Overview of hash-based digital signature schemes

Gustavo Zambonin

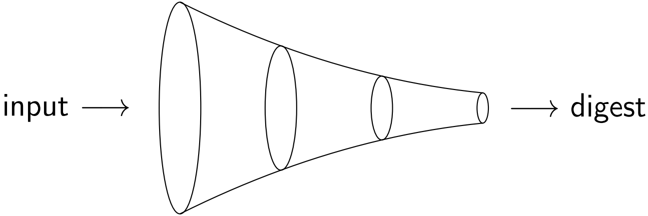
Federal University of Santa Catarina
Department of Informatics and Statistics

gustavo.zambonin@grad.ufsc.br

Motivation

- Independent from number theory or algebraic problems
  - Possibly ''post-quantum secure''
- For every digital signature scheme, one can use any hash function available
  - Chosen according to specific needs (hardware, software)
- One-way functions are necessary and sufficient for secure signatures [Rom90, KK05]

$$\mathcal{H} : \{0,1\}^* \longrightarrow \{0,1\}^n$$

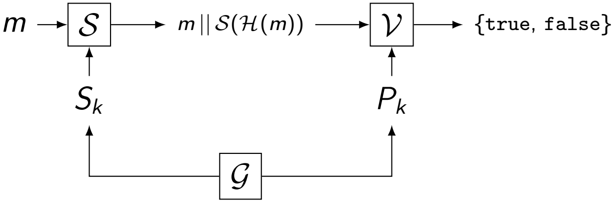


- RIPEMD: $n \in \{128, 160, 256, 320\}$
- SHA-2, SHA-3, BLAKE: $n \in \{224, 256, 384, 512\}$
- Keccak: any n

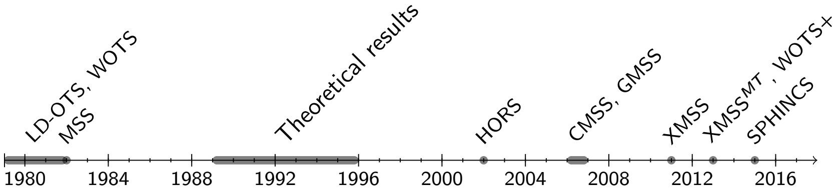
Foundations

Digital signatures

- Provide authentication, integrity and non-repudiation
- Based on public-key cryptography
- Triple of probabilistic polynomial time algorithms [Gol04]
  - Key generation ($\mathcal{G}$), signing ($\mathcal{S}$), verifying ($\mathcal{V}$)
- There should exist a way to bind a signer to its key



Timeline



Outline of the most important moments in hash-based digital signature schemes research, starting in 1979 with Lamport's one-time scheme, and shortly after with the work of Merkle, allowing many-time schemes through the use of hash trees.

The years marked as productive for ''theoretical results'' consist primarily of research about optimal one-time signature schemes and creation of variants.

One-time signature schemes

- Key pair shall be used only once
- Lamport-Diffie (LD-OTS)
  - First hash-based scheme
  - Arbitrary-length messages can be signed, one bit at a time
- Winternitz (WOTS)
  - Multiple bits are signed simultaneously
  - Generalization of LD-OTS
  - Tradeoff between performance and signature size
- HORS
  - Few-time scheme, security decreases with each signature
  - HORST — HORS with trees

Winternitz OTS

Key generation step

Let $w \in \mathbb{N}, w > 1$ be the Winternitz tradeoff parameter. Then,

$$t_1 = \left\lceil \frac{n}{w} \right\rceil$$

$$t_2 = \left\lceil \frac{\lfloor log_2 t_1 \rfloor + 1 + w}{w} \right\rceil$$

$$t = t_1 + t_2$$

The private and public keys are, respectively,

$$S_k = (y_{t-1}, \ldots, y_0) \xleftarrow{\$} \{0,1\}^n$$

$$P_k = (\mathcal{H}^{2^w-1}(y_{t-1}), \ldots, \mathcal{H}^{2^w-1}(y_0))$$

Winternitz OTS

Signing step

The hash chain exponents $\epsilon_i \in \{0,1\}^w$ are generated as follows:

$$\mathcal{H}(m) = (\epsilon_{t-1}, \ldots, \epsilon_{t-t_1}) \qquad \begin{aligned} c &= \sum_{i=t-t_1}^{t-1} (2^w - 1 - \epsilon_i) \\ &= (\epsilon_{t_2-1}, \ldots, \epsilon_0) \end{aligned}$$

