Multi-User Signature Forgery Game

$$pk_1, \ldots, pk_N$$

(m, i) — sign message m with key i

$$\sigma_{m,i} = \mathsf{Sign}(sk_i, m)$$

$$\sigma_{x,j} = \mathsf{Sign}(sk_j, x)$$

(x, j) — sign message x with key j

…(more signing oracle queries)…

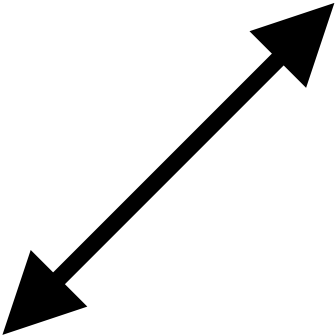
$$(i', m', \sigma')$$

$$(pk_i, sk_i) \leftarrow \mathsf{Kg}(1^k), 1 \leq i \leq N$$

Signature Scheme: $\Pi = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vfy})$

$$\mathsf{SigForge}^{\mathtt{RO},\mathtt{GO},N}_{\mathcal{A},\Pi}(k) = \begin{cases} 1 & \text{if } \mathsf{Vfy}(pk_{i'}, m', \sigma') = 1 \textit{ and } (m', i') \text{ is fresh} \\ 0 & \text{otherwise} \end{cases}$$

$$\mathtt{H}(\cdot), \mathtt{Mult}(\cdot,\cdot), \mathtt{Inv}(\cdot)$$



S-bit hint (preprocessing)

09

UF-CMA Security

Multi-User Signature Forgery Game

UF-CMA Security

$\mathsf{H}(\cdot), \mathtt{Mult}(\cdot,\cdot), \mathtt{Inv}(\cdot)$

S-bit hint (preprocessing)

$\longleftarrow$ $pk_1, \ldots, pk_N$

$\longrightarrow$ (m, i) — sign message m with key i

$\longleftarrow$ $\sigma_{m,i} = \mathsf{Sign}(sk_i, m)$

$\longrightarrow$ (x, j) — sign message x with key j

$\longleftarrow$ $\sigma_{x,j} = \mathsf{Sign}(sk_j, x)$

…(more signing oracle queries)…

$\longrightarrow$ (i', m', σ')

$\longleftarrow$ $\mathsf{SigForge}^{\mathtt{RO},\mathtt{GO},N}_{\mathcal{A},\Pi}(k) = \begin{cases} 1 & \text{if } \mathsf{Vfy}(pk_{i'}, m', \sigma') = 1 \textit{ and } (m', i') \text{ is fresh} \\ 0 & \text{otherwise} \end{cases}$

Signature Scheme: $\Pi = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vfy})$

$(pk_i, sk_i) \leftarrow \mathsf{Kg}(1^k), 1 \leq i \leq N$

Reduction Idea

Multi-User Security of Short Schnorr Signatures

Single-User Security → Discrete-Log Problem

- Hardness assumption
- True in the Generic Group Model (GGM)

Multi-User Security → Bridge-Finding Game (in the GGM)