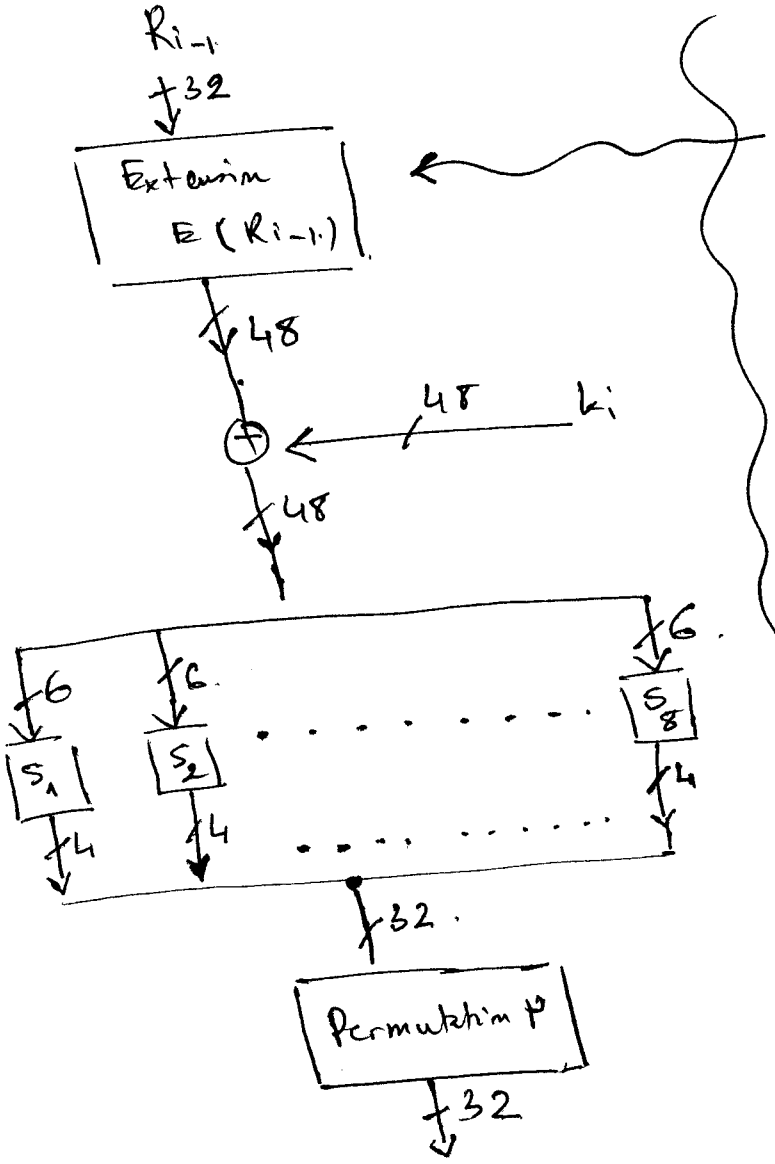
(2.2) La fonction f.

Rappelons que $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$ au rond i.



Désorganise en bloc de 4 bits en répétition de certains bits : renforce l'idée de la diffusion. On obtient $6 \times 8 = 48$ bits

Les S_i : S-box reçoit 6 bits et renvoit 4 bits : les S_i sont distincts et sont codés dans des tables. Augmente la confusion (par leur non-linéarité) i.e. $S_i(a \oplus b) \neq S_i(a) + S_i(b)$

- Les S-box augmentant la sécurité du DES, permettant aussi de parer à l'attaque par cryptanalyse différentielle introduite en 1990 par Shamir et Biham (connu par les chercheurs d'IBM 16 ans par avance !!!).

P renforce la diffusion.