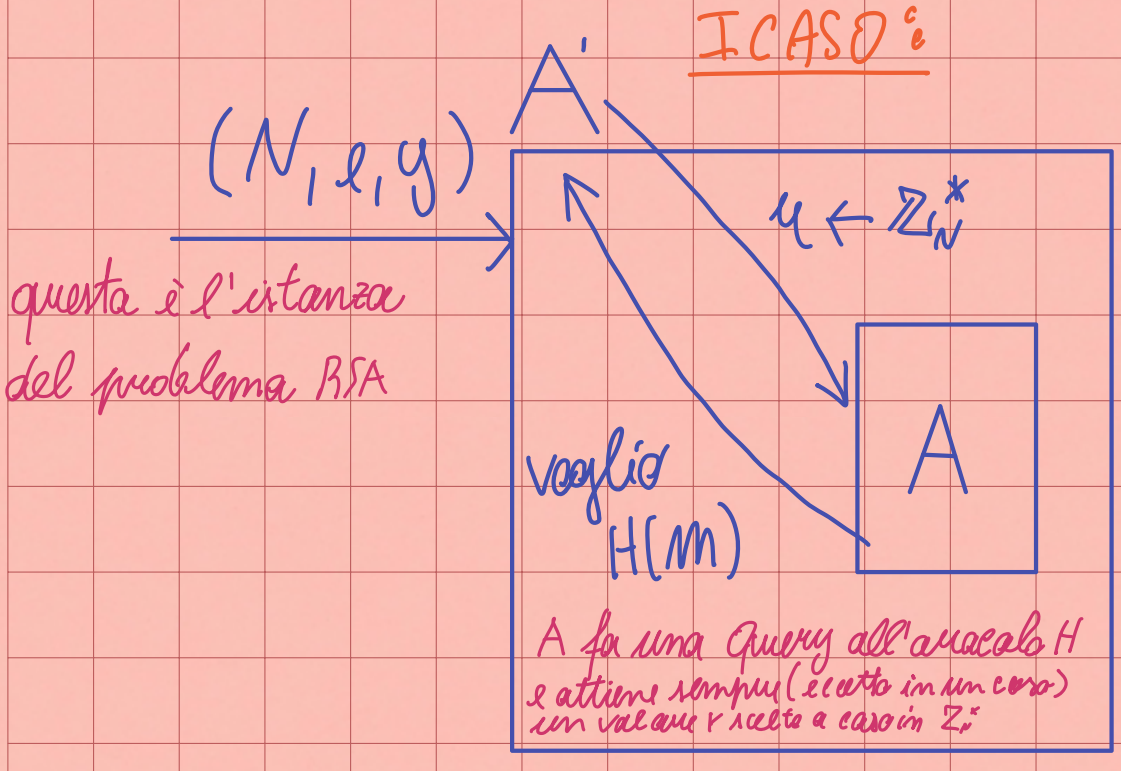
è un ROM $\Rightarrow$ RSA-FDH è sicuro.

A' vuole risolvere il problema RSA.

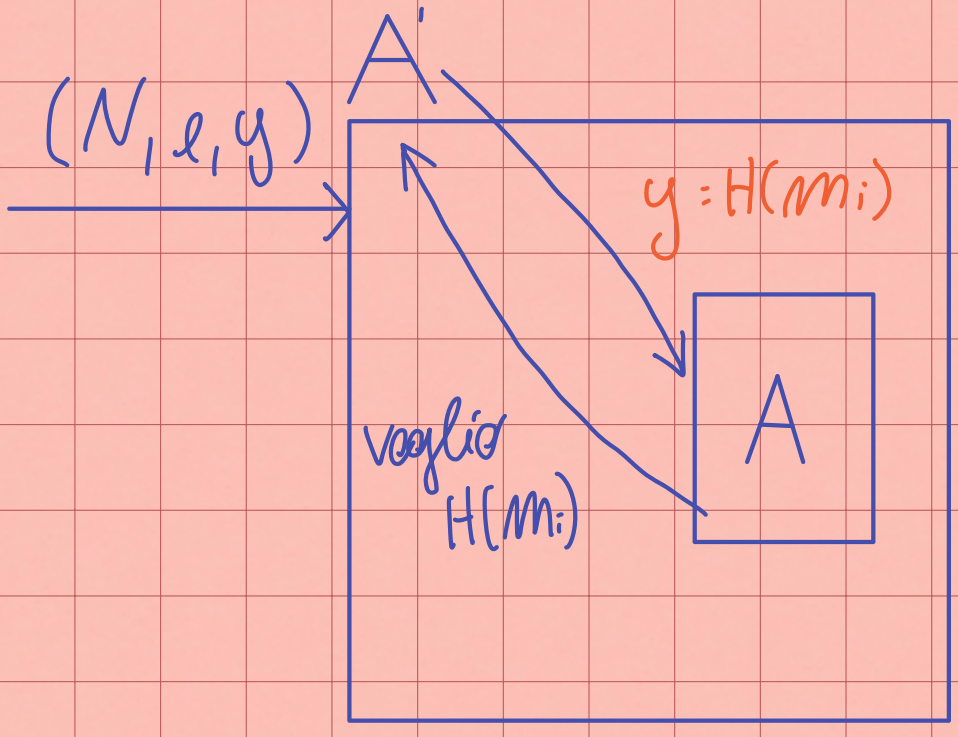
A vuole vincere nell'esperimento $Sig\text{-}forge^{(n)}_{A,\Pi}$ vuol dire che vuole trovare quell'x t.c. $x^e \equiv y \bmod N$ cioè in sostanza, la pre-immagine di y.

2 CASI POSSIBILI:

- CASO IN CUI A QUERY SOLO H
- CASO IN CUI A QUERY ANCHE $SIGN_{SK}(\cdot)$



nell' i-esima query da parte di A:



A' scommette che per l'i-esima query di A, esso riesca a produrre una falsificazione.
La scommessa di A' è rappresentata dal fatto che per un m_i A' invia ad A il valore y al posto di un $r \in \mathbb{Z}_N^*$ a caso.

Se A trova una falsificazione significa che riesce a trovare quel σ tale che:

$$\sigma^e = H(m_i) \bmod N$$

ma dato che $H(m_i) = y$, A ha trovato in

pratica quell' x t.c. $x^e = y \bmod N$, cioè l'inversa RSA.

CONSIDERAZIONI:

- y è un valore casuale perché nell'esperimento RSA esso veniva scelto unif. a caso in $\mathbb{Z}_N^*$
- y valori $H(m_j)$ vengono scelti a caso in $\mathbb{Z}_N^*$ perché H è un ROM

Di conseguenza la prob. che A produca una contraffazione sul messaggio i-esimo m_i è $1/q$. Pertanto:

se A è efficiente A' inverte RSA in maniera efficiente; ma RSA è difficile e ciò è impossibile.

II CASO

A' deve simulare l'oracolo H, ma non conosce d, quindi non sa come produrre firme

$$\sigma = H(m)^d \bmod N$$

deve dare in risposta alle query di A.

A' per simulare la firma deve in output una tripla $(m_j, \sigma_j, \sigma_j^e)$ dove

- m_j è la query
- σ_j è $H(m)^d$
- σ_j^e è $H(m)$