genua A Bundesdruckerei Company

Hash-Based Signatures in Practice

Stefan-Lukas Gazdag

ETSI / IQC Quantum-Safe Cryptography Workshop

15th of September 2017

genua A Bundesdruckerei Company

- Adequate performance
- Practical sizes
- Proper state management

  https://eprint.iacr.org/2016/357
- Suitable life time of the key
- Trustability and security NOW

- **Stateful** vs. stateless private key
  (LMS / XMSS vs. SPHINCS)
- State management may add to runtime
- Access restricted
  => critical resource
  => parallelisation somewhat complex
- Writing key to disk may be problematic
- Copies of the private key may reveal old state

How about hash-based signatures for TLS?

genua A Bundesdruckerei Company

- Con:
  - Typically parallel processes in use
  - High signing frequency possible
  - Non-trivial key distribution and revocation
  - Virtual machines
- Pro:
  - HBS do fit common certificate standards

    Does work in test environments, but not that well for real-world use.

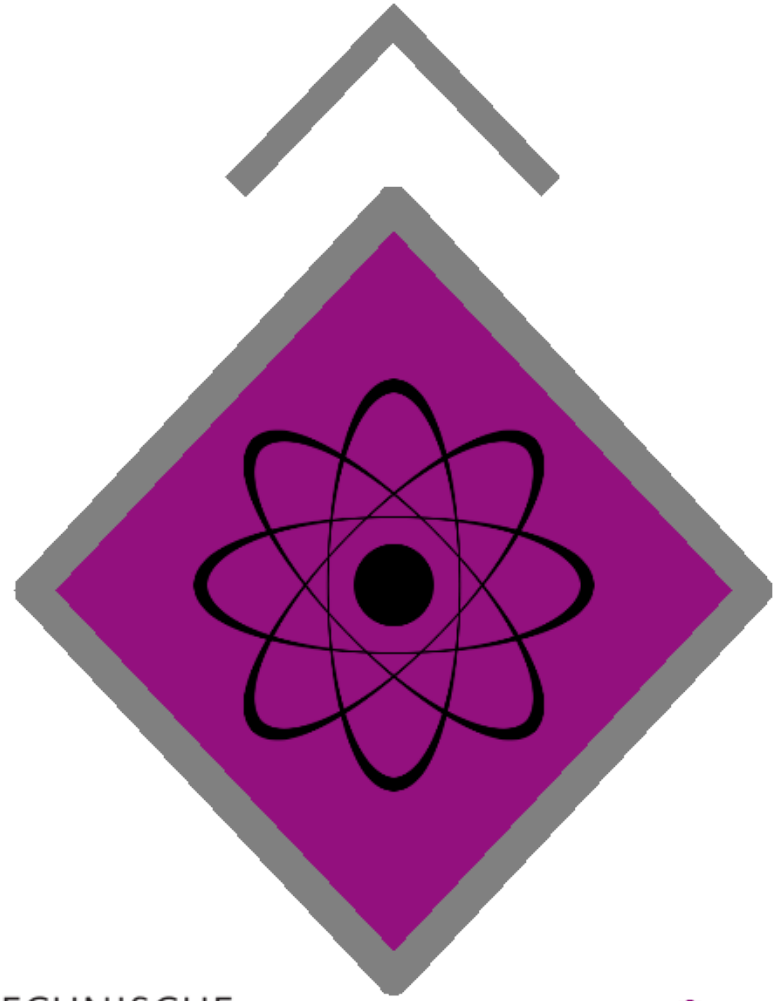
- SSH setting different to TLS
  - Different key distribution
  - Lower signing frequency

Remember: Key has to be stored in a save environment, e.g. on a smart card

- Key distribution similarly possible to status quo
- Current protocols / data structures may be extended
- User experience stays the same

Again: laptop / computer using smart card

Real-world example: update signatures



TECHNISCHE UNIVERSITÄT DARMSTADT

genua A Bundesdruckerei Company

www.square-up.org

genua A Bundesdruckerei Company

- Build server asks for signature(s)
- Key server handles the request
- Build server releases package
- Products can install new firmware / software after verifying signature

Goal:
Products in the field can install new software in post-quantum setting!

- Dedicated key server

  => smart card or hardware security module
- Restricted environment
- Manageable number of signatures per day
- Acceptable timing restrictions (more or less)
- Acceptable size restrictions (more or less)
- Introducing new key fairly easy
- „Hybrid“ signature release

genua A Bundesdruckerei Company

- Current situation:
  - XMSS
  - OpenSSH
  - First products (firewall systems) with post-quantum updates by the end of this year.

genua A Bundesdruckerei Company

Other use cases?

Other use cases

genua A Bundesdruckerei Company

- Verified Boot
- Attribute-based authentication

Questions?

stefan-lukas_gazdag@genua.eu