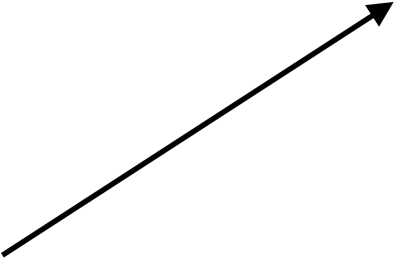
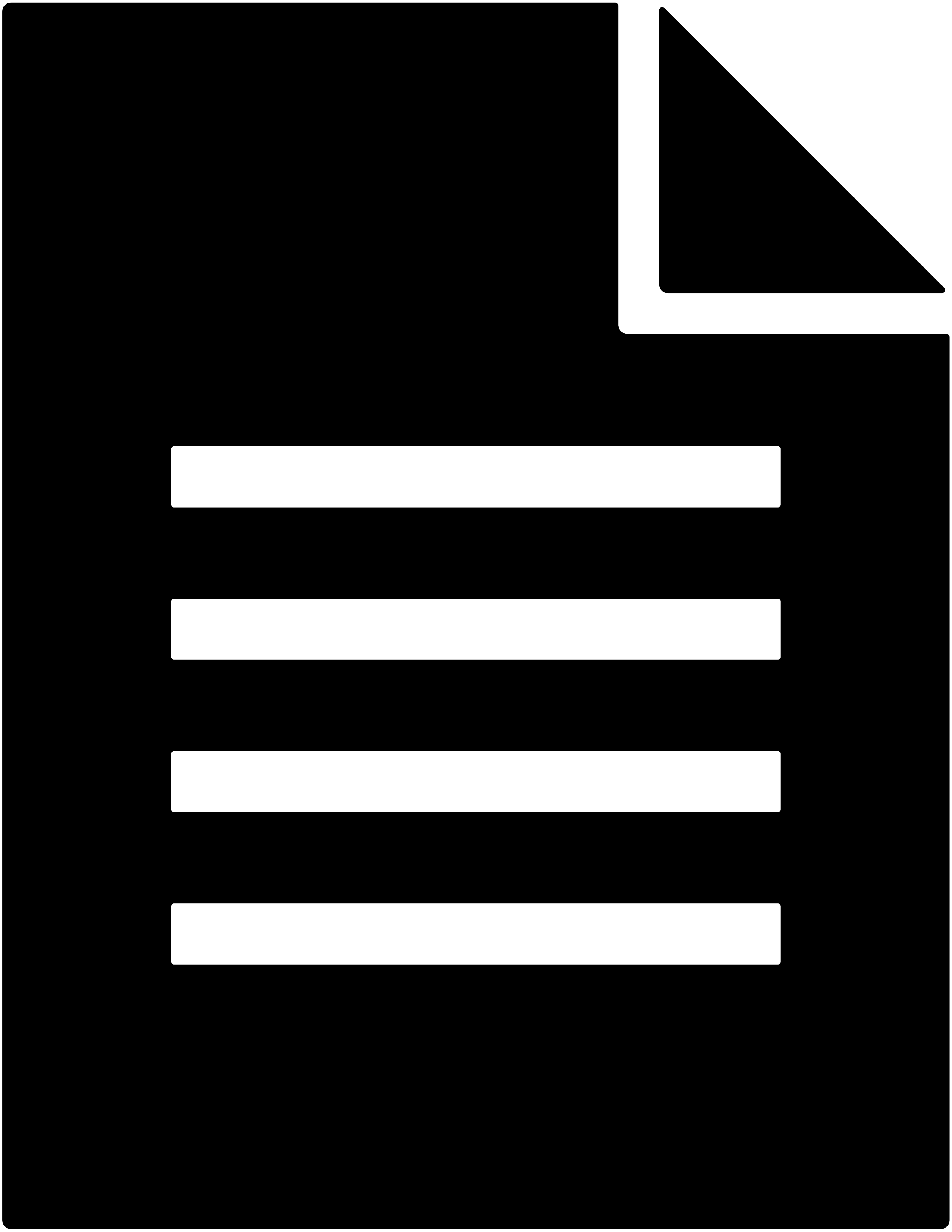
Verify(, ,)

