Summary of Our Results

Research Questions

06

Are **short** Schnorr signatures secure against **preprocessing attacks**?

▷ **Answer 1:** No! (trivial attack)

$\mathsf{Kg}(1^k)$	$\mathsf{Sign}(sk, m)$	$\mathsf{Vfy}(pk, m, \sigma)$
1 : $sk \leftarrow \mathbb{Z}_p$	1 : $r \xleftarrow{\$} \mathbb{Z}_p$; $I \leftarrow g^r$	1 : $R \leftarrow g^s \cdot pk^{-e}$
2 : $pk \leftarrow g^{sk}$	2 : $e \leftarrow \mathsf{H}(I \Vert m)$	2 : **if** $\mathsf{H}(R \Vert m) = e$ **then**
3 : **return** (pk, sk)	3 : $s \leftarrow r + sk \cdot e \mod p$	3 : **return** 1
	4 : **return** $\sigma = (s, e)$	4 : **else return** 0

pre

(m, r) such that $e = \mathsf{H}(I \| m) = 0$

always return 1!

Summary of Our Results

Research Questions

Are **short** Schnorr signatures secure against **preprocessing attacks**?

▷ **Answer 1:** No! (trivial attack)

(m, r) such that $e = \mathsf{H}(I \| m) = 0$!

$\mathsf{Kg}(1^k)$	$\mathsf{Sign}(sk, m)$	$\mathsf{Vfy}(pk, m, \sigma)$
1 : $sk \leftarrow \mathbb{Z}_p$	1 : $r \xleftarrow{\$} \mathbb{Z}_p$; $I \leftarrow g^r$	1 : $R \leftarrow g^r \cdot pk^{-e}$
2 : $pk \leftarrow g^{sk}$	2 : $e \leftarrow \mathsf{H}(I \| m)$	2 : **if** $\mathsf{H}(R \| m) = e$ **then**
3 : **return** (pk, sk)	3 : $s \leftarrow r + sk \cdot e \mod p$	3 : **return** 1
	4 : **return** $\sigma = (s, e)$	4 : **else return** 0

always return 1!

Summary of Our Results

Research Questions

Are **short** Schnorr signatures secure against **preprocessing attacks**?

- **Answer 2:** Yes, **key-prefixed** short Schnorr signatures are secure!