One time hash based signatures

- Lamport Signature
  
  Key gen
  
  \[ \text{Key gen} \]
  
  \[ |\text{sk}| = 2n^2 \]
  
  \[ \text{SPHINCS} \]
  
  \[ \text{sk} = [k_0, k_1, k_2, k_3, \ldots] \]
  
  \[ \text{pk} = [h_{\text{root}}] \]
  
  \[ \text{Sign} (\text{sk}, m) = m' \]

- Winternitz Z.

- Redeemed delegation

- Lamport

- Winternitz
Verification $(w_i, h_L, h_R)$:

$$H(H(h_L) || H^4(w_i(h_R))) = \text{root}.$$ 

Refereed Delegation

Verifier

Client accepts $y$

then $y = f(x)$

Security goal:

Any-trust setting

N servers, assume at least 1 server is honest

1. Check if all equal

\[ Y'_1 = Y'_2 = Y'_3 \]

2. Run a reconciliation protocol to find a correct server.

Performance goal:

Verifier's work: $\mathcal{O}(N \cdot \log |E|)$
Idea

\[ S(x) = g(g(g(\ldots g(x)))\ldots) = g^{|f|}(x) \]

Example: \( x' \neq y \)

\[ x \xrightarrow{g} y' \]

\[ y = g(x) \]

Method

\[ y_1', y_2', x \]

\[ y_1', y_2', x \]

\[ y_1', y_2', x \]

\[ y_1', y_2', x \]

\[ y_1', y_2', x \]

\[ y_1', y_2', x \]