Digital Signatures

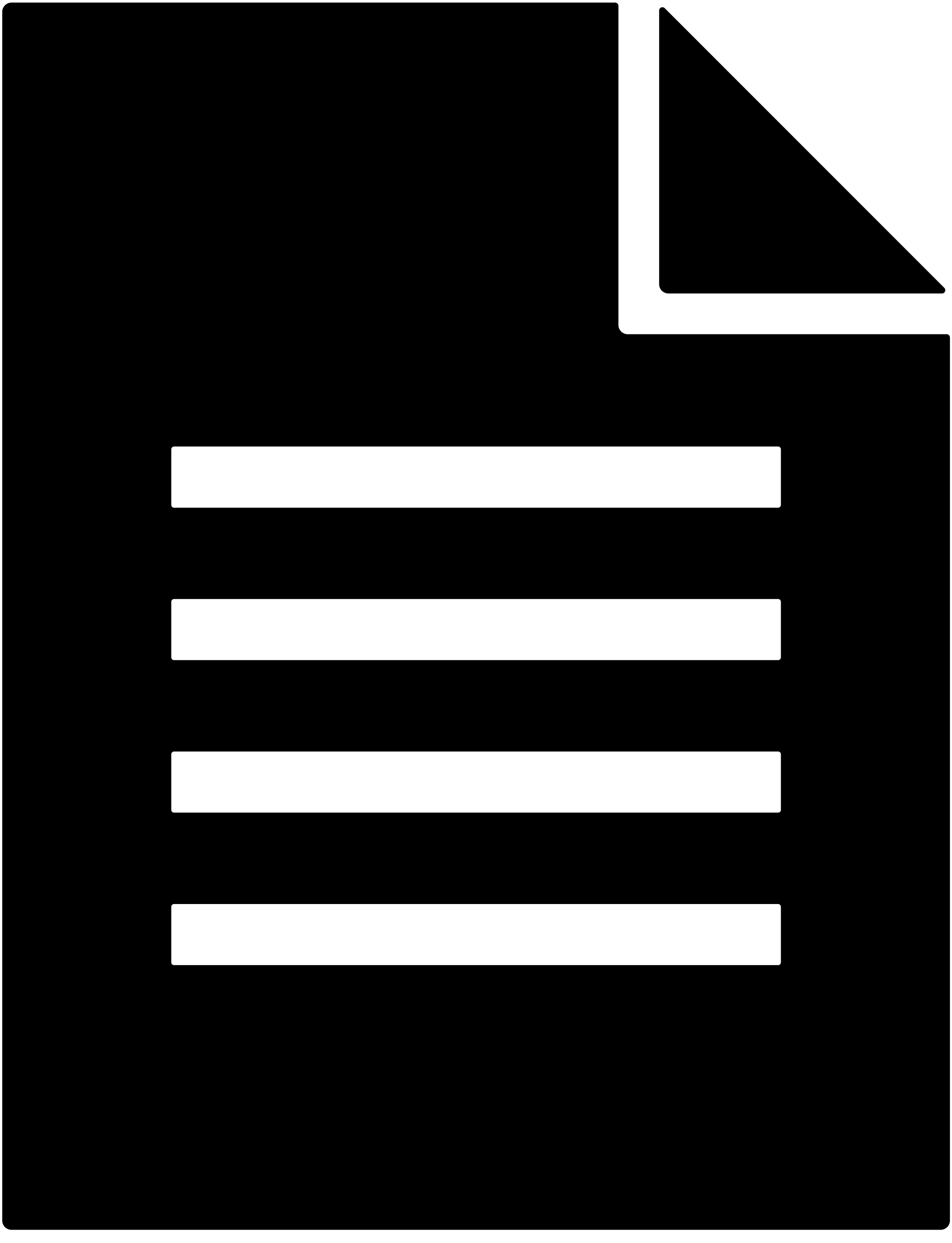
Fail!

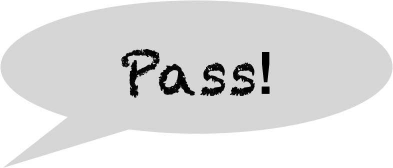
03





Verify(, ,)




Pass!

Desiderata

Security

Efficiency

k bits of (multi-user) security

preprocessing attacks

efficient signing/ verification

- The vast majority of real-world crypto systems use one of a handful of groups
- Adversary with nation-state level resources might spend a lot of time *precomputing hints* to help break protocols/ 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,
...

Auxiliary-Input Model

- Offline attacker $\mathcal{A}_{\mathsf{pre}}$ is unbounded and outputs an S-bit hint for online attacker $\mathcal{A}_{\mathsf{on}}$
- $\mathcal{A}_{\mathsf{on}}$ will try to win security games using the hint

of a handful of groups

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

- Adversary with nation-state level resources might spend solve hard problems using these building blocks

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

Short Signature Schemes:

iO-based

Short Schnorr

ECDSA

RSA-FDH

BLS

Schnorr

k bits of (multi-user) security

preprocessing attacks

efficient signing/
verification

short signatures