DIGITAL SIGNATURES

We defined signature schemes $\Pi = (KGen, Sign, Vrfy)$ and UF-CMA security.

FACT OWFs $\Rightarrow$ UF-CMA DS.

We focus on more practical constructions. The first one is based on RSA. (TDP)

$$f_{pk}(x) = x^e \bmod n \qquad f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$$

$$f_{sk}^{-1}(y) = y^{ed} \bmod n$$

The basic idea:

- Kgen: $pk = (n, e)$; $sk = (n, d)$ $\quad n = p \cdot q$

$$e \cdot d \equiv 1 \bmod (p-1)(q-1)$$

- Sign(m): $\sigma = m^d \bmod n \quad \left(f_{sk}^{-1}(m) \right)$

- Vrfy: $\sigma^e \stackrel{?}{=} m \bmod n \quad \left(f_{pk}(\sigma) \stackrel{?}{=} m \right)$

(m, σ)

Not secure! Forger: Pick any $\sigma \in \mathbb{Z}_n^*$. Let $m = \sigma^e \bmod n$.

Output (m, σ).

Better attack on RSA: I want to forge on $m^* \in \mathbb{Z}_n^*$.

I pick $m \in \mathbb{Z}_n^*$ and get $\sigma = m^d \bmod n$.

I compute $m \cdot m^* = m'$ and get $\sigma' = (m \cdot m^*)^d \bmod n$

Then $\sigma^* = \sigma^{-1} \cdot \sigma' = (m^*)^d \bmod n$.

The fix: FULL-DOMAIN HASH. (FDH).

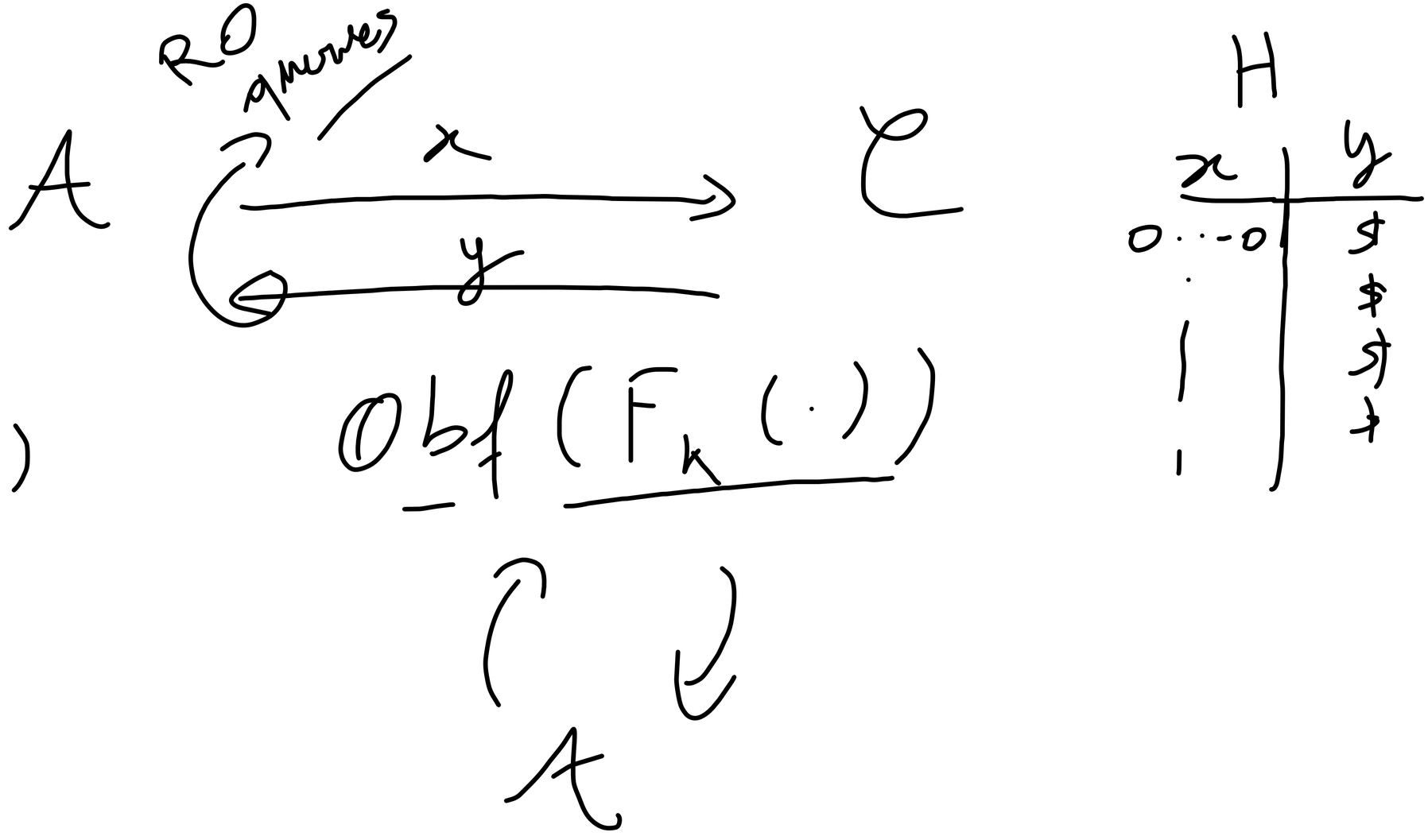
$$Sign(sk, m) = f_{sk}^{-1}(H(m)) \qquad \left(\sigma = (H(m))^d \bmod n\right)$$

