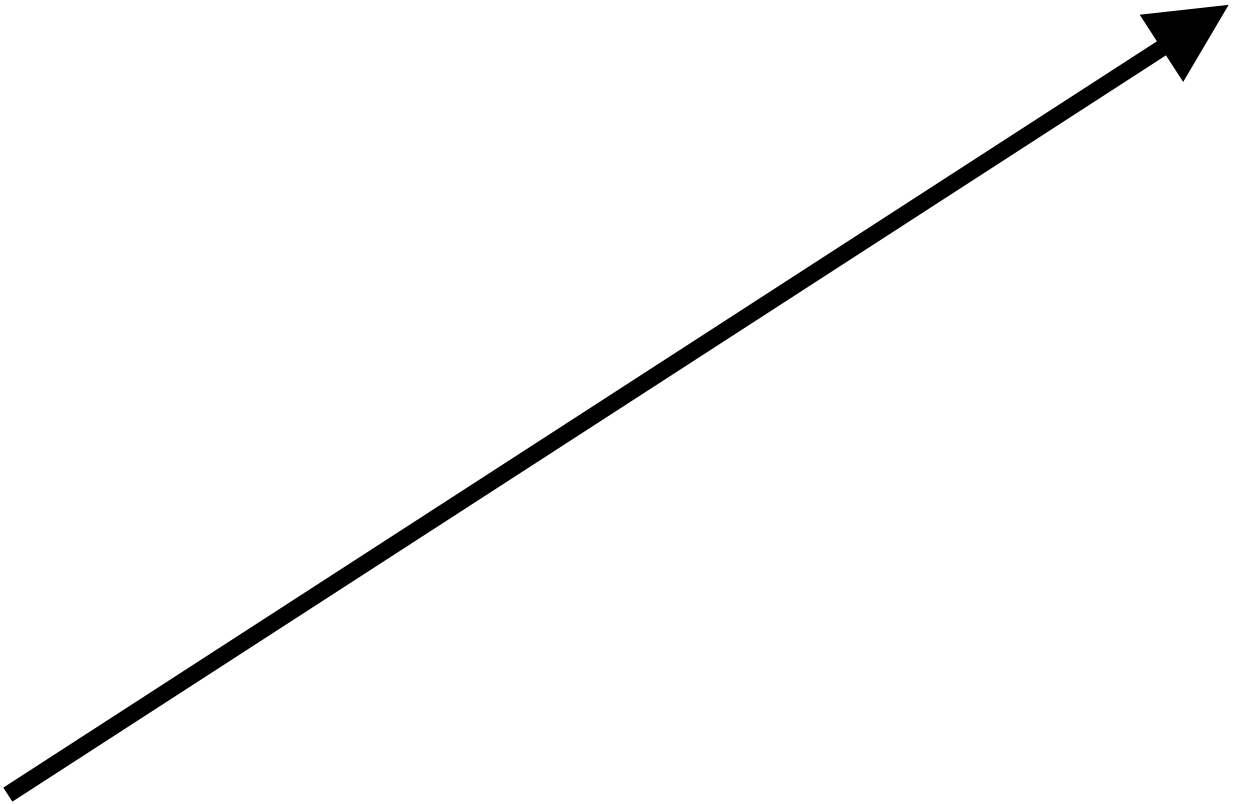
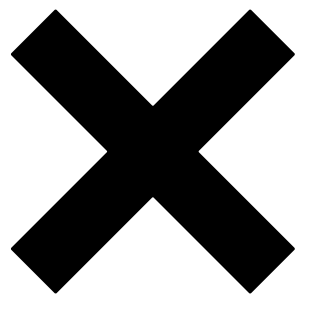

Verify(, ,)

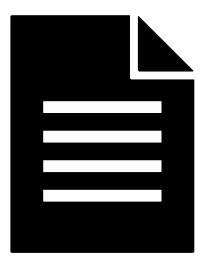
Digital Signatures

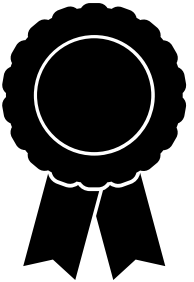

Fail!

