SPHINCS+

PQC 7/3 or 5.

NIST PQC standard.

call for

4th round.

KEM (encryption)

1 lattice

Signature

3

2 lattice

1 hash.

PQC : lattice

idea code

hash

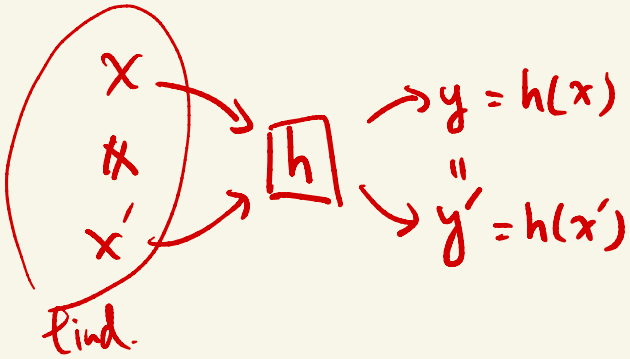
⋮

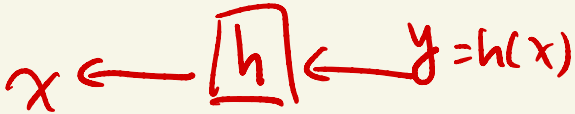
$2^n \xrightarrow{QC} poly(n)$

$2^n \xrightarrow{Grover} \sqrt{2^n}$

hash functions

SHA - 256





Winternitz One-time signature

$H^{256}(sk[0])$ ..... $H^{256}(sk[31])$

$\sigma = H^{255}(sk[0])$

$m_0 = 1$

m_0 ... m_{31}

8bit 8bit

$Vrfy(pk, m_0=1, H^{255}(sk[0]))$

$H(H^{255}(sk[0])) =? H^{256}(sk[0])$

$sk[0]$ .... $sk[31]$ — $pk[0]$

↘ sk

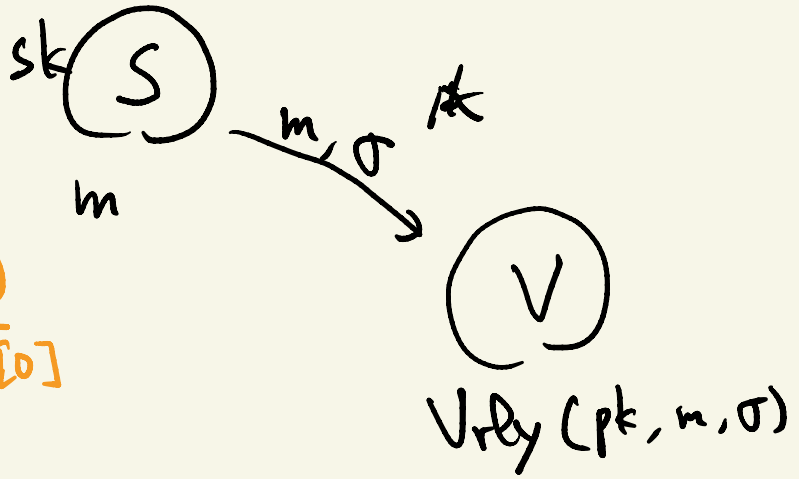
pk ↑ $H(\ldots)$ ↗

Signature

KeyGen : sk, pk. → public.

