Summary of Our Results

Research Questions

05

Do **short** Schnorr signatures have **multi-user security**?

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

- **Answer:** Yes, still provide k bits of multi-user security!
- No concrete security loss (naïve reduction has loss of multiplicative factor of N)
- **Proof:** In the Random Oracle Model (ROM) + Generic Group Model (GGM)

▷ **Answer 1:** No! (trivial attack)

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

- **Answer 3:** Yes, “short” version of **standardized implementations** of Schnorr signatures are secure!

06

- **Answer:** Yes, still provide k bits of multi-user security!
- No concrete security loss (naïve reduction has loss of multiplicative factor of N)
- **Proof:** In the Random Oracle Model (ROM) + Generic Group Model (GGM)

```
Kg$(1^k)$
    $sk \leftarrow \mathbb{Z}_p$
    $pk \leftarrow g^{sk}$
    return $(pk, sk)$
```

```
Sign$(sk, m)$
    $r \xleftarrow{\$} \mathbb{Z}_p$; $I \leftarrow g^r$
    $e \leftarrow \mathsf{H}(I \| m)$
    $s \leftarrow r + sk \cdot e \mod p$
    return $\sigma = (s, e)$
```

```
Vfy$(pk, m, \sigma)$
    $R \leftarrow g^s \cdot pk^{-e}$
    if $\mathsf{H}(R \| m) = e$ then
        return $1$
    else return $0$
```

pre

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

!