Teorema 5.4. Se $(Gen, h)$ è resistente a collisioni, allora $(Gen, H)$ lo è.

Dimostrazione:

Mostriamo che una collisione in $H^s$ dà una collisione in $h^s$.

Siano $x$ ed $x'$ due stringhe differenti di lunghezza $L$ ed $L'$ t.c.:

$$H^s(x) = H^s(x')$$

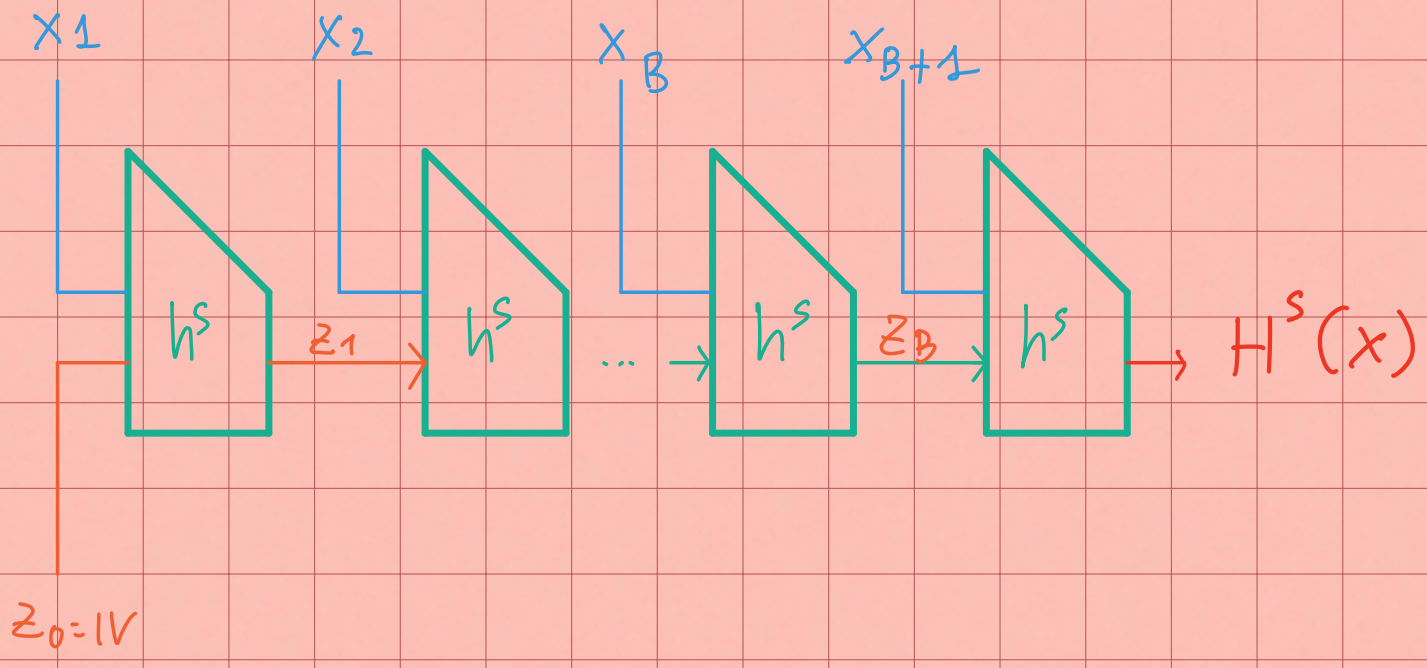
dove

$$\underbrace{x = x_1 \dots x_B \; x_{B+1}}_{\text{lungo } L}$$

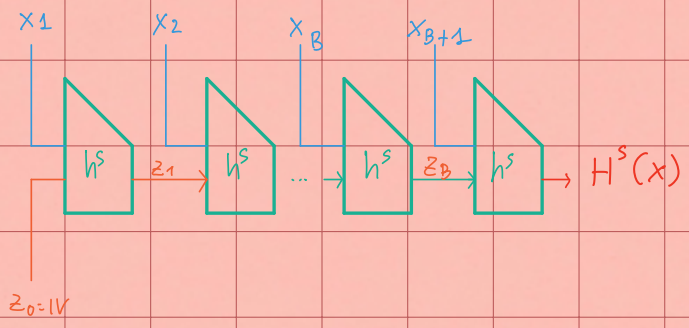
$$\underbrace{x' = x'_1 \dots x'_{B'} \; x'_{B'+1}}_{\text{lungo } L'}$$

# TRASFORMAZIONE DI MERKLE-DAMGARD

$$X = X_1 X_2 \dots X_B X_{B+1}$$



# 2 CASI DA CONSIDERARE




## CASO 1: $(L \neq L')$

Se le lunghezze di $X, X'$ sono diverse, allora gli ultimi passi del calcolo di $H^s(X)$ e $H^s(X')$ sono

$H^s(X) = z_{B+1} = h^s(z_B \| X_{B+1})$
$H^s(X') = z_{B'+1} = h^s(z_{B'} \| X_{B'+1})$

per hp. $X$ e $X'$ sono t.c. $H^s(X) = H^s(X')$, questo implica quindi che $z_{B+1} = z_{B'+1}$ allora

$w = z_B \| X_{B+1}$ e $w' = z_{B'} \| X_{B'+1}$ sono una
$\downarrow L$ $\downarrow L'$

diverse perché per hp. $L \neq L'$ e producono una collisione in $h^s$

## CASO 2: $(L = L')$

Quindi $B = B'$ e $X_{B+1} = X_{B'+1}$

Siano:

$z_1 \dots z_{B+1}$ gli output intermedi delle $h^s$ per calcolare $H^s(X)$

$I_1 \dots I_{B+1}$ gli input intermedi delle $h^s$ per calcolare $H^s(X)$ dove $I_i = (z_{i-1} \| X_i)$, $i = 1 \dots B+1$

$z'_1 \dots z_{B'+1}$ e $I'_1 \dots I_{B'+1}$ come sopra ma per $H^s(X')$.

poniamo come input di un ipotetico ulteriore blocco $I_{B+2} = z_{B+1}$ e $I_{B'+2} = z_{B'+1}$.

Definiamo con $N$ il più grande indice per cui risulta

$I_N \neq I'_N$.

Poiché per hp. $x \neq x'$ deve esistere un $i$ tale che $x_i \neq x'_i$ => $N$ certamente esiste

questo mi dice anche che tutti gli input successivi ad $N$ sono tutti Tali che $I_{N+i} = I'_{N+i}$ con $i = 1 \dots B+1$

esempio: TUTTI UGUALI

$x =$ 0 1 0 0 1 0 1 1 1 0 1

$x' =$ 0 1 1 0 0 1 1 1 0 0 1

i=1 i=2 i=3 i=4 i=5 i=6 i=7 i=8 i=9 i=10 i=11

$X_{DIFF} = \{3, 5, 6, 9\}$

$MAX(X_{DIFF}) = 9 = N$ è l'indice massimo in cui gli input differiscono, e sappiamo esiste perché per hp. $x \neq x'$

D'altra parte dato che

$$I_{B+2} = z_{B+1} = \underbrace{H^s(x) = H^s(x')}_{\text{per hp.}} = z_{B'+1} = I_{B'+2}$$

questo $N$ deve essere $N \leq B+1$.

Se $I_N \neq I'_N$ => $I_{N+1} = I'_{N+1}$ => $z_N = z'_N$ in quanto fanno parte dell'input $N+1$

=> e quindi:

$$h^s(I_N) = z_N = z'_N = h^s(I'_N)$$

e quindi le stringhe $I_N, I'_N$ sono una collisione per $h^s$