Sign(sk, m) → σ

Vrfy(pk, m, σ) = {0, 1} (0: reject, 1: accept)



$m_1 = 255$

$\sigma_1 = H^{256-255}(sk[1])$

$= H^1(sk[1])$

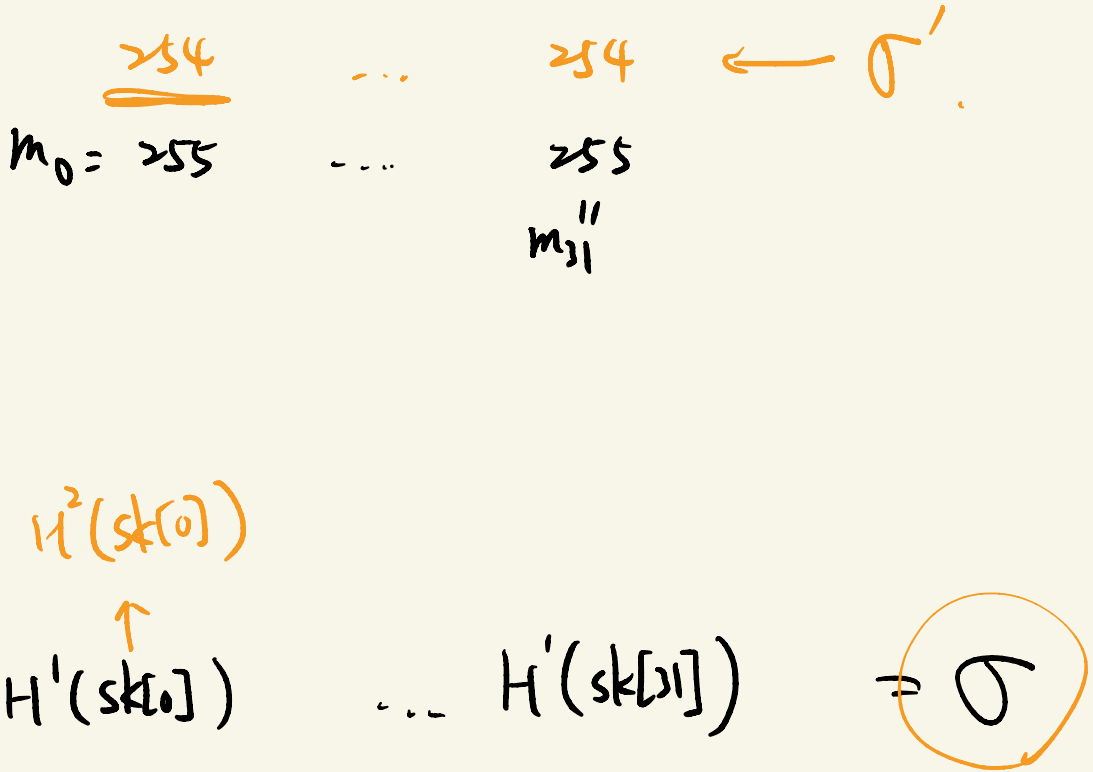
Vrly: $H^{255}(\sigma_1) \stackrel{?}{=} pk[1]$

