Multi-User Security of Short Schnorr Signatures

in the ROM+GGM

where $p \simeq 2^{2k}$.

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

$$\xleftarrow{\quad pk_1, \ldots, pk_N \quad}$$

$$\xrightarrow{\quad (m, i) \text{ — sign message } m \text{ with key } i \quad}$$

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

$$\xrightarrow{\quad (x, j) \text{ — sign message } x \text{ with key } j \quad}$$

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

...(more signing oracle queries)...

$$\xrightarrow{\quad (i', m', \sigma') \quad}$$

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

Signature Scheme: $\Pi = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vfy})$
$(pk_i, sk_i) \leftarrow \mathsf{Kg}(1^k), 1 \le i \le N$

13

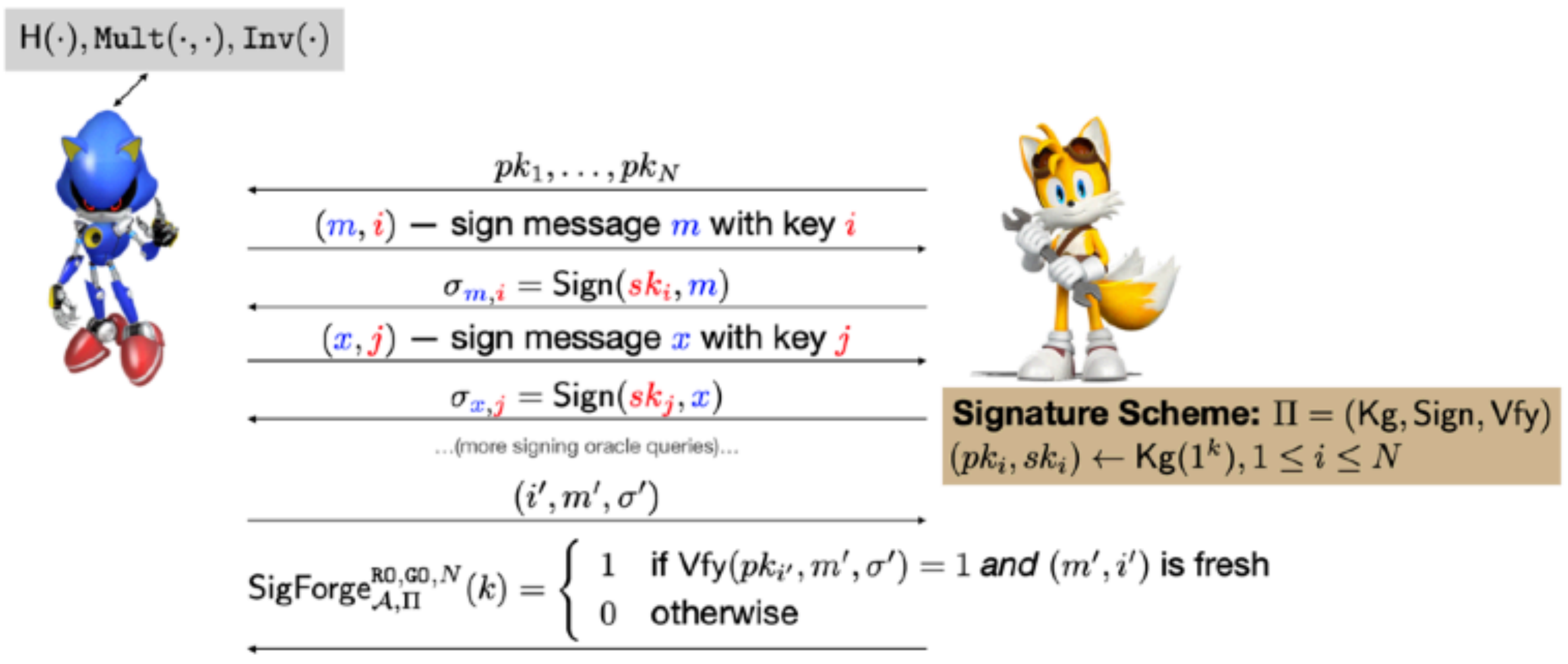
$$
\begin{aligned}
\Pr\left[\mathsf{SigForge}^{\mathtt{RO},\mathtt{GO},N}_{\mathcal{A},\Pi}(k)=1\right] &\leq \Pr[\mathsf{BRIDGE}]+\Pr[\mathsf{Bad}] \\
&\leq \mathcal{O}\left(\frac{q^2+qN}{p}+\frac{q}{2^k}\right) \\
&\leq \mathcal{O}\left(\frac{q+N}{2^k}\right),
\end{aligned}
$$

Note: Kiltz et al. [KMP16] proved a similar bound for *regular* Schnorr signatures though the authors observed (personal communication) that their analysis extends to short Schnorr signatures

- ▷ The GGM used in [KMP16] is not equivalent to Shoup's model and is not suitable for analyzing preprocessing attacks

Multi-User Security of Short Schnorr Signatures

in the ROM+GGM



$$
\begin{aligned}
\Pr\left[\mathsf{SigForge}_{\mathcal{A},\Pi}^{\mathtt{RO},\mathtt{GO},N}(k) = 1\right] &\le \Pr[\mathsf{BRIDGE}] + \Pr[\mathsf{Bad}] \\
&\le \mathcal{O}\left(\frac{q^2 + qN}{p} + \frac{q}{2^k}\right) \\
&\le \mathcal{O}\left(\frac{q+N}{2^k}\right),
\end{aligned}
$$

where $p \simeq 2^{2k}$.

Note: Kiltz et al. [KMP16] proved a similar bound for *regular* Schnorr signatures though the authors observed (personal communication) that their analysis extends to short Schnorr signatures

- ▷ The GGM used in [KMP16] is not equivalent to Shoup's model and is not suitable for analyzing preprocessing attacks

Modeling Preprocessing Attacks

Auxiliary-Input Model/Bit-Fixing Model

Auxiliary-Input Model

- ▷ Offline attacker $\mathcal{A}_{\mathsf{pre}}$ is unbounded and outputs an S-bit hint for online attacker $\mathcal{A}_{\mathsf{on}}$
- ▷ $\mathcal{A}_{\mathsf{on}}$ will try to win security games using the hint

Bit-Fixing Model (ROM)

- ▷ $\mathcal{A}_{\mathsf{pre}}$ fixes random oracle $\mathsf{H}(\cdot)$ at P locations
- ▷ $\mathcal{A}_{\mathsf{on}}$ initially knows nothing about remaining unfixed values (picked uniformly at random)