled yet, e.g. statefulness (need to keep track of key index, consequences for simultaneous access / high frequency signing)
- . . . Side-channel security unknown

A plan to foster practical use

- Need advanced standard including:
  - Multi-tree: providing sufficient number of keys for practical applications
  - Collision resistance requirement replaced by second preimage resistance requirement: allows hash with smaller output, improved security
- Investigate consequences of statefulness, notably for public key infrastructures

A plan to foster practical use

- Test implementation in an industrial environment (software update authentication use case) using crypto libraries (e.g. OpenSSL, Bouncy Castle)
- Integrate with common protocols (TLS, SSH, S/MIME. . .); integrate along with post-quantum key exchange in cipher suite
- Investigate side-channel resistance (using provable security approach)
- Optimal parameter selection strategy and recommendations required, following initial work on XMSS