$m_i = t$

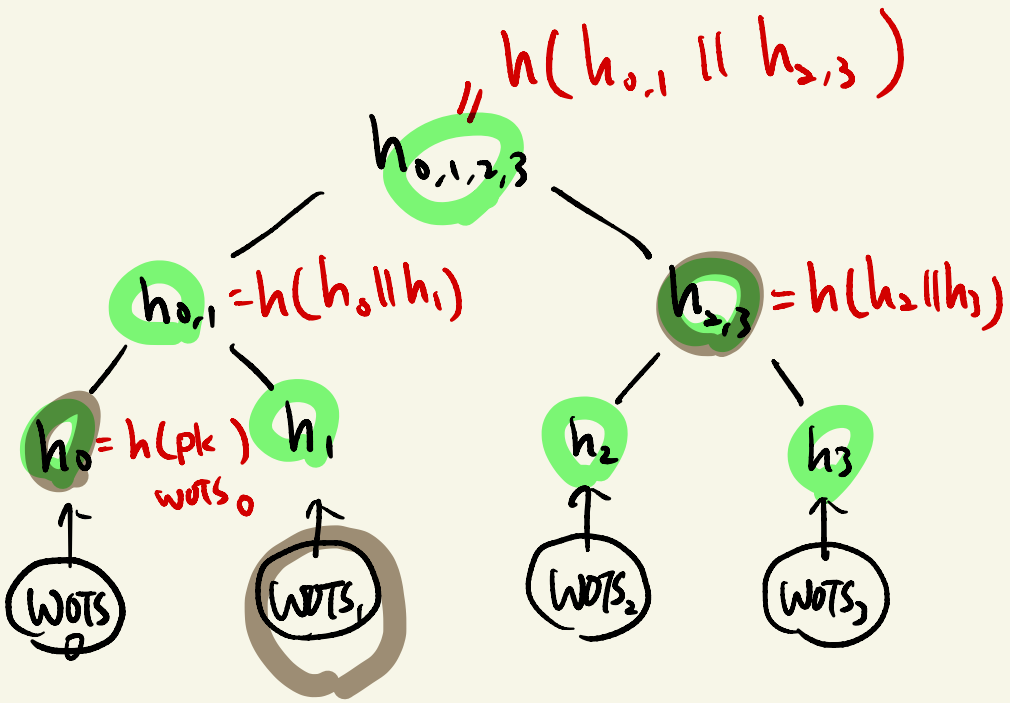
$\sigma_i = H^{256-t}(sk[i])$

Vrly $= H^t(\sigma_i)$

$= pk[i]$


254 ... 254 ← σ'
m0 = 255 ... 255
m'11
H²(sk[0])
H¹(sk[0]) ... H¹(sk[31]) ⇒ σ

Merkle tree.


$h(h_{0,1} \| h_{2,3})$
$h_{0,1,2,3}$
$h_{0,1} = h(h_0 \| h_1)$
$h_{2,3} = h(h_2 \| h_3)$
$h_0 = h(pk)$
$wots_0$
h_1
h_2
h_3
WOTS
$WOTS_1$
$WOTS_2$
$WOTS_3$

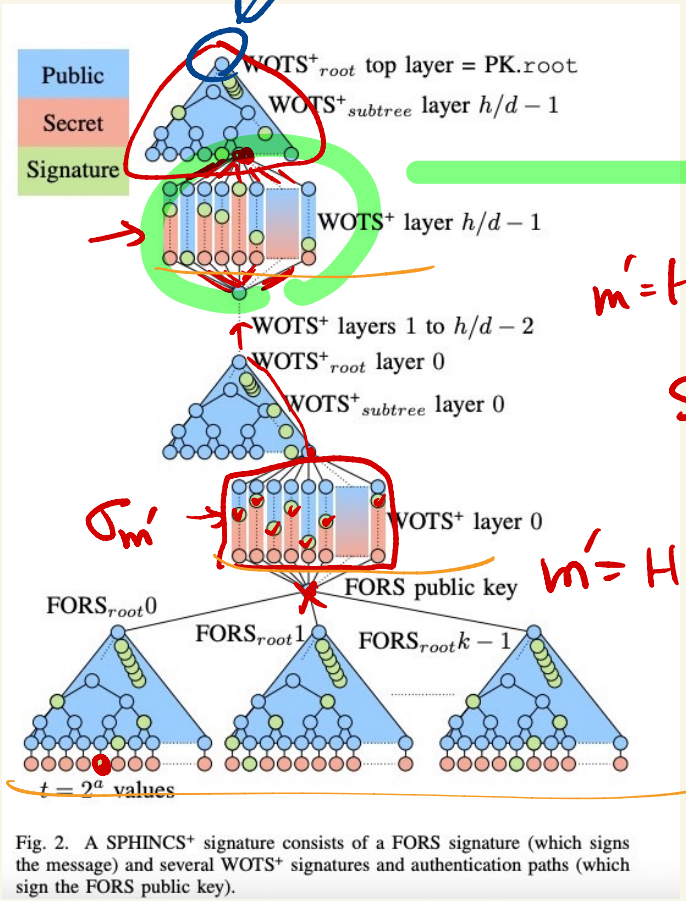


Fig. 2. A SPHINCS+ signature consists of a FORS signature (which signs the message) and several WOTS+ signatures and authentication paths (which sign the FORS public key).

