

Summary of Our Results

Research Questions





Are short snippets secure against preprocessing attacks?

➤ Answer 1: No! (trivial attack)

$\text{Kg}(1^k)$	$\text{Sign}(sk, m)$	$\text{Vfy}(pk, m, \sigma)$
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 : $e \leftarrow \text{H}(I m)$	2 : if $\text{H}(R m) = e$ then
3 : return (pk, sk)	3 : $s \leftarrow r + sk \cdot e \bmod p$	3 : return 1
	4 : return $\sigma = (s, e)$	4 : else return 0



pre



$$(n, r) \text{ such that } e \equiv H(I || n) \equiv 0$$









ro





always return 2!







Summary of Our Results

Research Questions



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

▷ **Answer 1:** No! (trivial attack)



(m, r) such that $e = H(I || m) = 0$!

$\text{Kg}(1^k)$

1: $sk \leftarrow \mathbb{Z}_p$
 2: $pk \leftarrow g^{sk}$
 3: **return** (pk, sk)

$\text{Sign}(sk, m)$

1: $r \xleftarrow{\$} \mathbb{Z}_p; I \leftarrow g^r$
 2: $e \leftarrow H(I || m)$
 3: $r \leftarrow r + sk \cdot e \bmod p$
 4: **return** $\sigma = (r, e)$

$\text{Vfy}(pk, m, \sigma)$

1: $I \leftarrow g^r \cdot pk^{-e}$
 2: **if** $H(I || m) = e$ **then**
 3: **return** 1
 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!