

Teorema 3.31: Se F è pseudocasuale, allora la costruzione 3.30 realizza uno schema di cifratura CPA-sicuro per messaggi di lunghezza n

PROCEDIMENTO DELLA DEMOSTRAZIONE:

Nota: per provare la sicurezza di schemi che fanno uso di funzioni pseudocasuali (PRF) si procede di solito in due fasi:

I FASE: consideriamo \tilde{f} dove al posto di f_K chiamiamo f realmente casuale.) ①
Mostriamo che questa modifica non influenza sulla probabilità di vittoria di A .) ②

II FASE: Analizziamo Π che utilizza F_K

I FASE

Dimostrazione:

1

Definiamo $\tilde{\Pi}$:

Sia $\tilde{\Pi} = (\tilde{G}_m, \tilde{E}_m, \tilde{D}_m)$ costituita partire da $\Pi = (G_m, E_m, D_m)$ t.c. :

- $\tilde{\Pi}$ usa $F \in \text{Fun}_m$ scelta unif. a caso.
- Π usa F_K con K scelto unif. a caso.

* $\tilde{\Pi}$ non è efficiente perché f ha lunghezza esponenziale $2^{2^m \cdot m}$ e dunque richiede spazio di memorizzazione esponenziale.

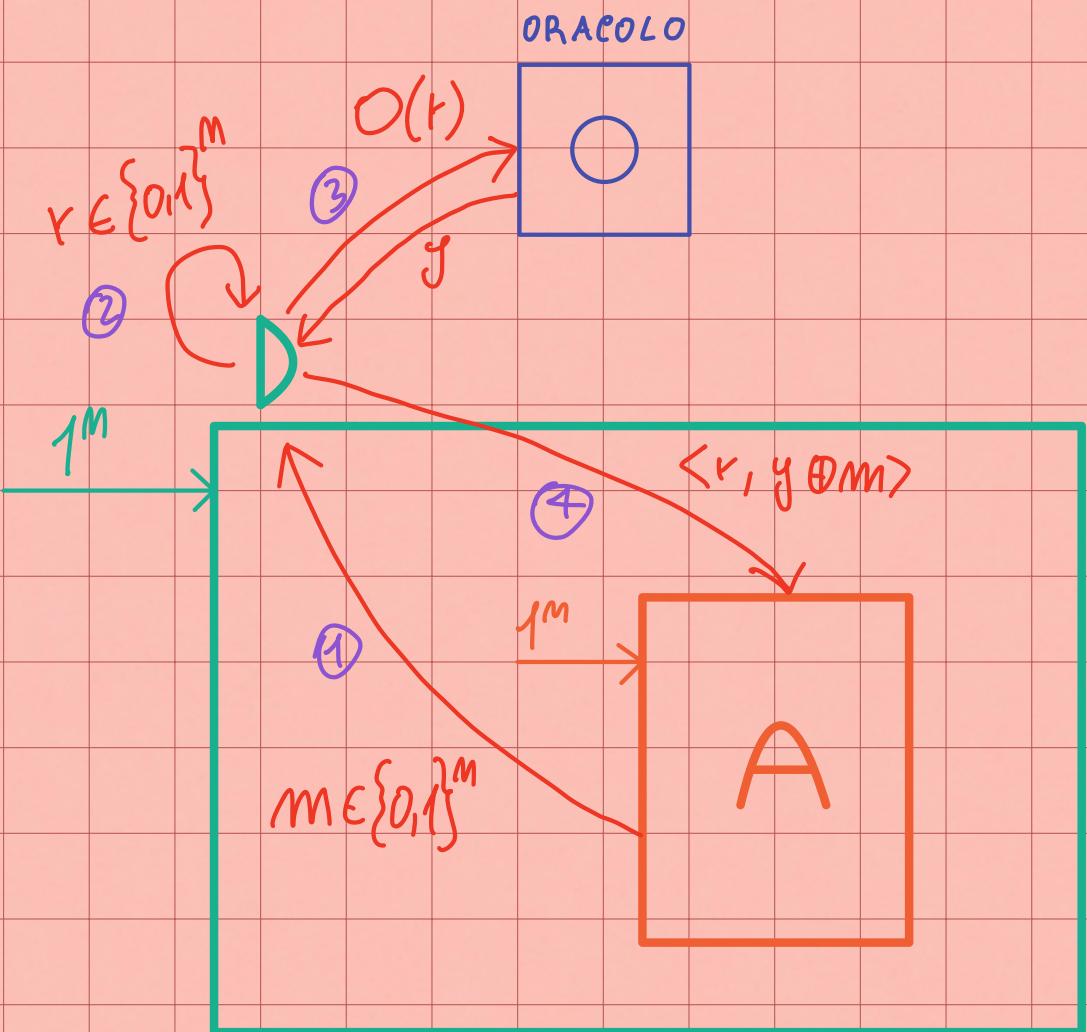
2

Sia A un Adv PPT e $q(n)$ il limite polinomiale superiore al n. di query che può fare al suo avversario per chiedere il cifrato di messaggi alla sua scelta. Mostriamo che

$$\Pr[\text{Priv}_{A, \tilde{\Pi}}^{epa}(n) = 1] - \Pr[\text{Priv}_{A, \Pi}^{epa}(n) = 1] \leq \text{negl}(n)$$

Per dimostrare questa cosa proceediamo per riduzione

DISTINGUISHER D:



- ① A richiede la cifratura di un messaggio lungo m
- ② D deve generare il PAD e può farlo genera un racaro ed ottiene il PAD attraverso l'oracle $O(r)$
- ③ Ottenuto il PAD y , estruisco l'output per A
- ④ Invia $\langle r, y \oplus m \rangle$

In particolare, $O(r)$ usa σF_k oppure F_k !!

- A può chiedere cifrature di m nel modo di cui sopra
- A dà in output quindi $m_0, m_1 \in \{0,1\}^m$.
