Teorema 3.18:

Se $G$ è un PRG, la costruzione 3.17 realizza uno schema di cifratura a chiave privata per messaggi di lunghezza fissa che ha cifrati indistinguibili in presenza di un eavesdropper.

Dim:

Facciamo vedere che $\forall$ Adv $A$ PPT $\exists$ negl$(n)$ t.c.

$$P_r[PrivK^{eav}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$

(3.17)

COSTRUIAMO LA RIDUZIONE:

PROBLEMA X: D (Distinguisher) vuole distinguere $G(k)$ da $r$ utilizzando A che supponiamo in grado di distinguere quale tra i mex. $m_0$ ed $m_1$ è stato cifrato.

La prob. di successo di D è $\frac{1}{p(n)}$ mentre quella di A è $\varepsilon(n)$. La prob. di successo di D nel raggiungere il proprio scopo è legata alla prob. di successo di A.

$\frac{\varepsilon(n)}{p(n)} \Rightarrow$ Se A è PPT allora D è PPT.

Distinguisher D:

Riceve in input una stringa $w \in \{0,1\}^{\ell(n)}$

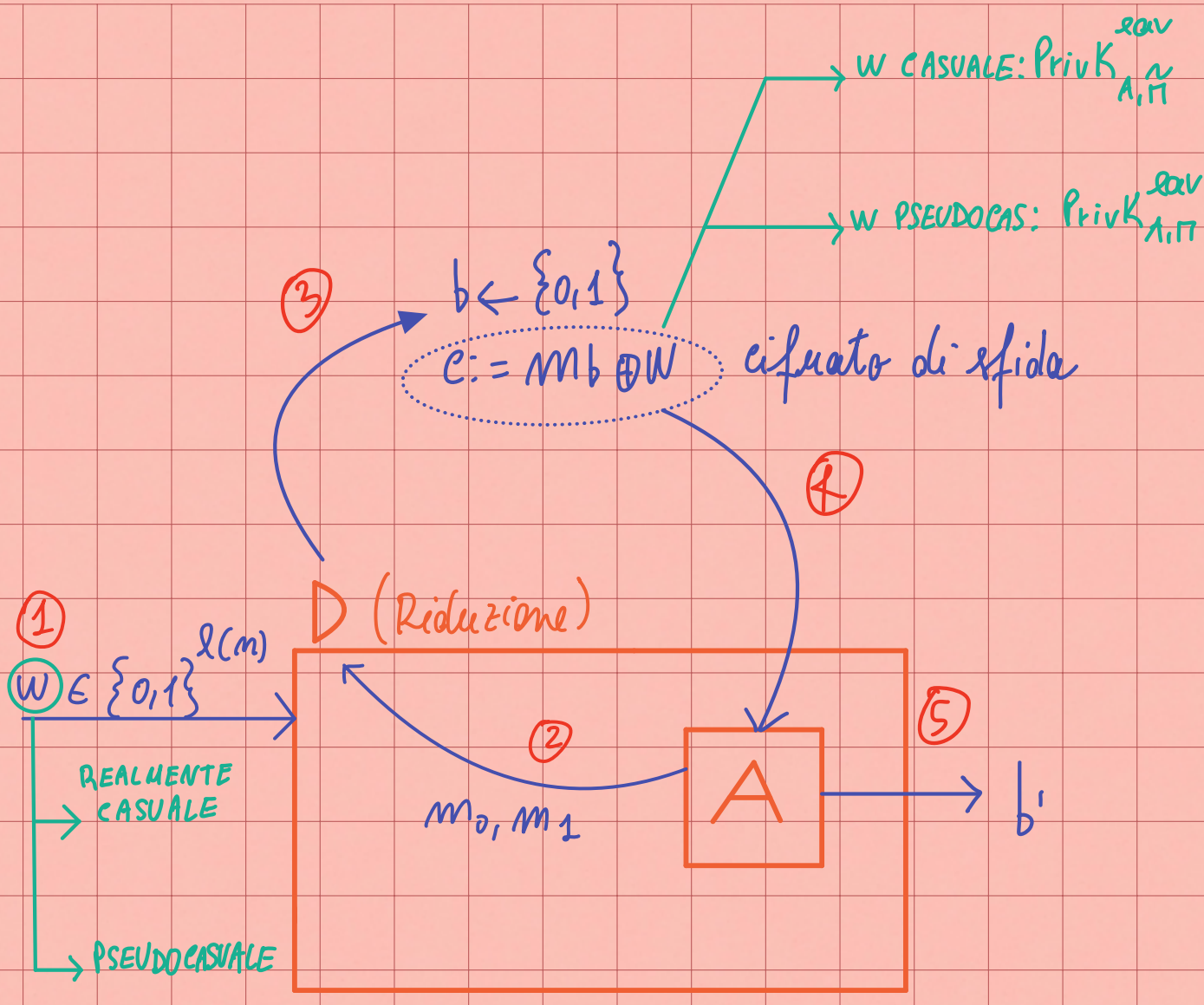
D, adesso finge di essere il challenger in modo da far percepire ad A di stare giocando nell'esperim.

1) Esegue $A(1^n)$ ottenendo $m_0, m_1 \in \{0,1\}^{\ell(n)}$

2) Sceglie $b \leftarrow \{0,1\}$ e pone $c := m_b \oplus w$

3) da c ad A ed ottiene da A il bit b'

4) se $b' = b$ da in output 1 (w è pseudocasuale); altrimenti, da in output 0 (w è Tot. casuale).




Consegue che:

- Se $w$ è Tot. uniforme, A pensa di giocare nell'esp. $PrivK^{eav}_{A,\tilde{\Pi}}$ dove $\tilde{\Pi}$ è lo schema one-Time pad.

$$Pr_{w \leftarrow \{0,1\}^{l(n)}}[D(w)=1] = Pr[PrivK^{eav}_{A,\tilde{\Pi}}(n)=1] = 1/2$$

- Se $w$ è Pseudocasuale, A pensa di giocare nell'esp. $PrivK^{eav}_{A,\Pi}$. In questo caso D ha successo se A ha successo, quindi

$$Pr_{w \leftarrow \{0,1\}^{\ell(n)}}[D(w)=1] = Pr[PrivK^{eav}_{A,\Pi}(n)=1]$$

Se questa prob. fosse non-negl(n) allora:

$$Pr\ caso\ 1 - Pr\ caso\ 2 =$$

$$1/2 - (1/2 + non\text{-}negl(n)) =$$

$$NON\text{-}negl(n)!$$

Significherebbe che D riesce a capire con una prob. non trascurabile quando w è generata da G(K). Questo però invalida l'ipotesi che G è un PRG, in quanto una delle condizioni per essere un PRG è che l'output che genera deve essere indistinguibile da una stringa tot. casuale.

Quindi $Pr[PrivK^{eav}_{A,\Pi}(n)=1] \leq \frac{1}{2} + negl(n)$

caso 1: con $\tilde{\Pi}$ $A \rightarrow \varepsilon(n) = \frac{1}{2}$ $\Rightarrow \frac{\varepsilon(n)}{P(n)}$ trasc.

caso 2: con $\Pi$ $A \rightarrow \varepsilon(n) = 1/2 + negl$ $\Rightarrow \frac{\varepsilon(n)}{P(n)}$ trasc.