$$Vrfy(pk, m, \sigma) = f_{pk}(\sigma) \stackrel{?}{=} H(m)$$

$H: \{0,1\}^* \to \mathbb{Z}_n^*$ $\qquad \left(\sigma^e \stackrel{?}{=} H(m) \bmod n\right)$

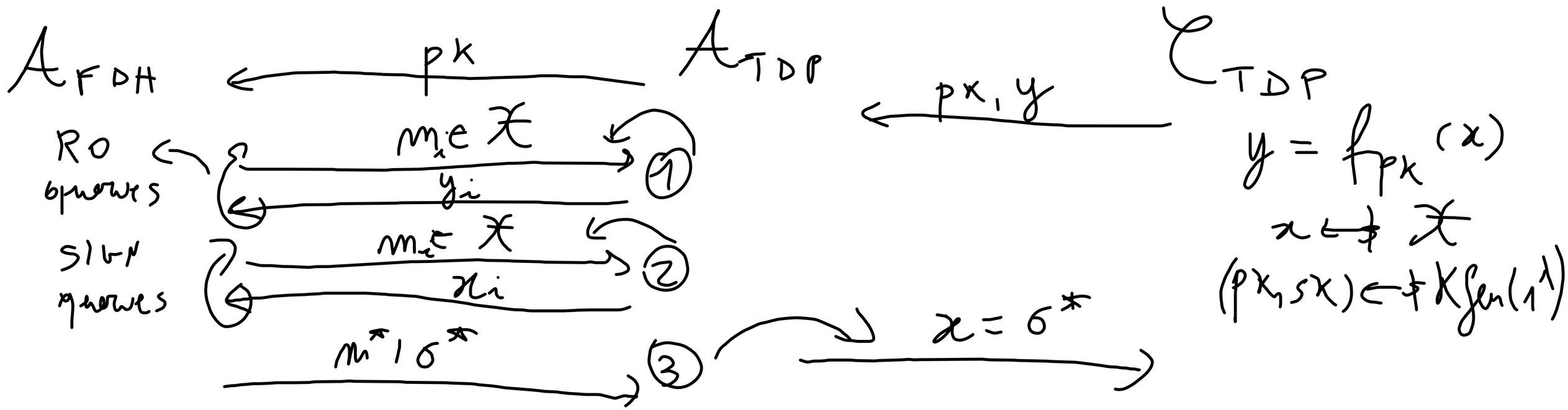
Provable security: It requires to model

H as a RANDOM ORACLE. (ROM)



THM FDH is UFCMA in the ROM assuming $(KGen, f, f^{-1})$ is a TDP (or RSA assumption).

Proof. Reduction to the TDP. But the reduction uses some "hacks".



Some assumptions (WLOG):

- Before asking signature on m_i, A_{FDH} asks RO query on m_i.
- If A_{FDH} forges on m^*, A_{FDH} asks m^* to RO. (Let i be the index s.t. $m_i = m^*$ to RO.)

Why WLOG? If A_{FDH} wins w.p. 1/poly without these queries, he also wins w.p. 1/poly by making these queries.

- It doesn't repeat queries.

The reduction picks $i \leftarrow\$ [q_h]$ where q_h is # of RO queries ($|poly(\lambda)$).

① RO queries. Upon $m_i \in \{0,1\}^*$:

- If $i \neq j$, "program" the RO by picking $x_i \leftarrow\$ \mathcal{X}$ and $y_i = f_{pk}(x_i)$ and return $y_i \left(= H(m_i)\right)$
- If $i = j$, then $y_i = y$. This means $H(m_j) \overset{!}{=} y$

② Upon SIGN query $m_i \in \{0,1\}^*$

return x_i as in ①. If $m_i = m_j$ ABORT.

③ Upon forgery (m^*, σ^*) output to challenger $x = \sigma^*$.