Il challenge (che in questo caso è D) sceglie $b \leftarrow \{0,1\}$ e cifra m_b in questo modo:
 - $r \leftarrow \{0,1\}^m$
 - Runna O(r) ed ottiene y
 - Da in output il cifrato di sfida $\langle r, y \oplus m_b \rangle$
- A può continuare ad effettuare quei fine a quando non decide di dare in output b' .
- Se $b' = b$ A ha vinto.

La prob. che A vince è $E(n)$, quella di D è $\frac{1}{p(n)}$. Le prob. sono legati, quindi la prob. di distinguere F_k da F_1

$$\frac{E(n)}{p(n)} \leftarrow A$$

$$\frac{p(n)}{p(n)} \leftarrow D$$

Quindi D è PPT se A è PPT. per le proprietà delle funz. negl(n) dice:

$\frac{\epsilon(n)}{p(n)}$ è negl(n) $\Leftrightarrow \epsilon(n) e p(n)$ sono negl(n)

altrimenti $\epsilon(n)$ non-negl(n) \Rightarrow

$\frac{\epsilon(n)}{p(n)}$ è non-negl(n)

2 CASI:

Come anticipato prima, se O usa al suo interno una F_k allora la visione che A ha è di giocare nell'esperimento

$\text{PrivK}_{A, \Pi}^{\text{epa}}(n)$

Se O invece usa al suo interno f , A pensa di stare giocando in

$\text{PrivK}_{A, f}^{\text{epa}}(n)$

Dato che la prob. di vittoria di B. dipende da A possiamo dire che:

$$\Pr[D^{F_K(\cdot)}(1^n) = 1] = \Pr[\text{Priv}_{A,\gamma}^{\text{cpa}}(n) = 1]$$

$$\Pr[D^{F(\cdot)}(1^n) = 1] = \Pr[\text{Priv}_{A,\tilde{\gamma}}^{\text{cpa}}(n) = 1]$$

F per h.p. è pseudocavale quindi questo implica che ormai è INDISTINGUISHABLE da una funzione salta totalmente a caso F. Quindi:

$$|\Pr[D^{F_K(\cdot)}(1^n) = 1] - \Pr[D^{F(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$



$$|\Pr[\text{Priv}_{A,\gamma}^{\text{cpa}}(n) = 1] - \Pr[\text{Priv}_{A,\tilde{\gamma}}^{\text{cpa}}(n) = 1]| \leq \text{negl}(n)$$

Pertanto possiamo analizzare la richiesta ipotetica $\hat{\gamma}$ che userà F.

