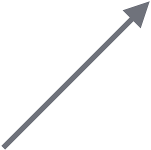
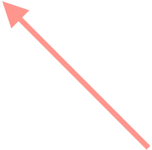
The (Short) Schnorr Signature Scheme

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

$\mathsf{Kg}(1^k)$	$\mathsf{Sign}(sk, m)$	$\mathsf{Vfy}(pk, m, \sigma)$
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 : $e \leftarrow \mathsf{H}(I \\| m)$	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





$2k$ bits

$2k$ bits

Short Schnorr Signature!

04

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 $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_p$

$\mathsf{Kg}(1^k)$	$\mathsf{Sign}(sk, m)$	$\mathsf{Vfy}(pk, m, \sigma)$
$1: sk \leftarrow \mathbb{Z}_p$	$1: r \xleftarrow{\$} \mathbb{Z}_p;\ I \leftarrow g^r$	$1: R \leftarrow g^s \cdot pk^{-e}$
$2: pk \leftarrow g^{sk}$	$2: e \leftarrow \mathsf{H}(I \Vert m)$	$2:$ **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

1110101101101100011010101101011010101101	0110101101001000001 0
$2k$ bits	k bits

Short Schnorr Signature!

Summary of Our Results

Research Questions

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