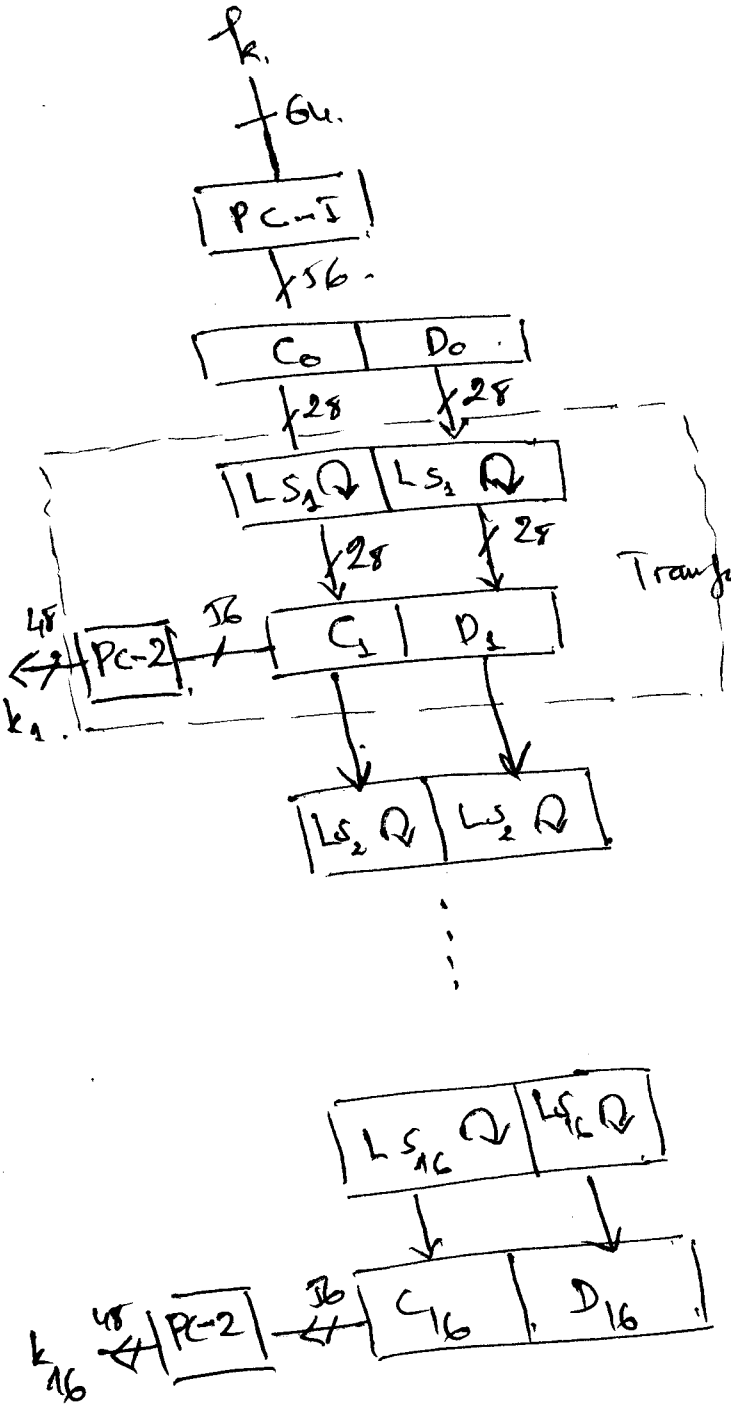
(2.3) ordonnancement clé

- Les 56 bits (actuels) sans bits de parité sont permutés par PC-1, ensuite partagé en deux blocs de 28 bits chacun C_0 et D_0.



- LS_i : left shift by i positions.

rnde i : LS_1 pour $i = 1, 2, 9, 16$.

i : LS_2 $i \neq 1, 9, 2, 16$

$\Rightarrow C_0 = C_{16}$ et $D_0 = D_{16}$.

- PC_2 permute les 56 bits et ignore 8 bits $\Rightarrow$ 48 bits.

- Ces opérations sont faciles à réaliser en hardware.