CDH difficile e H ROM allora KEM EL Gamal è CPA sicuro

Sia:

- $pk = \langle G, g, q, h \rangle$
- $c = g^y$
- QUERY = "A chiede $H(h^y)$"

$$Pr[KEM^{CPA}_{A,\Pi}(n) = 1] = Pr[KEM^{CPA}_{A,\Pi}(n) = 1 \wedge \overline{QUERY}] + Pr[KEM^{CPA}_{A,\Pi}(n) = 1 \wedge QUERY]$$

$$\leq$$

$$\underbrace{Pr[KEM^{CPA}_{A,\Pi}(n) = 1 \mid \overline{QUERY}]} + \underbrace{Pr[QUERY]}$$

dimostriamo che sono quantità trascurabili

I PEZZO:

Nell'esperimento $KEM^{cpa}_{A,\Pi}(n)$ A riceve $\langle pk, c, \hat{k} \rangle$ dove $\hat{k}$ è $H(h^y)$ oppure un valore scelto a caso.

Se $\overline{Query}$ = "A non chiede $H(h^y)$" si è verificato significa che $H(h^y)$ per A è un valore casuale quindi:

$$Pr[KEM^{cpa}_{A,\Pi}(n) = 1 \mid \overline{QUERY}] = \frac{1}{2}$$

II PEZZO:

Sia:

t = n. polinomiale di query che A fa al ROM

Esibisco una riduzione in cui:

- A gioca in $KEM^{cpa}_{A,\Pi}(n)$
- A' sfrutta A per risolvere CDH

Quando A fa delle query ad H, A' intercetta le query e simula le risposte inviando stringhe di 1 bit scelte a caso.

- Al termine dell'esecuzione, siano $w_1, w_2, \dots, w_t$ le t query che A ha fatto ad H.

- A' sceglie un w_i con $i \in \{1, \dots, t\}$ e la da in output. A' sta scommettendo che w_i sia il quella query in cui "A abbia chiesto $H(h^y)$". La prob. che sia effettivamente questo valore è:

$$P_r[A'(G, g, q, h, c) = h^y] \leq \frac{P_r[\text{Query}]}{t}$$

Ma se CDH è difficile allora $\exists$ negl(n) t.c.

$$\frac{P_r[\text{Query}]}{t} \leq negl(n)$$ per cui, moltiplicando a dx e sx per t ho che:

$$P_r[\text{QUERY}] \leq negl'(n)$$