II Fase:

Dobbiamo mostrare che:

$$\Pr_{\mathbf{r}} [\text{PrivK}_{A,\tilde{B}}^{\text{CPA}}(n) = 1] \leq \frac{1}{2} + q(n)/2^n$$

Sia r^* la stringa casuale usata per procedere il cifrario di sfida

$$\langle r^*, f(r^*) \oplus m \rangle$$

CASO 1:

r^* non è stato mai usato prima da $O(\cdot)$ per rispondere alle query di A. Quindi il PAD $f(r^*)$ A lo vede per la prima volta e quindi è totale dal suo punto di vista.

CASO 2:

altrimenti il pad $f(r^*)$ è stato già usato. È dato che siamo in un contesto CPA, l'Adversary dispone di un database che ha memorizzato tutte le scispati che ha ottenuto interpellando l'aula calo. Può quindi trovare m_b facendo

$$\Pr_{\mathbf{r}} [\text{PrivK}_{A,\tilde{B}}^{\text{CPA}}(n) = 1] =$$

$$\Pr_{\mathbf{r}} [b' = b] = 1/2$$

$$f(r^*) \oplus (f(r^*) \oplus m_b) = m_b$$

$F(t^*)$ viene ottenuto dall'Adv facendo:

data che $e := F(t^*) \oplus m$

Allora $F(t^*) := e \oplus m$

\downarrow \downarrow
ottenuto che ha inviato A-
dalla query

Poiché A può effettuare al massimo un numero polinomiale di query $q(n)$, A potrebbe al più $q(n)$ valori di t^* scelti unif. a caso.

Per cui la prob. che A potrebbe t^* cioè un t usato 2 o più volte è

$\frac{q(n)}{2^n} \leftarrow$ quelli di cui A può
scoprire

→ tutti i possibili t^*

Indichiamo con Repeat l'evento t^* uguale a qualche t scelto prima. La prob.

$\Pr [\Pr_{K_{A,\tilde{m}}^{e_{\text{par}}} (n)=1}]$ è uguale a:

$$\Pr_t \left[\text{PrivK}_{A, \hat{m}}^{cpa} (m) = 1 \wedge \text{Repeat} \right] + \Pr_t \left[\text{PrivK}_{A, \hat{m}}^{cpa} (m) = 1 \wedge \overline{\text{Repeat}} \right]$$

$$\leq \\ \Pr_t \left[\text{Repeat} \right] + \Pr_t \left[\text{PrivK}_{A, \hat{m}}^{cpa} (m) = 1 \mid \overline{\text{Repeat}} \right] \cdot \Pr_t \left[\overline{\text{Repeat}} \right]$$

$$\leq \\ \Pr_t \left[\text{Repeat} \right] + \Pr_t \left[\text{PrivK}_{A, \hat{m}}^{epa} (m) = 1 \mid \overline{\text{Repeat}} \right]$$

$$q(m)/2^m + 1/2$$

$$\downarrow \\ \text{negl}(m)$$

questo in
pratica è il
CASO 1

Abbiamo quindi dimostrato che:

$$|P_t[\text{Priv}_{A,\pi}^{\text{epa}}(m)=1] - P_t[\text{Priv}_{A,\tilde{\pi}}^{\text{epa}}(m)=1]| \leq \text{negl}(m)$$

e quindi

$$P_t[\text{Priv}_{A,\pi}^{\text{epa}}(m)=1] \leq P_t[\text{Priv}_{A,\tilde{\pi}}^{\text{epa}}(m)=1] + \text{negl}(m)$$

$$\leq q(m)/2^m + 1/2 + \text{negl}(m)$$

$$\leq 1/2 + q(m)/2^m + \text{negl}(m)$$

$$\leq 1/2 + \text{negl}'(m)$$