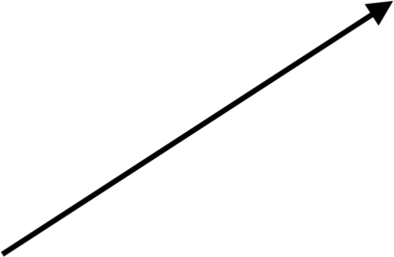
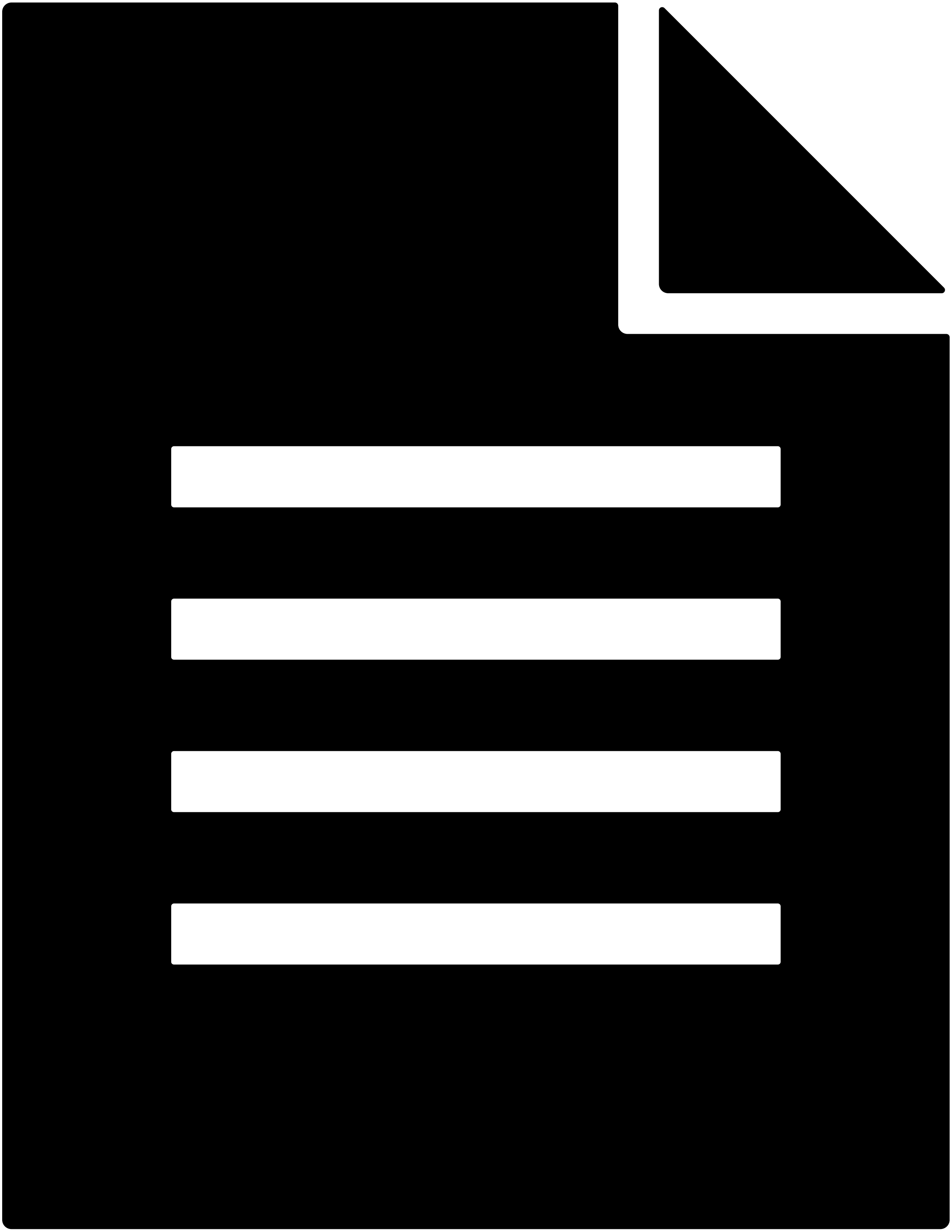
Verify(, ,)

