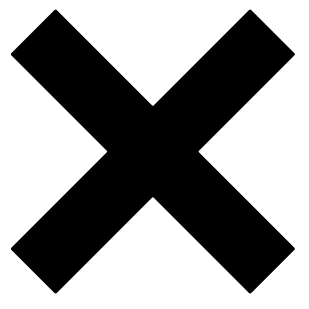
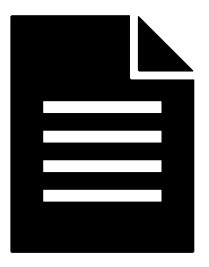

Verify(, ,)

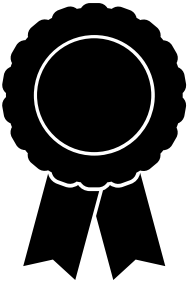
Digital Signatures


Fail!

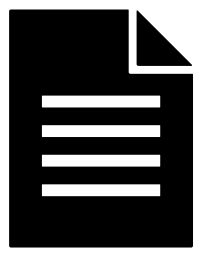
03

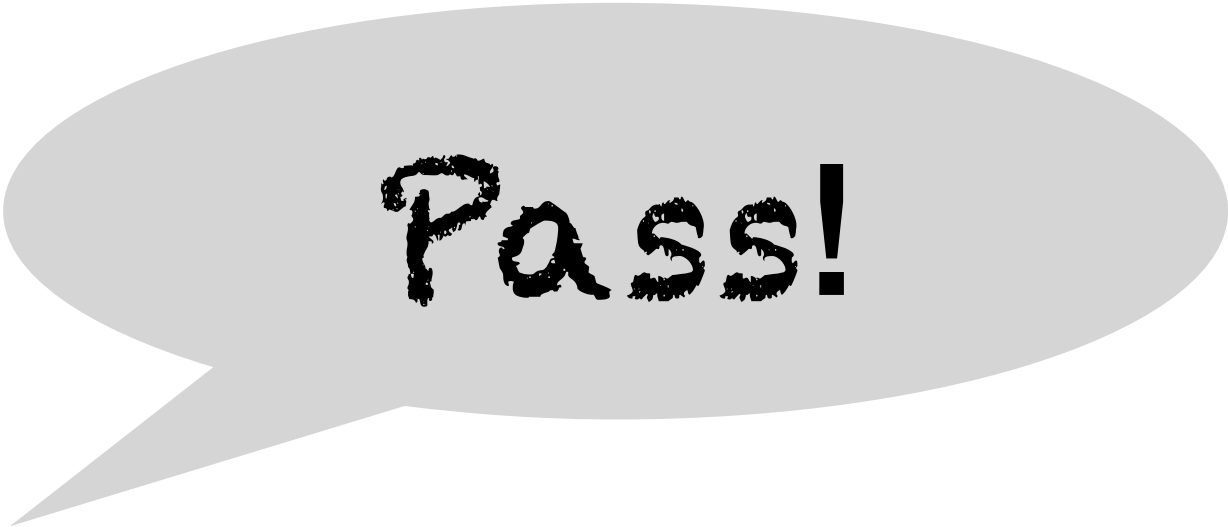







Verify(, ,)




Pass!

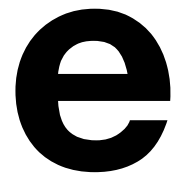
Desiderata

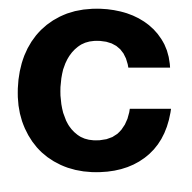
Security

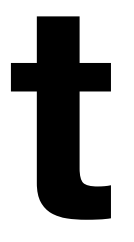
Efficiency

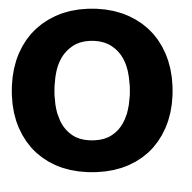
k bits of (multi-user) security

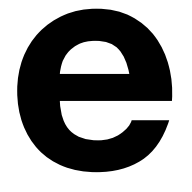
short signatures



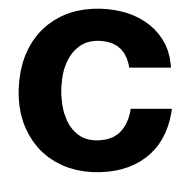

C

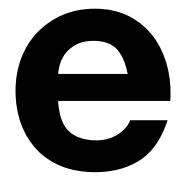


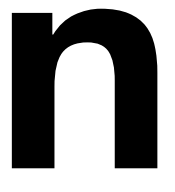


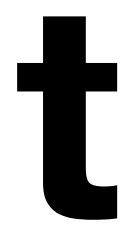



ffi


C







- 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


fi

- The vast majority of real-world crypto systems use one

- Adversary with nation-state level resources might spend

a lot of time *precomputing hints* to help break protocols/

of a handful of groups

solve hard problems using these building blocks

NIST

National Institute of
Standards and Technology

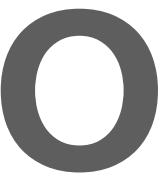
SHA-2/3, SHAKE,
P-256/384, Curve25519/448,
DSA groups, AES, Triple DES,
…

k bits of (multi-user) security

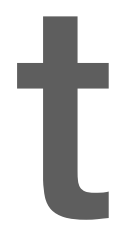
preprocessing attacks


fi

C




C




S