Hash-based signatures V

Few-times signatures

Tanja Lange

Eindhoven University of Technology

SAC – Post-quantum cryptography

Can we do with fewer leaves?

Reason for the large number in Goldreich/Levin: must never hit same leaf twice.

By the birthday paradox we need 2^{256} leaves, where each leaf is chosen by hash function $H(m)$.

Can we do with fewer leaves?

Reason for the large number in Goldreich/Levin: must never hit same leaf twice.

By the birthday paradox we need 2^{256} leaves,
where each leaf is chosen by hash function $H(m)$.

Change definition of H to have many components

$$H(m) = (h_0, h_1, \ldots, h_{k-1}),$$

where each $h_i \in \{0, 1, 2, \ldots, t-1\}$ for some t.
Collisions mean that all h_i match.

Can we do with fewer leaves?

Reason for the large number in Goldreich/Levin: must never hit same leaf twice.

By the birthday paradox we need 2^{256} leaves, where each leaf is chosen by hash function $H(m)$.

Change definition of H to have many components

$$H(m) = (h_0, h_1, \ldots, h_{k-1}),$$

where each $h_i \in \{0, 1, 2, \ldots, t-1\}$ for some t.
Collisions mean that all h_i match.

r-subset resilience

Let $H(m_j) = (h_{j,0}, h_{j,1}, \ldots, h_{j,k-1})$.
H is r-subset-resilient if given $H(m_1), H(m_2), \ldots, H(m_r)$ the probability of finding m' with $H(m') = (h'_0, h'_1, \ldots, h'_{k-1})$ and $h'_f \in \{h_{j,i} | 0 \leq i < k, 1 \leq j \leq r\}$ for $0 \leq f < k$ is negligible.

Can we do with fewer leaves?

Reason for the large number in Goldreich/Levin: must never hit same leaf twice.

By the birthday paradox we need 2^{256} leaves,
where each leaf is chosen by hash function $H(m)$.

Change definition of H to have many components

$$H(m) = (h_0, h_1, \ldots, h_{k-1}),$$

where each $h_i \in \{0, 1, 2, \ldots, t-1\}$ for some t.
Collisions mean that all h_i match.

r-subset resilience

Let $H(m_j) = (h_{j,0}, h_{j,1}, \ldots, h_{j,k-1})$.
H is r-subset-resilient if given $H(m_1), H(m_2), \ldots, H(m_r)$ the probability of finding m' with $H(m') = (h'_0, h'_1, \ldots, h'_{k-1})$ and $h'_f \in \{h_{j,i} | 0 \leq i < k, 1 \leq j \leq r\}$ for $0 \leq f < k$ is negligible.

The same leaf public key can be used for $r + 1$ signatures if H if r-subset-resilient.

Few-times signature HORS

(Hash to Obtain Random Subset)

General parameters:

- Integer parameters k, t, ℓ.
- Hash function $H : \{0,1\}^* \to \{0,1\}^{k \cdot \log_2 t}$.
- One-way function $f : \{0,1\}^\ell \to \{0,1\}^\ell$.

KeyGen:

- Picks t strings $s_i \in \{0,1\}^\ell$, compute $v_i = f(s_i)$ for $0 \le i < t$.
- Public key $P = (v_0, v_1, \ldots, v_{t-1})$; secret key $S = (s_0, s_1, \ldots, s_{t-1})$.

Sign $m \in \{0,1\}^*$:

- Compute $H(m) = (h_0, h_1, \ldots, h_{k-1})$, where each $h_i \in \{0, 1, 2, \ldots, t-1\}$.
- Signature on m is $\sigma = (s_{h_0}, s_{h_1}, s_{h_2}, \ldots, s_{h_{k-1}})$.

Verify:

- Compute $H(m) = (h_0, h_1, \ldots, h_{k-1})$ and $(f(s_{h_0}), f(s_{h_1}), f(s_{h_2}), \ldots, f(s_{h_{k-1}}))$.
- Verify that $f(s_{h_i}) = v_{h_i}$ for $0 \le i < t$.