Summary of Our Results

Research Questions



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

Summary of Our Results

Research Questions



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