Digital Signatures

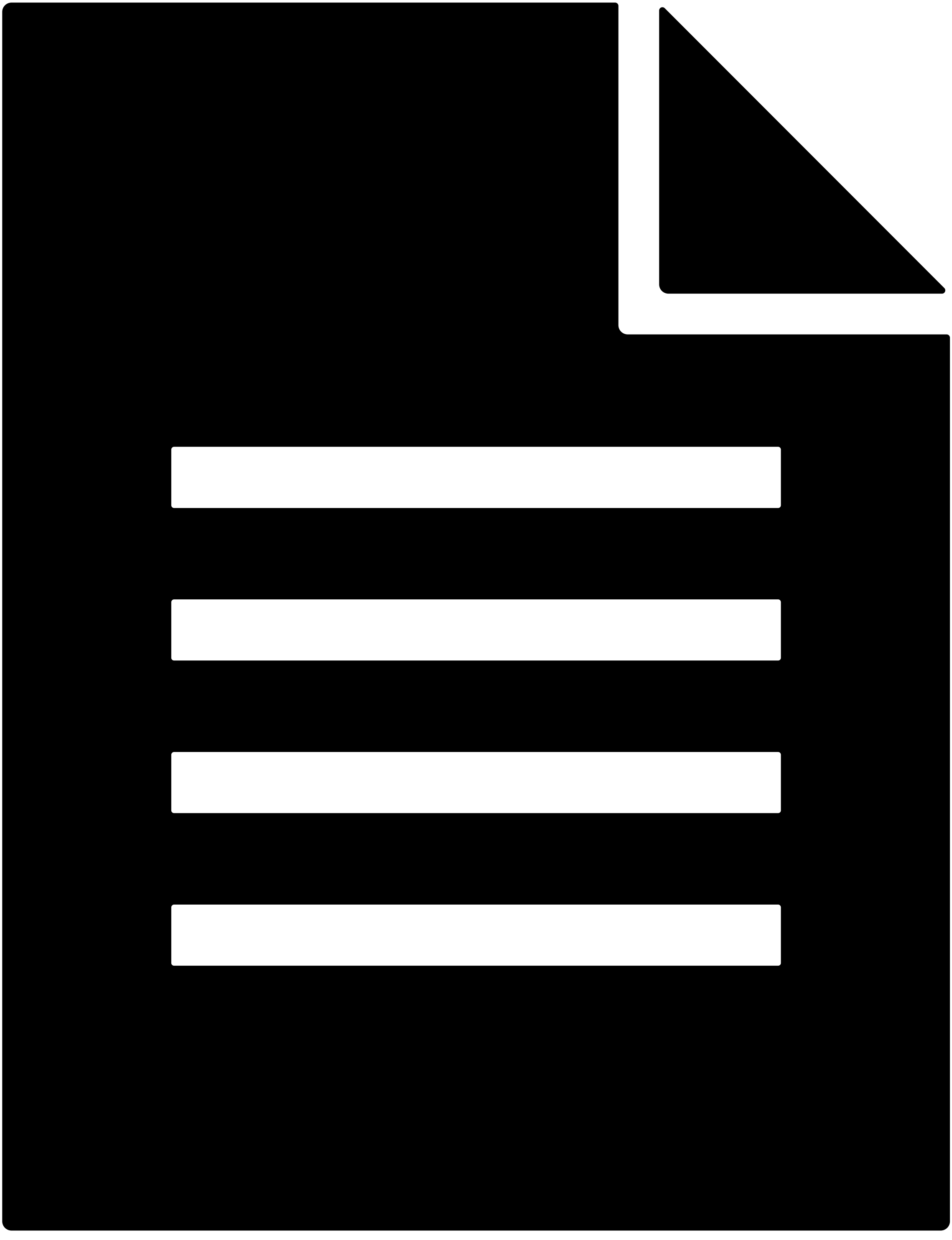
Fail!

03





Verify(, ,)



Pass!

