



**The (Short) Short Signature Scheme**

- **Public parameters:**

- ▷ Group  $G = \langle g \rangle$  of size  $p \approx 2^{2k}$ , where  $k$  is the security parameter
- ▷ Hash function  $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$

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









24 bits



2nd Bits







shorts shorts Signatures!



# The (Short) Schnorr Signature Scheme

- **Public parameters:**

- ▷ Group  $G = \langle g \rangle$  of size  $p \approx 2^{2k}$ , where  $k$  is the security parameter
- ▷ Hash function  $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$

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

1110101101101100011010101101011010101101

$\nearrow$

01101011010010000010

$\nwarrow$

$2k$  bits

$k$  bits

Short Schnorr Signature!

# Summary of Our Results

## Research Questions



Are **short** Schnorr signatures secure (**multi-user security**)?