Randomized FDH-RSA (PSS0)

 $\mathsf{PSS0}$ is a randomized variant of the FDH-RSA scheme. It has the same key generation algorithm.

PSS0 also uses H: $\{0,1\}^* \to Z_3^*$, a random function to which all parties have oracle access to, and it has a parameter s

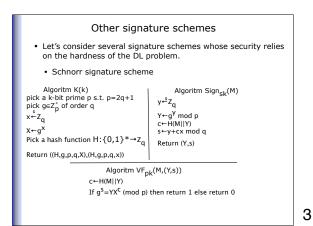
1

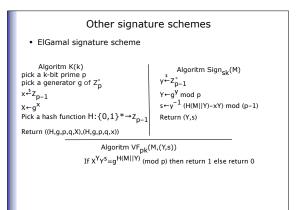
Security of PSS0

• <u>Theorem</u>. [Under the RSA assumption the PSS0 signature scheme is uf-cma secure in the random oracle (RO) model.] Let K_{FSa} be an RSA generator and let 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 $q_{hash} \ge q_{sign} + 1$. Then there exists an adversary I with comparable resources s.t.

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

2





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.

5