Desiderata

Security

Efficiency

k bits of (multi-user) security

preprocessing attacks

efficient signing/
verification

short signatures

Short Signature Schemes:

RSA-FDH

ECDSA

Schnorr

Short Schnorr

BLS

iO-based

$\omega(k)$ bits

$4k$ bits

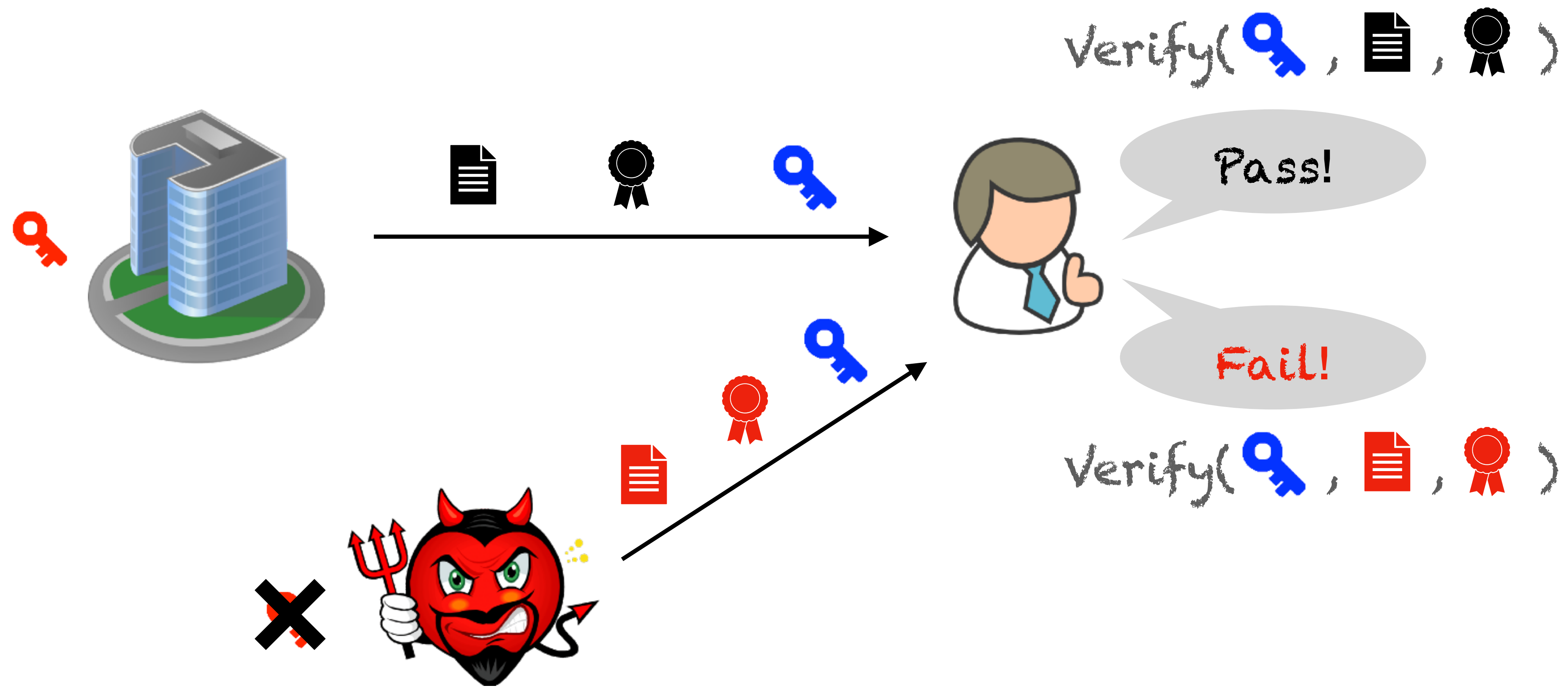
$4k$ bits

$3k$ bits

$2k$ bits

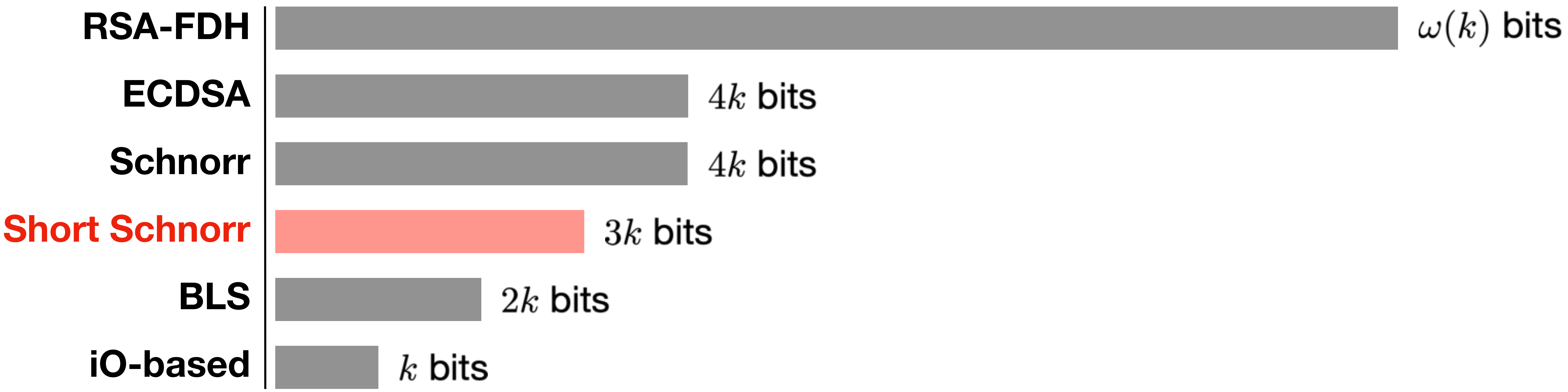
■ k bits

Digital Signatures



Desiderata	
Security	Efficiency
k bits of (multi-user) security	efficient signing/ verification
preprocessing attacks	**short signatures**

Short Signature Schemes:



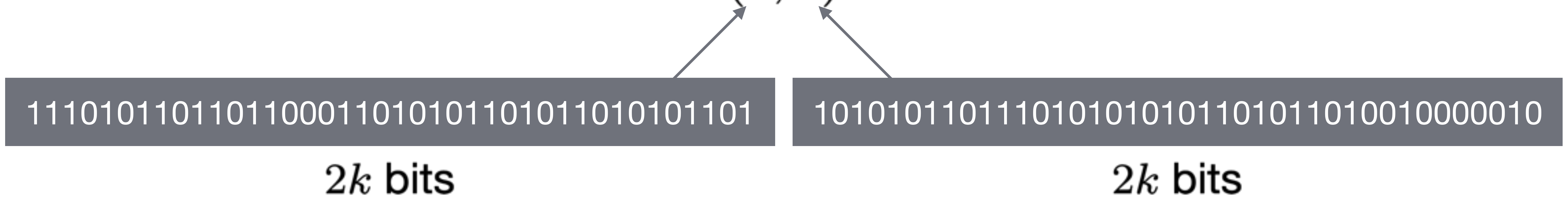
The (Short) Schnorr Signature Scheme

- **Public parameters:**
  - ▷ Group $G = \langle g \rangle$ of size $p \approx 2^{2k}$, where k is the security parameter
  - ▷ Hash function H : $\{0,1\}^* \to \mathbb{Z}_p$

```
Kg(1^k)
    $sk \leftarrow \mathbb{Z}_p$
    $pk \leftarrow g^{sk}$
    return $(pk, sk)$

Sign(sk, m)
    $r \xleftarrow{\$} \mathbb{Z}_p$; $I \leftarrow g^r$
    $e \leftarrow \mathsf{H}(I \| m)$
    $s \leftarrow r + sk \cdot e \mod p$
    return $\sigma = (s, e)$

Vfy(pk, m, σ)
    $R \leftarrow g^s \cdot pk^{-e}$
    if $\mathsf{H}(R \| m) = e$ then
        return 1
    else return 0
```



1110101101101100011010101101011010101101

$2k$ bits

1010101101110101010101101011010010000010

$2k$ bits