Good simulation: RO queries are simulated with random values. SIGN queries are also good because x_i is the pre-image of $y_i = H(m_i)$

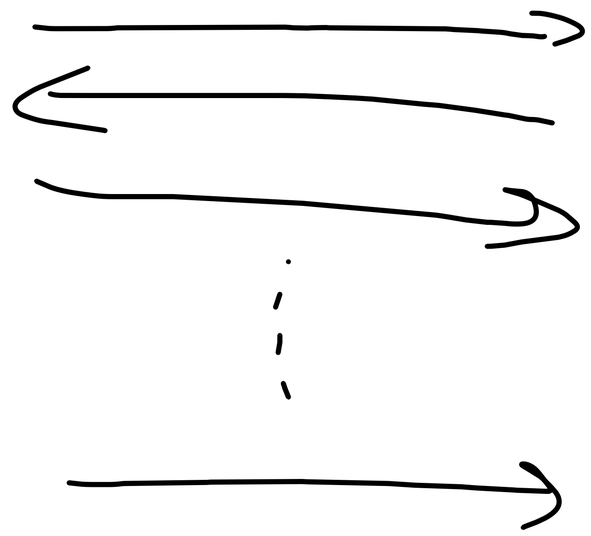
So $f_{pk}(y_i) = H(m_i)$ ✓ ↗ $m_j = m^*$

Forgery: w.p. $1/poly$ the guess on j is correct;

w.p. $1/poly$ σ^* is pre-image of $H(m^*) = y$. ▨

IDENTIFICATION SCHEMES

Alice $\mathcal{P}_{(pk,sk)}$ Bob $\mathcal{V}_{(pk)}$



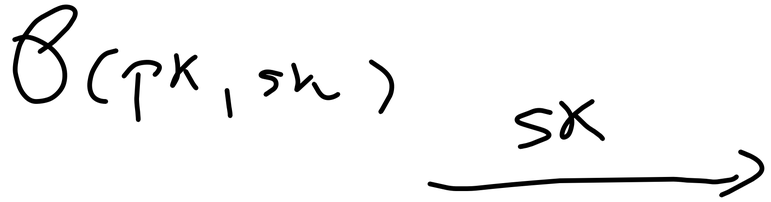
Way to convince Bob a statement is true by a protocol.

"I Know sk corresponding to pk".

Two properties:

- SOUNDNESS: $\mathcal{P}^*$ not knowing sk cannot convince Bob.

- ZERO-KNOWLEDGE: Protocol reveals nothing on sk.



NOT ZERO KNOWLEDGE!

Check pk, sk "correct"

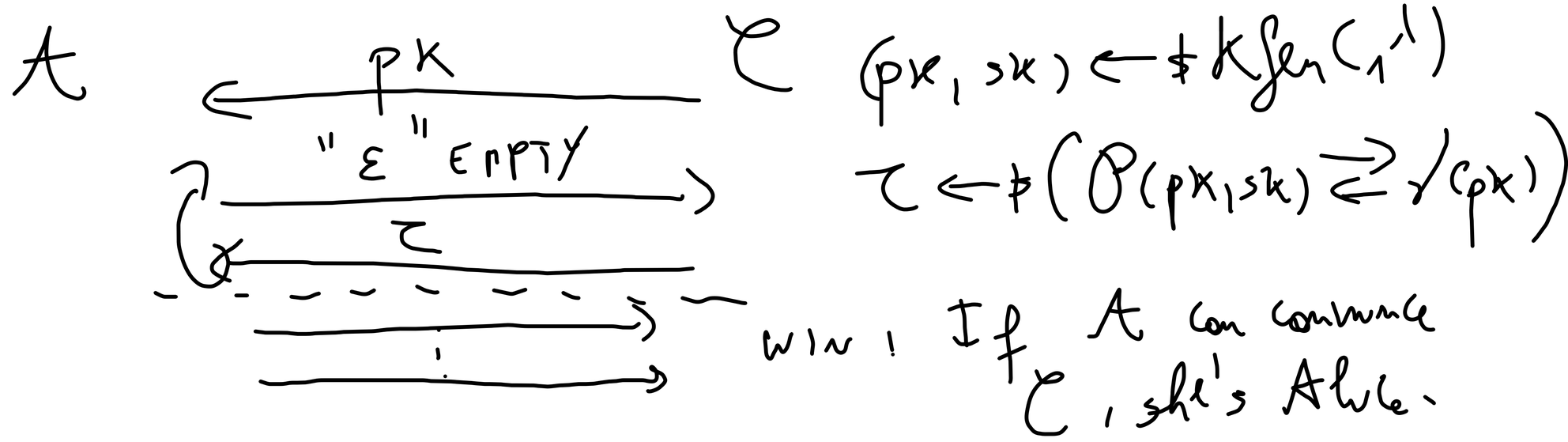
$\mathcal{P}(pk, sk)$ $\qquad$ $\mathcal{V}(pk)$

$\sigma = Sign(sk, m)$ $\xleftarrow{\quad m \quad}$ $m \leftarrow\!\$\ \mathcal{M}$

$\xrightarrow{\quad \sigma \quad}$ $Vrfy(pk, m, \sigma) \stackrel{?}{=} 1$

For us: Only focus on PASSIVE SECURE ID schemes.

DEF. $\Pi = (KGen, \mathcal{P}, \mathcal{V})$ is PASSIVELY secure if



$$Out(A(pk) \rightleftarrows \sqrt{(pk)}) = 1$$