Randomized FDH-RSA (PSS0)

PSS0 is a randomized variant of the FDH-RSA scheme. It has the same key generation algorithm.

PSS0 also uses H: $\{0,1\}^* \to Z_N^*$, a random function to which all parties have oracle access to, and it has a parameter *s*

Algorithm $\mathrm{Sign}^{H(\cdot)}_{N,p,q,d}(M)$	Algorithm $\mathrm{VF}^{H(\cdot)}_{N,e}(M,\sigma)$
$r \xleftarrow{\$} \{0,1\}^s$	Parse σ as (r,x) where $\lvert r \rvert = s$
$y \leftarrow H(r \parallel M)$	$y \leftarrow H(r \parallel M)$
$x \leftarrow y^d \bmod N$	If $x^e \bmod N = y$
Return (r,x)	Then return 1 else return 0

Security of PSS0

- Theorem. [Under the RSA assumption the PSS0 signature scheme is uf-cma secure in the random oracle (RO) model.] Let K_{rsa} be an RSA generator and let $\mathcal{DS}$ be the PSS0 signature scheme. Let *F* be an adversary making at most q_{hash} queries to its hash oracle and at most q_{sign} queries to its signing oracle where $q_{hash} \geq q_{sign} + 1$. Then there exists an adversary I with comparable resources s.t.

$$\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{DS}}(F) \leq \mathbf{Adv}^{\text{ow-kea}}_{\mathcal{K}_{\text{rsa}}}(I) + \frac{(q_{\text{hash}} - 1) \cdot q_{\text{sig}}}{2^s}$$

Other signature schemes

- Let's consider several signature schemes whose security relies on the hardness of the DL problem.
  - Schnorr signature scheme

Algoritm K(k)	Algoritm Sign_{sk}(M)
pick a k-bit prime p s.t. p=2q+1	$y \xleftarrow{\$} Z_q$
pick $g \in Z_p^*$ of order q	$Y \leftarrow g^y \bmod p$
$x \xleftarrow{\$} Z_q$	$c \leftarrow H(M \parallel Y)$
$X \leftarrow g^x$	$s \leftarrow y + cx \bmod q$
Pick a hash function $H: \{0,1\}^* \to Z_q$	Return (Y,s)
Return ((H,g,p,q,X),(H,g,p,q,x))	

Algoritm VF_{pk}(M,(Y,s))

$c \leftarrow H(M \parallel Y)$

If $g^s = YX^c$ (mod p) then return 1 else return 0

Other signature schemes

- ElGamal signature scheme

Algoritm K(k)	Algoritm Sign_{sk}(M)
pick a k-bit prime p	$y \xleftarrow{\$} Z_{p-1}^*$
pick a generator g of Z_p^*	$Y \leftarrow g^y \bmod p$
$x \xleftarrow{\$} Z_{p-1}$	$s \leftarrow y^{-1}\,(H(M \parallel Y) - xY) \bmod (p-1)$
$X \leftarrow g^x$	Return (Y,s)
Pick a hash function $H: \{0,1\}^* \to Z_{p-1}$	
Return ((H,g,p,q,X),(H,g,p,q,x))	

Algoritm VF_{pk}(M,(Y,s))

If $X^Y Y^s = g^{H(M \parallel Y)}$ (mod p) then return 1 else return 0

Security of Schnorr and ElGamal signatures

- The Schnorr and ElGamal signature schemes are uf-cma secure in the random oracle (RO) model in groups where the discrete logarithm (DL) problem is hard.