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

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

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

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

Summary of Our Results

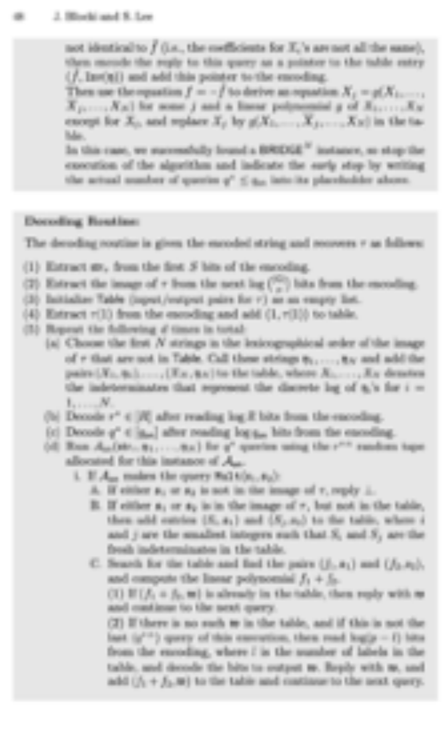
Research Questions

07

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

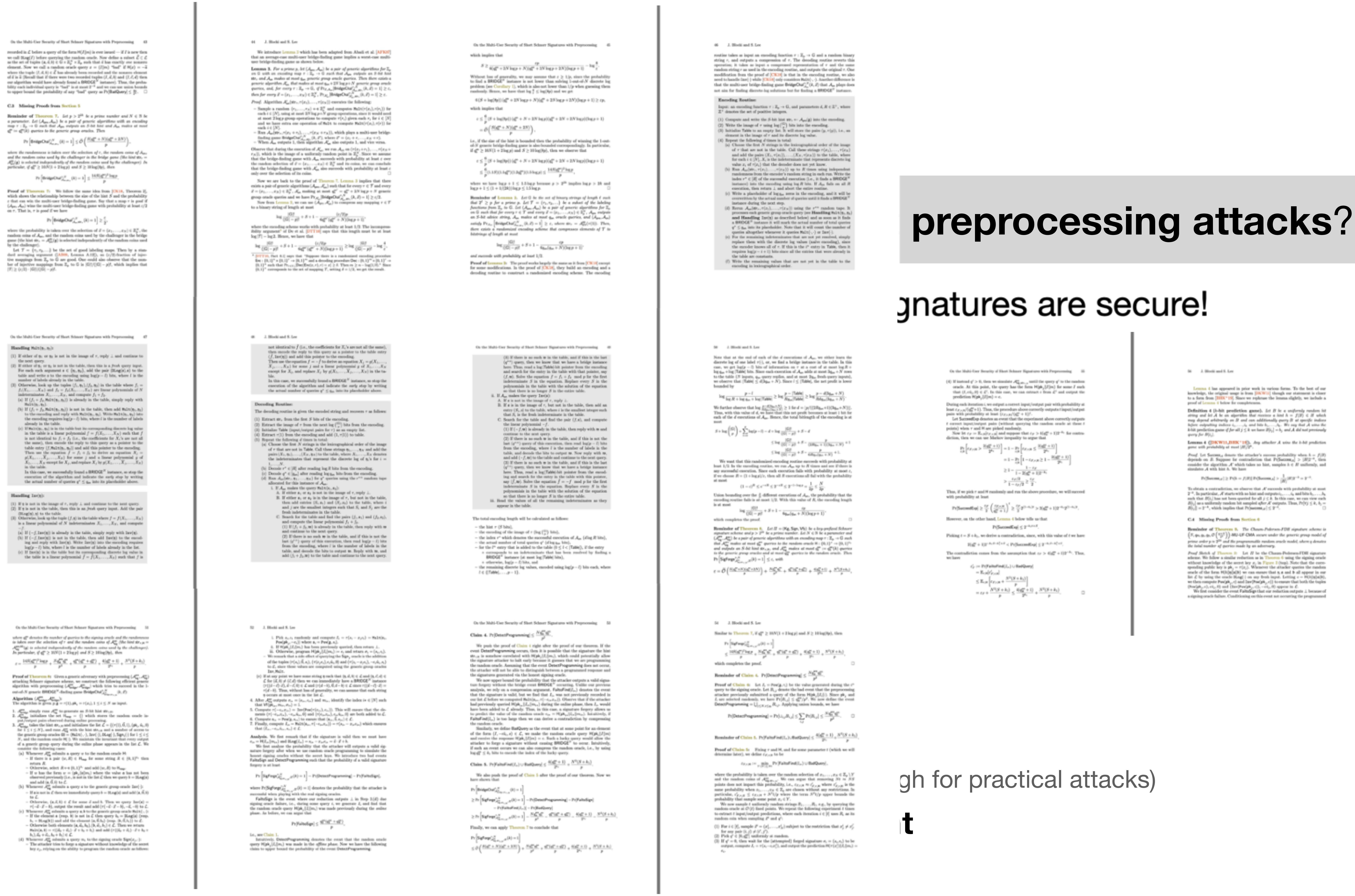
Caveats:

- Not a **standardized** implementation
- Preprocessing attacker is **time-bounded** (large enough for practical attacks)
- Complex proof technique: **compression argument**



Su

Res



preprocessing attacks?

gnatures are secure!

gh for practical attacks)

t

Summary of Our Results

Research Questions

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

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