Teorema 8.79:

Se H è una f. di compressione relativamente al gruppo G, e il problema del log. discreto difficile rispetto a G allora H è una funzione Hash collision-resistant per stringhe di lunghezza fissata.

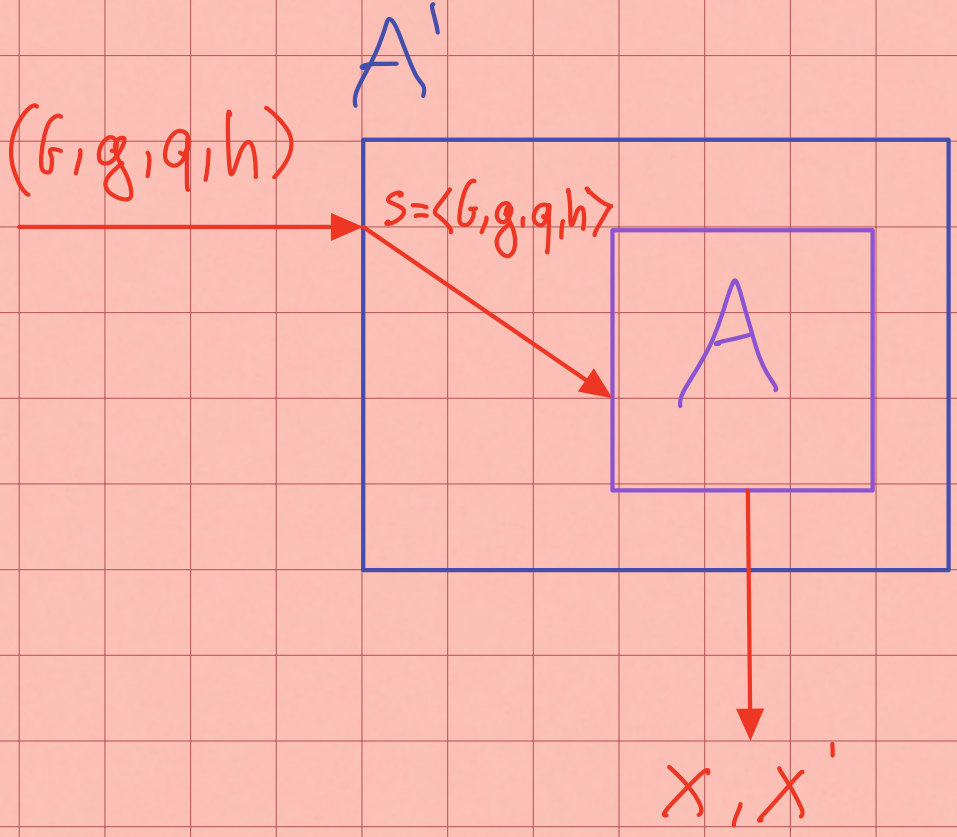
dimostrazione:

hp:
- Adv A PPT
- $Pr[Hash\text{-}call_{A,\Pi}(n) = 1] = \varepsilon(n)$

facciamo vedere che costruendo una riduzione A' che sfrutta la capacità di A nel trovare due x, x' t.c. $x \neq x'$ e $H(x) = H(x')$ si potrebbe risolvere il problema del log. disc. che A' cerca di risolvere in tempo polinomiale.

La prob. di successo di A' dipende dalla prob. di successo di A nel trovare una coll, che è stata fissata a $\varepsilon(n)$.

riduzione:



① A' vuole risolvere il problema di Diffie-Hellman quindi riceve in input (G, g, q, h) dove $h \in G$

② Ricordando che H è def. come $H^s(x_1, x_2) = g^{x_1} h^{x_2}$, passiamo proprio il seme di cui ha bisogno ad A. $s = \langle G, g, q, h \rangle$

③ A produce $x \neq x'$ per i quali pensa di aver trovato una collisione.

- se $x \neq x'$ allora A ha davvero trovato una collisione

- altrimenti 2 casi possibili:

CASO 1:	CASO 2:
se $h = 1$ il problema del Dlog. è banale perché $g^0 = 1$	se $h \neq 1$ allora scrivo $x = (x_1, x_2) \in \mathbb{Z}_q^*$ $x' = (x_1', x_2') \in \mathbb{Z}_q^*$

A' ricavando x, x' calcolo

$$\left[(x_1 - x_1')(x_2 - x_2')^{-1} \bmod q \right]$$

calcolare questo valore significa risolvere il prob. del log discr. Ma dato che Dlog è un problema difficile la sua prob. di calcolarlo in t. poly è $\varepsilon(n)$ Trascurabile. Di conseguenza, dato che avevamo supposto

le due prob. di vittoria di A e A' legate, implica che anche la prob. di trovare una collis. da parte di A è trasc. quindi H1 coll. resistant.