XMSS:
Extended Hash-Based Signatures:
Update and further steps

draft-irtf-cfrg-xmss-hash-based-signatures-01

Andreas Huelsing
Denis Butin
Stefan-Lukas Gazdag
Aziz Mohaisen

Major improvements

- **Added keying of hash functions** with pseudorandomly generated keys for all hashes but the message hash. For that a Hash Function Address Scheme was introduced.

  This was done to prevent multi-target attacks:

  - Considering the old scheme an attacker was able to perform a forgery when finding a preimage for one of the hash values over all signatures.

Major improvements

- Keying of hash functions (cont'd):
  - Eash hash function call now depends on the “position” in the tree. So for each call different keys and bitmasks are used.
  - Proof is in the standard-model, but pseudorandom generation of keys, which is secure in ROM.

Major improvements

- **Replaced bitmasks by pseudorandomly generated values** (only seed stored in public key). As mentioned, security proven in ROM for this part, not in the standard-model.
- **Removed zero bitmasks**, as we now only store a small seed (n bytes) for bitmask generation in the XMSS public key, which is pretty small compared to the bitmask solution before.

  Example for XMSS_SHA2-256_M32_W16_H10:

  OID + 64 bytes (now) vs. OID + 1120 bytes (previously)

Parameters

- **Removed w = 4 and w = 8** to reduce huge number of parameter sets. Simplified algorithms (like base_w) as we don’t need to support the w = 8 case now. Only kept w = 16 due to best performance / signature size trade-off.
- **Removed AES-based parameter sets**.
- **Replaced SHA-3 by SHA-2** (and ChaCha20 – RFC 7539) in light of more widespread usage and faster implementations for SHA-2
- **Adapted construction** accordingly, e.g. keyed mode for SHA-2, which doesn't offer that mode itself.

Minor changes / “Esthetic surgery”

- Removed the OID in the XMSS and XMSS^MT signatures. This was redundant, since the OID is already part of the public key in both cases.
- Adapted XDR formats according to the changes.
- Removed definitions like max() from notation, when no longer needed in this document.
- Changed ’l’ to ’len, ’l_1’ to ’len_1’ and ’l_2’ to ’len_2’ to avoid confusion between the characters ’l’ and ’1’.
- Changed appearances of "is equal" or "mod" to % operator for better readability.
- Fixed the log notation in the Schemes section
- Adpated security considerations

Further steps

- Detail security rationale
- Combine “algorithm OID” for WOTS+ with “XMSS OID”
- More detailed explanation of bit security and best attack costs for given parameter sets
- Reference implementation

Any comments on the draft are very welcome.

Thank you!

a.t.huelsing@tue.nl

dbutin@cdc.informatik.tu-darmstadt.de

stefan-lukas_gazdag@genua.eu

amohaisen@gmail.com