







# Summary of Our Results

# Research Questions



Are short signatures secure against

**preparing attacks (multi-user security)?**



Do short signatures have multi-user security?



Are short snippets secure against preprocessing attacks?



