Se RSA difficile allora Costruzione cifratura a chiave pubblica RSA con predicato hard core è CPA sicura.

Sia A un Adv PPT in $PubK^{eav}_{A,\Pi}(n)$ t.c. ha prodotto m_0, m_1

$$Pr[PubK^{eav}_{A,\Pi}(n)=1] = \frac{1}{2} Pr[A(N,e,c)=0 \mid c \text{ cifrato di } m_0] + \frac{1}{2} Pr[A(N,e,c)=1 \mid c \text{ cifrato di } m_1]$$

(PK; cifrato di m_0 o di m_1)

ho esplicitato cosa significa per A vincere nell'esperimento $PubK^{eav}_{A,\Pi}(n)$.

Consideriamo adesso per un attimo A che gioca in quest'altro esperimento:

$$Pr[RSA\text{-}lsb_{A,GenRSA}(n)=1] = \frac{1}{2} Pr[A(N,e,x^e \bmod N)=0 \mid lsb(x)=0] + \frac{1}{2} Pr[A(N,e,x^e \bmod N)=1 \mid lsb(x)=1]$$

(PK; cifrato di 0 o di 1)

c'è evidentemente una uguaglianza tra i due esperimenti:

$$Pr[A(N,e,c)=b \mid c \text{ cifrato di } b] = Pr[A(N,e,x^e \bmod N)=b \mid lsb(x)=b]$$

che per le uguaglianze viste significa

$$Pr[PubK^{eav}_{A,\Pi}(n)=1] = Pr[RSA\text{-}lsb_{A,GenRSA}(n)=1]$$

avendo supposto $lsb(x)$ essere un predicato Hard-Core significa che:

$$\exists\ negl(n) \text{ t.c. } Pr[RSA\text{-}lsb_{A,GenRSA}(n)=1] \leq \frac{1}{2} + negl(n)$$

e quindi automaticamente:

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