Teorema: RSA difficile ed H ROM allora KEM su RSA è CCA sicuro

# Background:

**COSTRUZIONE KEM SU RSA (ROM):**

$\Pi = (Gen, Encaps, Decaps)$

1. $Gen: (N, e, d) \leftarrow GenRSA(1^n)$

   $H: \mathbb{Z}_N^* \rightarrow \{0,1\}^n$

   $PK = \langle N, e \rangle \quad SK = \langle N, d \rangle$

2. $Encaps: c = r^e \bmod N \leftarrow Encaps_{PK}(1^n)$

   $K = H(r)$ con $r \in \mathbb{Z}_N^*$ e con il vincolo $lsb(r) = m$

3. $Decaps: r = c^d \bmod N = Decaps(c)$

   $K = H(r)$

$KEM^{CCA}_{A,\Pi}(n)$:

1. C run $(PK, SK) \leftarrow Gen(1^n)$
2. $(c, K) \leftarrow Encaps_{PK}(1^n)$
3. C $b \leftarrow \{0,1\}$ e

   if $b = 0$

   $\hat{K} := K$

   else

   $\hat{K} \leftarrow \{0,1\}^n$
4. A riceve $(c, \hat{K}, PK)$ e l'accesso a $Decaps_{SK}(\cdot)$. Da in output $b'$.

   se $b' = b$ allora C out 1 else 0.

# DIMOSTRAZIONE:

Siano:

- QUERY = "A query r ad H"
- SUCCESS = "$b = b'$"

$$Pr[SUCCESS] = Pr[SUCCESS \wedge \overline{QUERY}] + Pr[SUCCESS \wedge QUERY]$$

$$\leq$$

$$Pr[SUCCESS \wedge \overline{QUERY}] + Pr[QUERY]$$

dimostreremo che questa somma vale $1/2 + negl(n)$

# PROVO IL PRIMO PEZZO:

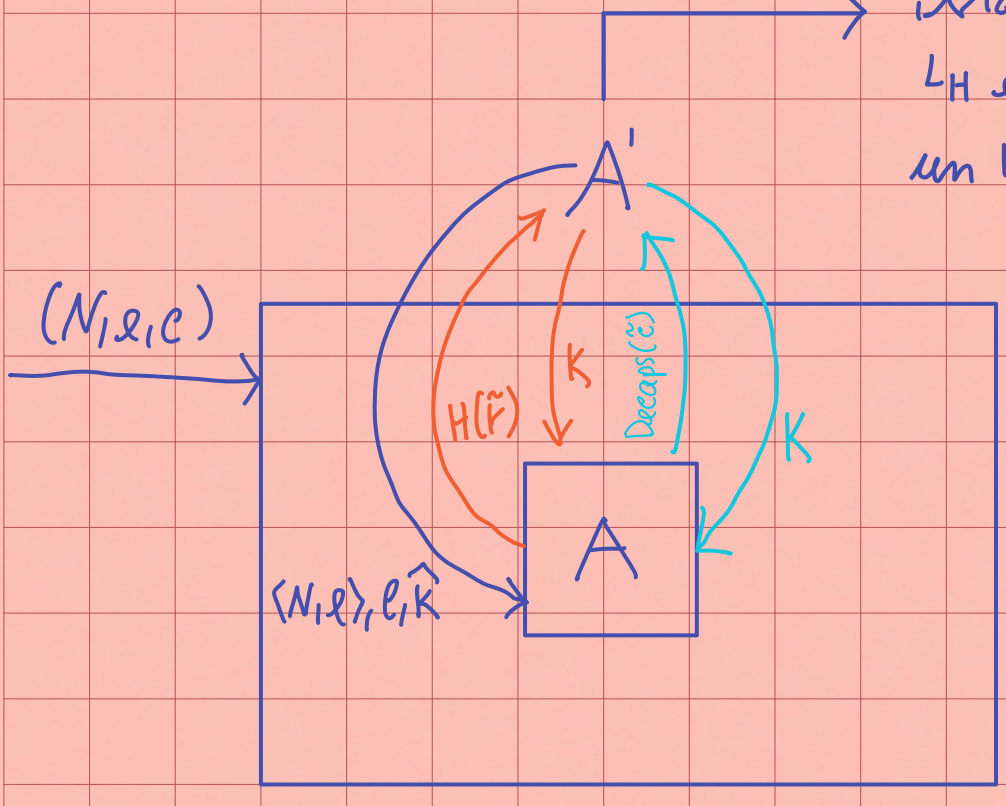
$$Pr[SUCCESS \wedge \overline{QUERY}] = Pr[\overline{QUERY}] \cdot Pr[SUCCESS \mid \overline{QUERY}]$$

- $Pr[\overline{QUERY}]$ può essere
  - $= 0$ da cui sapremmo in automatico che $Pr[SUCCESS \wedge \overline{QUERY}] = 0$
  - $> 0$ da cui $Pr[SUCCESS \wedge \overline{QUERY}] \leq Pr[SUCCESS \mid \overline{QUERY}]$

- $Pr[SUCCESS \mid \overline{QUERY}] = 1/2$

  fino a quando QUERY non si verifica, $K = H(r)$ è distribuito uniform. a caso.

