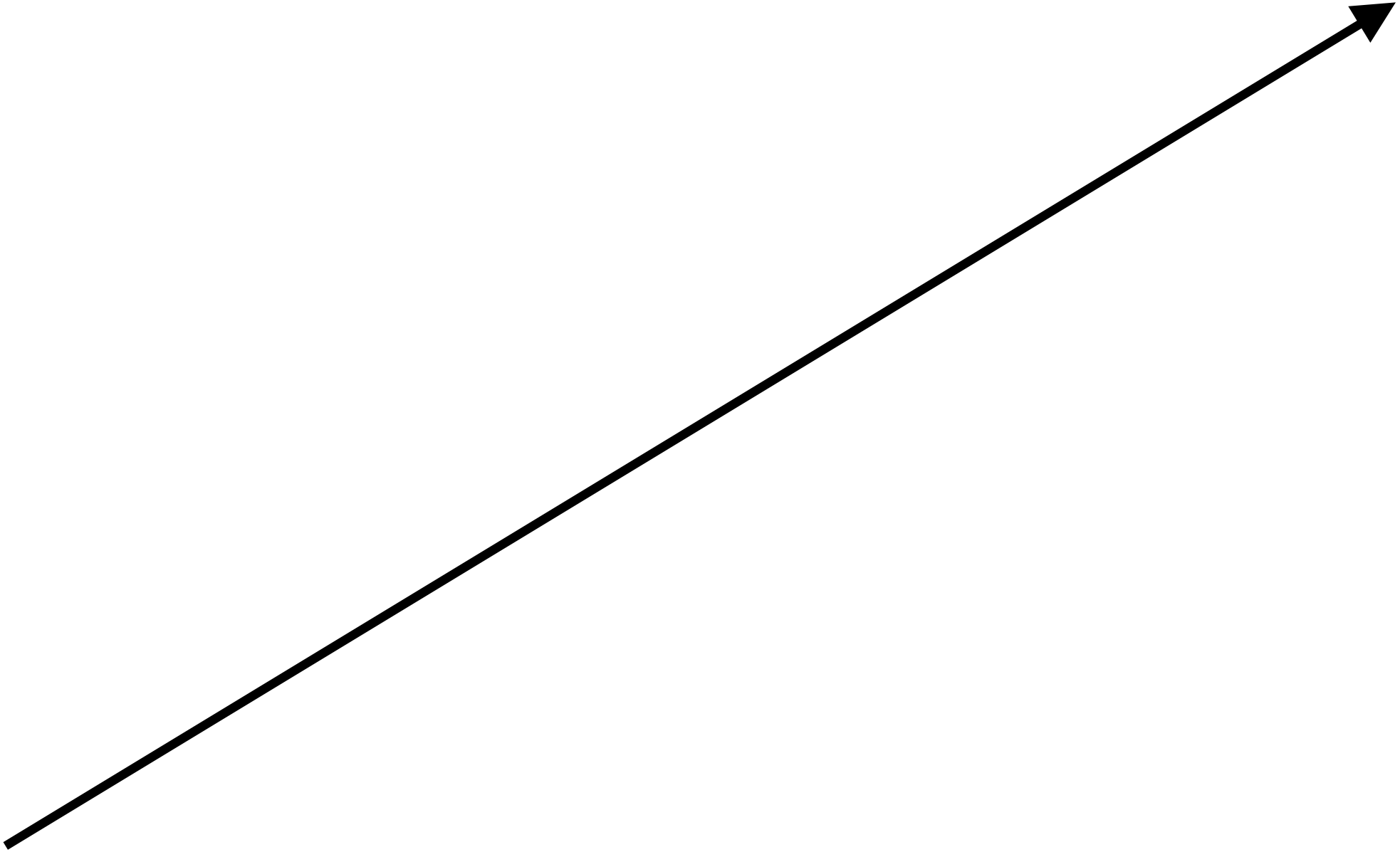
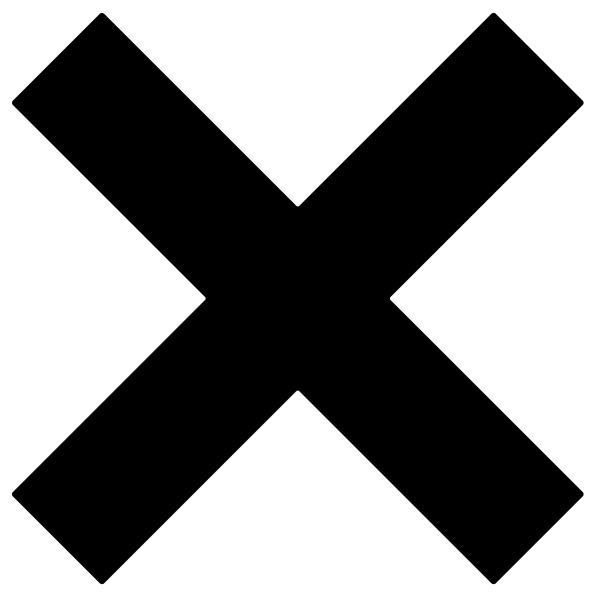
Verify(, ,)

Digital Signatures

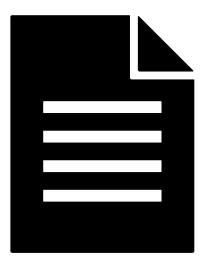

Fail!

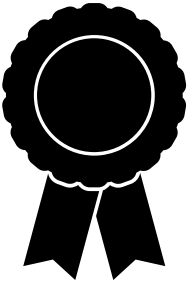
02



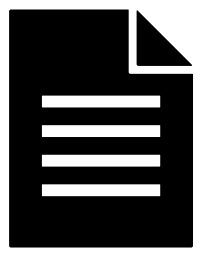


03






Verify(, ,)



Pass!

preprocessing attacks


security

k bits of (multi-user)

efficient signing/

short signatures

verification

- k **bits of security:** attacker running in time t wins signature forgery game with prob. $\leq \frac{t}{2^k}$
- Multi-user security: 1-out-of-N setting