Finally, the one-time signature is constructed.

$$\sigma = (\mathcal{H}^{\epsilon_{t-1}}(y_{t-1}), \ldots, \mathcal{H}^{\epsilon_0}(y_0))$$

Recall that

$$P_k = (\mathcal{H}^{2^w-1}(y_{t-1}), \ldots, \mathcal{H}^{2^w-1}(y_0)) \text{ and}$$
$$\sigma = (\mathcal{H}^{\epsilon_{t-1}}(y_{t-1}), \ldots, \mathcal{H}^{\epsilon_0}(y_0))$$

To verify σ, all ϵ_i are calculated and the hash chains are finished:

$$\forall \sigma_i \in \sigma, \mathcal{H}^{2^w-1-\epsilon_i}(\sigma_i) = P_{k_i}$$

Winternitz OTS

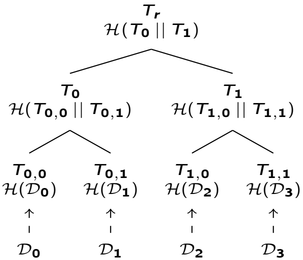
Improvements

- Shorter signature sizes in all improvements
- Eliminate the need for a collision resistant $\mathcal{H}$
  - Use of a non-compressing function family F_n
  - Random walk through F_n instead of simple iterations
- Round-specific bitmasks on each hash iteration $i \in \mathbb{N}$

$$
\begin{aligned}
(b_0, \dots, b_j) &\in \{0,1\}^{n \times j}, j \geq i \\
c^0(x) &= x \\
c^i(x) &= \mathcal{H}(c^{i-1}(x) \oplus b_i)
\end{aligned}
$$

Many-time signature schemes (Merkle)

- One-time signatures on each leaf, tree built from public keys
- Size and traversal of the tree are common issues
- Clever ways to store the key pair (e.g. seed of pseudorandom generator)
- Generally stateful schemes, i.e. track which OTS pairs were used



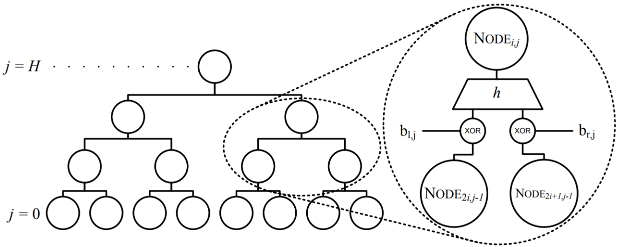
Take $\mathcal{D}_n$ as any data block. A Merkle tree can be constructed recursively through the concatenation of hashes of a node's children.

CMSS, GMSS

- Main idea: Merkle trees with layers
- Root of a child tree is signed with an OTS private key corresponding to a leaf of its parent
- CMSS as a special case of GMSS
- Simple Winternitz as chosen OTS scheme
- Amortized cost of key pair generation, competitive with classical schemes such as RSA, ECDSA

XMSS, XMSS^{MT}

- Bitmasks between levels of the tree
- Sub-tree on each leaf called L-tree
  - Stores each element of a WOTS public key in a balanced way
  - Bitmasks are the same for all L-trees
  - Only a second preimage resistant $\mathcal{H}$ is needed



Bibliography

Oded Goldreich.
Foundations of Cryptography: Volume 2, Basic Applications.
Cambridge University Press, New York, NY, USA, 2004.

Jonathan Katz and Chiu-Yuen Koo.
On constructing universal one-way hash functions from arbitrary one-way functions.
Cryptology ePrint Archive, Report 2005/328, 2005.
http://eprint.iacr.org/2005/328.

J. Rompel.
One-way functions are necessary and sufficient for secure signatures.
In *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 387–394, New York, NY, USA, 1990. ACM.