

Summary of Our Results

Research Questions



Are short Schnorr signatures secure against preprocessing attacks?

Answer 1: No! (trivial attack)

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





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















always return 1!







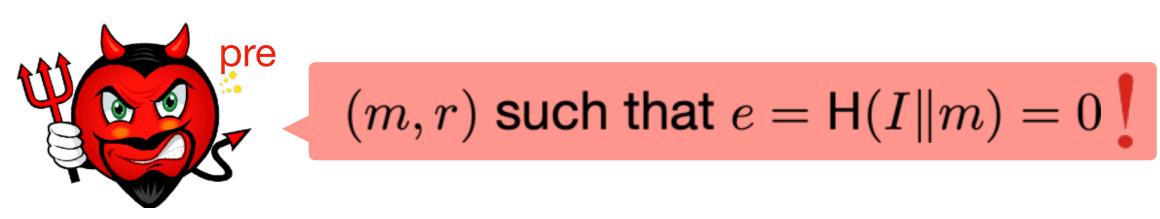
Summary of Our Results

Research Questions



Are short Schnorr signatures secure against preprocessing attacks?

▶ Answer 1: No! (trivial attack)



$Kg(1^k)$	Sign(sk,m)	$Vfy(pk, m, \sigma)$
1: $sk \leftarrow \mathbb{Z}_p$	1: $r \stackrel{\$}{\leftarrow} \mathbb{Z}_p$; $I \leftarrow g^r$	1: $\mathbb{R} \leftarrow g^{s} \cdot pk^{-s}$
$2: pk \leftarrow g^{sk}$	$2: \bigcirc \leftarrow H(I m)$	2: if $H(\mathbb{Z}\ m)=$ \circ then
3: return (pk, sk)	$3: \mathbf{r} \leftarrow r + sk \cdot \mathbf{o} \mod p$	$\mathfrak{3}$: return 1
	4 : return $\sigma = (\mathbf{r}, \mathbf{e})$	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!