$m' = H(m \| WOTS^{+}_{root}\ layer\ 0\ pk)$

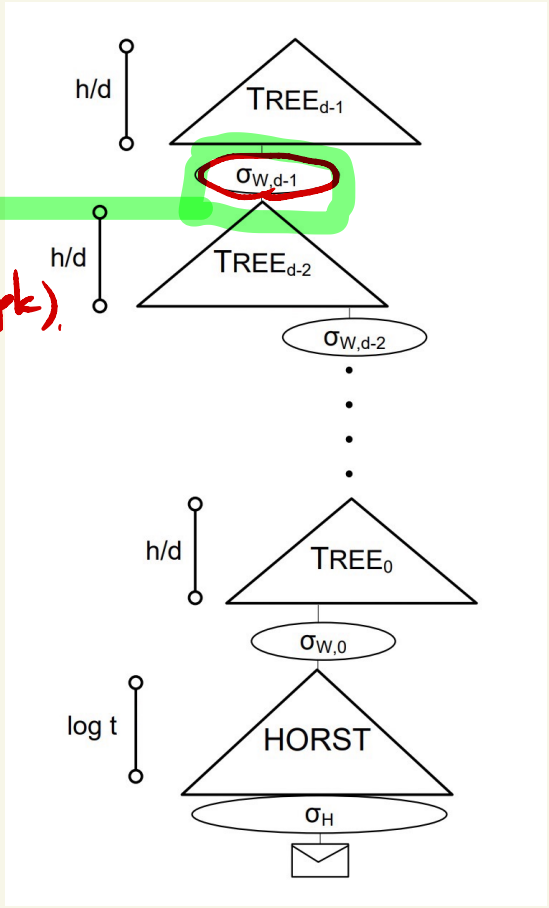
Stateless.

$m' = H(m \| FORS\ public)$

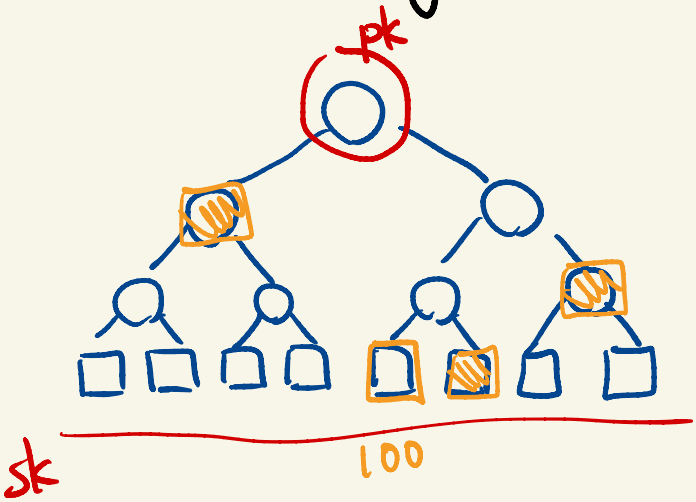
PRF( )

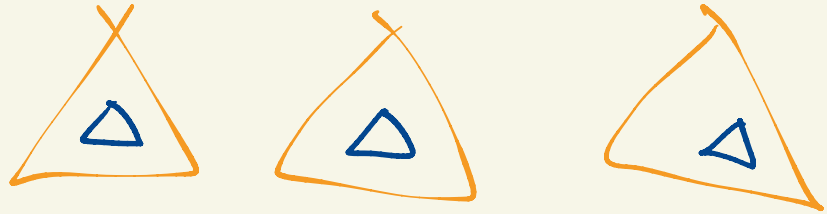
r_0

r_1



Few-time signature





message = 100 010 011 001