03

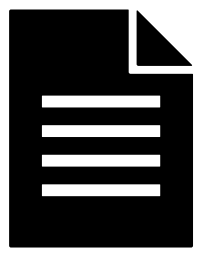


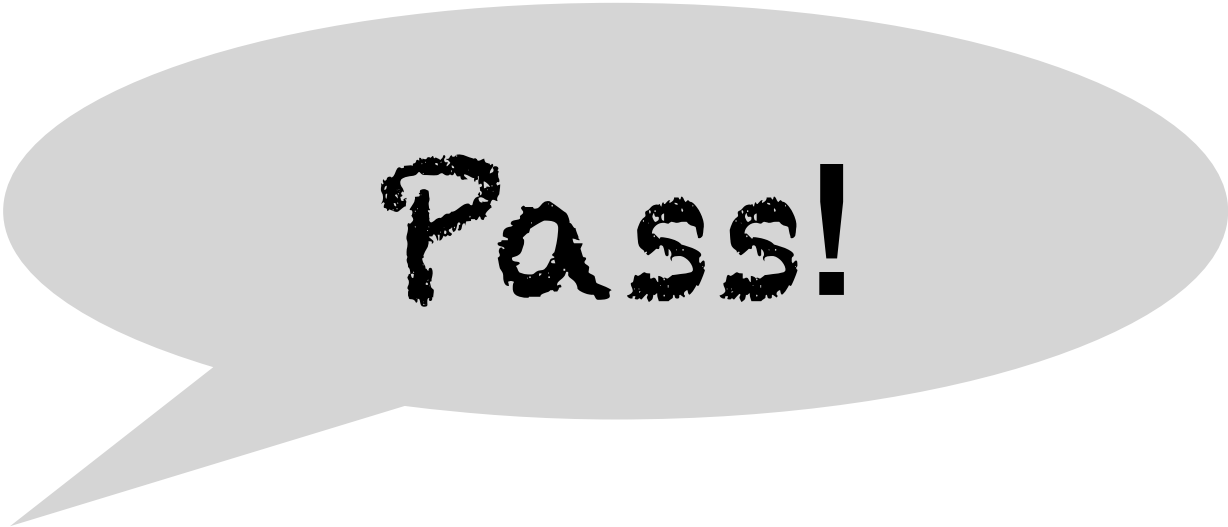







Verify(, ,)




Pass!

Desiderata

Security

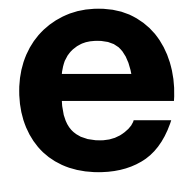
Efficiency

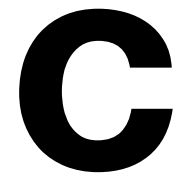
k bits of (multi-user) security

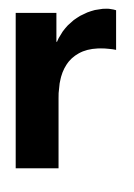
- k **bits of security:** attacker running in time t wins signature forgery game with prob. $\leq \frac{t}{2^k}$
- Multi-user security: 1-out-of-N setting

Given N public keys, $\mathcal{A}$ wins if
it forges a signature that is valid
under *any one* of these public keys

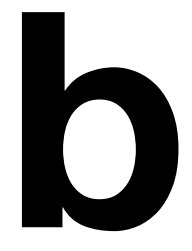
preprocessing attacks

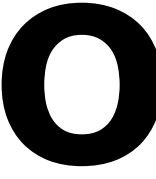


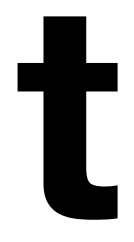

C

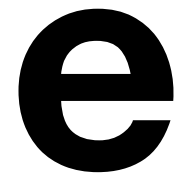



y



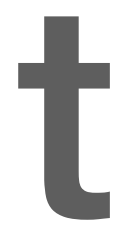


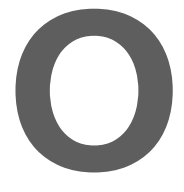




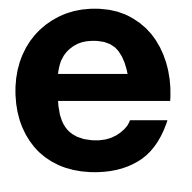
short signatures

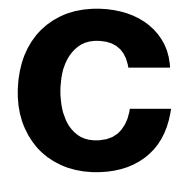

C

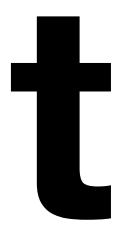


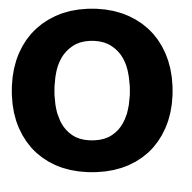


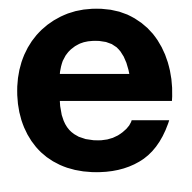

S



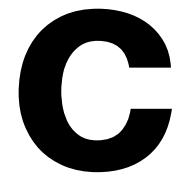

C








ffi


C