Se uno schema di codifica Π è sicuro rispetto a $PubK^{eav}_{A,\Pi}(n)$, allora lo è anche rispetto a $PubK^{mult}_{A,\Pi}(n)$

In breve: si espande $PubK^{mult}$ con 0, 0 = 0 + 1, 1 = 1. Poi si dimostra (costruendo un avversario) che $\frac{1}{2}+ngl(n) \geq$ 0, 0 = 0 + 0, 1 = 1 e di conseguenza $\frac{1}{2}+ngl(n) \geq$ 0, 1 = 0 + 1, 1 = 1 così facendo vale che: $1+ngl(n) \geq$ 0, 0 = 0 + 1, 1 = 1 + 0, 1 = 0 + 0, 1 = 1 $\rightarrow$ 0, 0 = 0 + 1, 1 = 1 + $\frac{1}{2}$

Si considera prima di tutto $t = 2$ ovvero due codifice per ogni vettore di messaggi, anche se questo valore può essere arbitrario. Vogliamo scoprire se $\epsilon(n)$ è trascurabile o meno nella disequazione:

$$Pr(PubK^{mult}_{A,\Pi}(n) = 1) \ \leq \ \frac{1}{2} + \epsilon(n)$$

$$Pr(PubK^{mult}_{A,\Pi}(n) = 1) = \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_0)) = 0) + \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_1), Enc_{pk}(m^2_1)) = 1)$$

Prima di tutto dimostriamo che esiste una funzione trascurabile tale che:

$$\frac{1}{2} + negl(n) \ \geq \ \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_0)) = 0) + \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_1)) = 1)$$

Nell'esperimento *mult* il secondo elemento avrà probabilità 0 in quanto non è mai possibile si verifichi lo scenario in cui è dato un misto di elementi del primo e del secondo vettore all'avversario. Tuttavia è possibile costruire un avversario A' che permette alla disequazione di risultare vera. Nell'esperimento $PubK^{eav}_{A,\Pi}(n)$ quando $b = 0$ ad A' costruitogli attorno viene passato $Enc_{pk}(m^2_0)$:

$$Pr(A'(Enc_{pk}(m^2_0)) = 0) = Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_0)) = 0)$$

Quando invece nell'esperimento $PubK^{eav}_{A,\Pi}(n)$, $b = 1$ ad A' viene passato $Enc_{pk}(m^2_1)$:

$$Pr(A'(Enc_{pk}(m^2_1)) = 1) = Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_1)) = 1)$$

Avendo assunto che Π sia sicuro è necessario che (dato μ trascurabile):

$$\frac{1}{2} + \mu(n) \ \geq \ Pr(PubK^{eav}_{A',\Pi}(n) = 1) =$$

$$\frac{1}{2} \cdot Pr(A'(Enc_{pk}(m^2_0)) = 0) \ + \ \frac{1}{2} \cdot Pr(A'(Enc_{pk}(m^2_1)) = 1) =$$

$$\frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_0)) = 0) \ + \ \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_1)) = 1)$$

Dimostrando che il $negl(n)$ in cima è trascurabile. Nello stesso modo si può dimostrare la presenza di una funzione trascurabile anche per:

$$\frac{1}{2} + negl(n) \ \geq \ \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_1), Enc_{pk}(m^2_1)) = 1) + \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_1)) = 0)$$

Sommando le espressioni di queste due affermazioni e sonsiderando che la somma di due espressioni trascurabili è anch'essa trascurabile, è possibile trovare una funzione trascurabile tale che:

$$1 + negl(n) \ \geq$$

$$\frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_0)) = 0) + \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_1), Enc_{pk}(m^2_1)) = 1) +$$

$$\frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_1)) = 0) + \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_1)) = 1) \ =$$

$$\frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_0), Enc_{pk}(m^2_0)) = 0) + \frac{1}{2} \cdot Pr(A(Enc_{pk}(m^1_1), Enc_{pk}(m^2_1)) = 1) \ + \ \frac{1}{2}$$

Ciò implica che (dove $\epsilon(n) = negl(n)$):

$$\frac{1}{2} + \epsilon(n) \ \geq \ Pr(PubK^{mult}_{A,\Pi}(n) = 1)$$

Completando la dimostrazione.