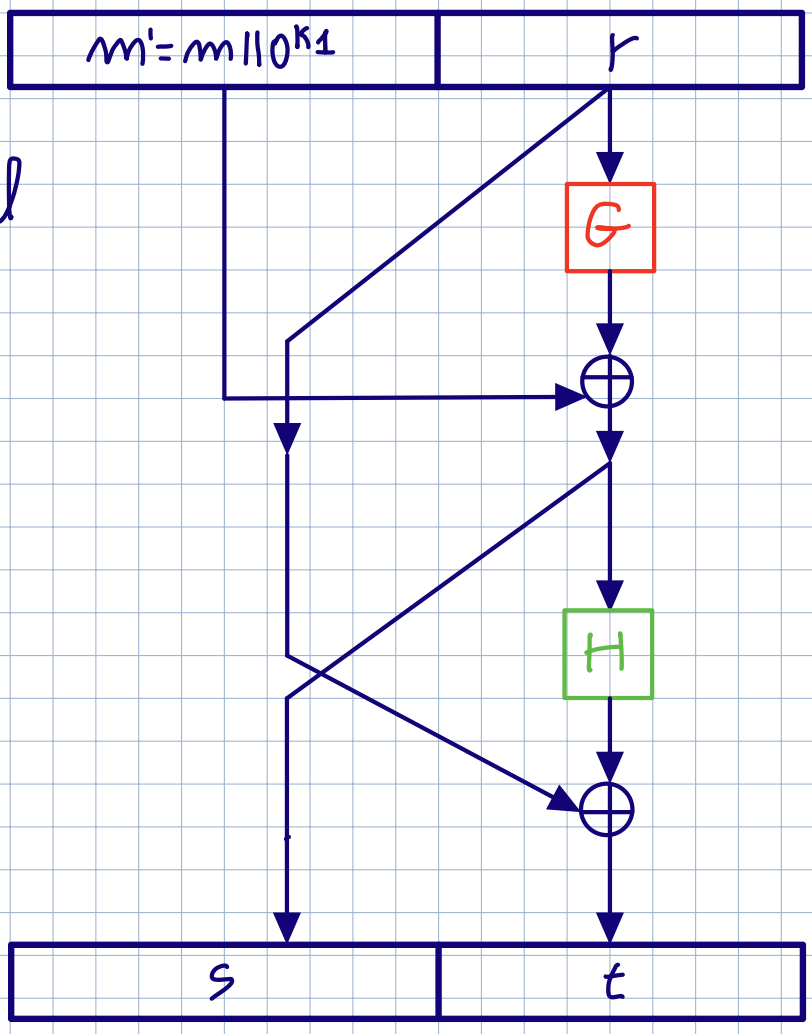
rete di Feistel a 2 round



$m' = m \| 10^{k_1}$

$\hat{m} = s \| t$

dove $s = G(r) \oplus m'$

$t = H(s) \oplus r$

formalmente:

consideriamo RSA, l, k_0, k_1 e definiamo due funzioni:

$H: \{0,1\}^{k_0} \longrightarrow \{0,1\}^{l+k_1}$

$G: \{0,1\}^{\ell+K_1} \longrightarrow \{0,1\}^{K_0}$

Definisco $\Pi = (Gen, Enc, Dec)$

1. $Gen: (N, e, d) \leftarrow GenRSA(1^n)$

$PK = \langle N, e \rangle$; $SK = \langle N, d \rangle$

2. Enc: su PK e m in input calcola

$r \leftarrow \{0,1\}^{K_0}$

ricava $m' = m \| 0^{K_1}$

ricavo $\hat{m} = s \| t$ dove

$s = G(r) \oplus m'$

$t = H(s) \oplus r$

calcola $c := \hat{m}^e \bmod N$

3. Dec: su SK e $c \in \mathbb{Z}_N^*$ calcola

$\hat{m} := c^d \bmod N$

se $|\hat{m}| > \ell + K_0 + K_1$ output $\perp$

altrimenti: considera $\hat{m}$ come $s \| t$

dove $s \in \{0,1\}^{\ell+K_1}$ e $t \in \{0,1\}^{K_0}$

se i bit meno significativi di K_1 di m' non sono nulli output $\perp$

altrimenti: output il bit più
significativo di $\hat{m}$