# PROVO IL SECONDO PEZZO




istanzia due liste:

$L_H$ ed $L_{DECAPS}$ poi sceglie un $K \leftarrow \{0,1\}^m$ ed inserisce in $L_{DECAPS} \leftarrow (c, K)$

poi sceglie $b \leftarrow \{0,1\}$

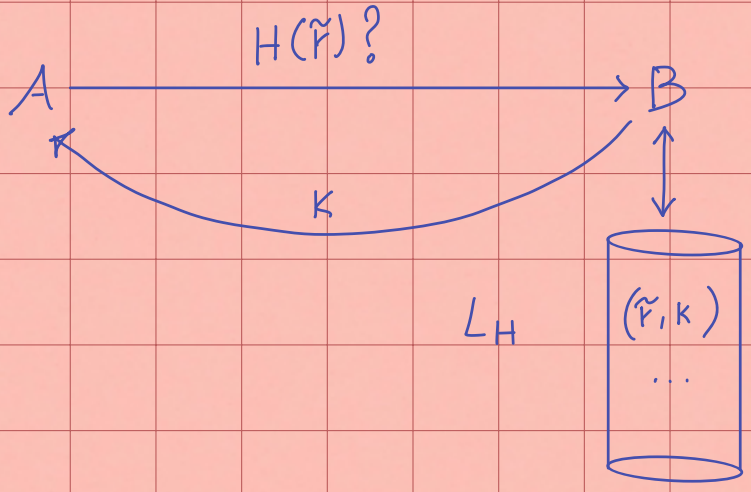
if $b = 0$

$\hat{K} := K$

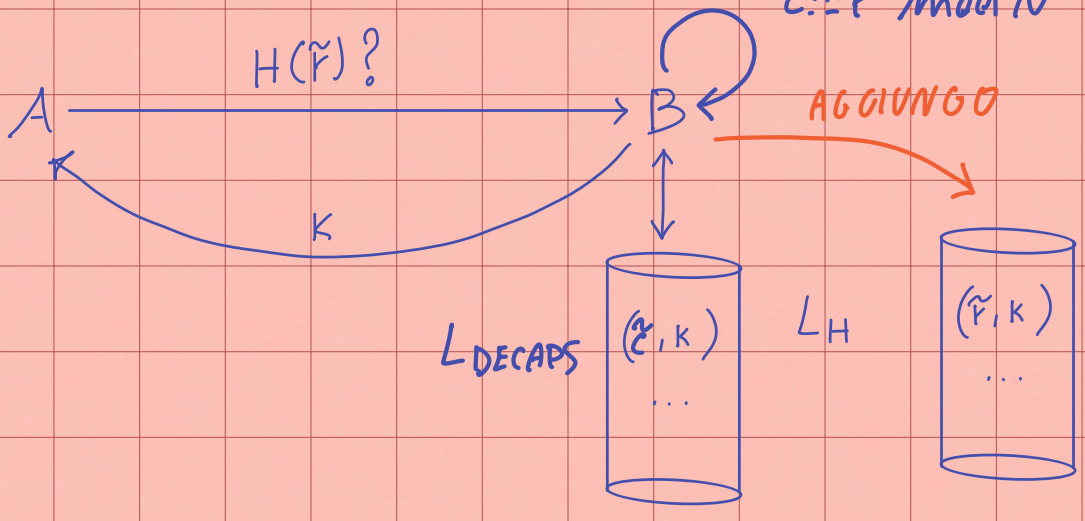
else $\hat{K} \leftarrow \{0,1\}^m$

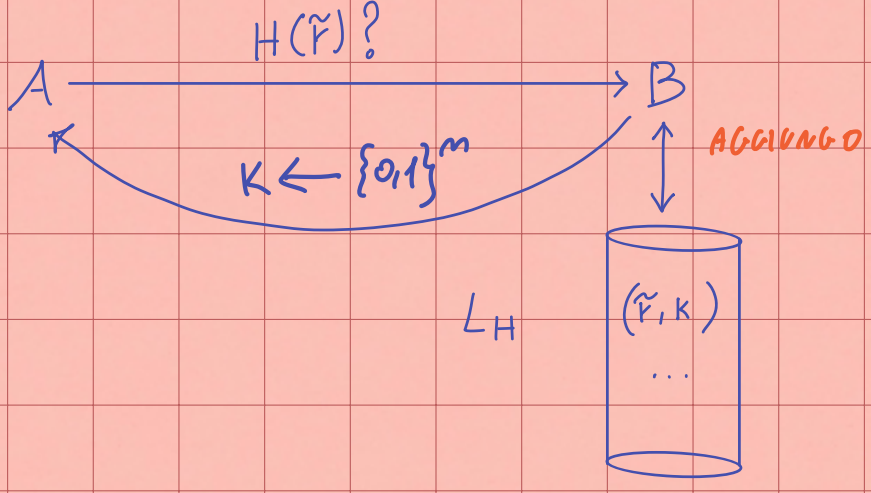
# CASO 1 (query solo per H)

(a)




(b)




il caso in cui A fa query anche a $Decaps_{SK}(\cdot)$ è speculare a questo.

Alla fine dell'esecuzione di $A_1$, se c'è un entry $(t, K)$ in $L_H$ per cui $t^e = c \bmod N$ ritorna $t$

A' dà in output una soluz corretta quando QUERY si verifica, ma dato che RSA è difficile allora $Pr[Query] \leq negl$