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)

Summary of Our Results

Research Questions

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

- **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)

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

Summary of Our Results

Research Questions

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

- **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)

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

- **Answer 1:** No! (trivial attack)