

ANNEXE. Le chiffrement étudié est un SPN simple conçu par le cryptographe Howard Heys dans le but d'expliquer les attaques différentielles et linéaires (voir Howard Heys, A Tutorial on Linear and Differential Cryptanalysis [http://www.engr.mun.ca/~howard/PAPERS/ldc\\_tutorial.pdf](http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf)). Le schéma est assez proche de celui de l'AES, mais il ne traite que des blocs de 16 bits, et comporte seulement 4 tours décrites ci-dessous. Les S-boxes sont toutes identiques à la première ligne de la première S-box du DES.

Chaque clef de tour est de 16 bits, obtenue par exemple chacune comme sous-clef d'une clef de 64 bits (sans réelle procédure de diversification de clefs).

Les trois premiers tours sont identiques, et le quatrième et dernier similaire, la permutation étant absente. Ceci permet une procédure de déchiffrement identique à celle de chiffrement, à ceci près qu'il faut utiliser l'inverse de la S-box utilisée pour chiffrer.

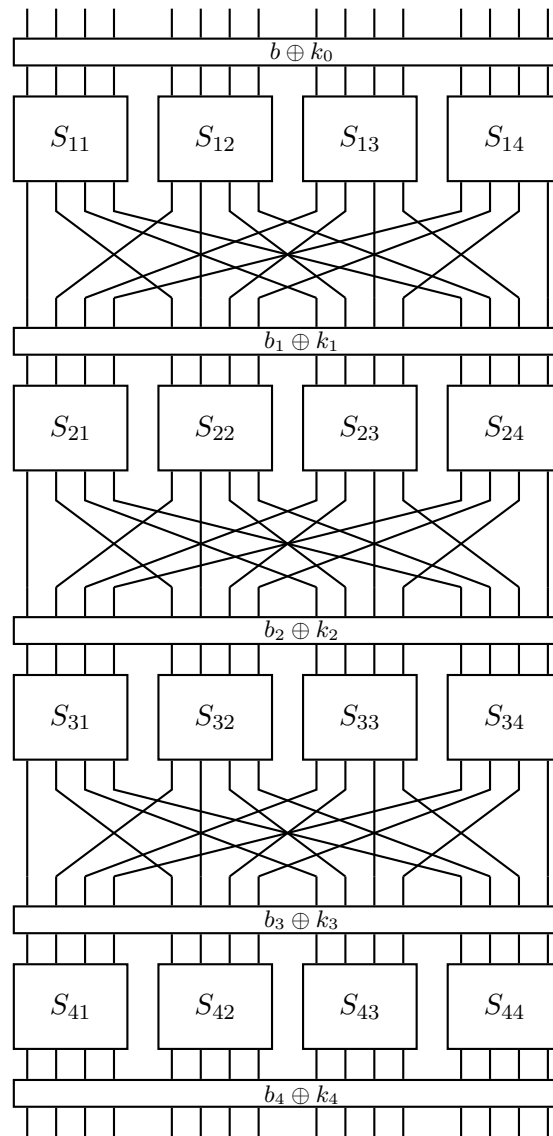


FIGURE 1 – Schéma du chiffrement

```

sbox_t sbox = {0xe, 0x4, 0xd, 0x1, 0x2, 0xf, 0xb, 0x8,
              0x3, 0xa, 0x6, 0xc, 0x5, 0x9, 0x0, 0x7};
/*      { 0,  1,  2,  3,  4,  5,  6,  7,
          8,  9,  a,  b,  c,  d,  e,  f} */
sbox_t isbox = {0xe, 0x3, 0x4, 0x8, 0x1, 0xc, 0xa, 0xf,
               0x7, 0xd, 0x9, 0x6, 0xb, 0x2, 0x0, 0x5};

```

FIGURE 2 – Table de substitution et son inverse (les quatre sont identiques)

		Différences en sortie															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Différences en entrée	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
	a	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	b	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
	c	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
	d	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
	e	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
	f	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

FIGURE 3 – table des différences

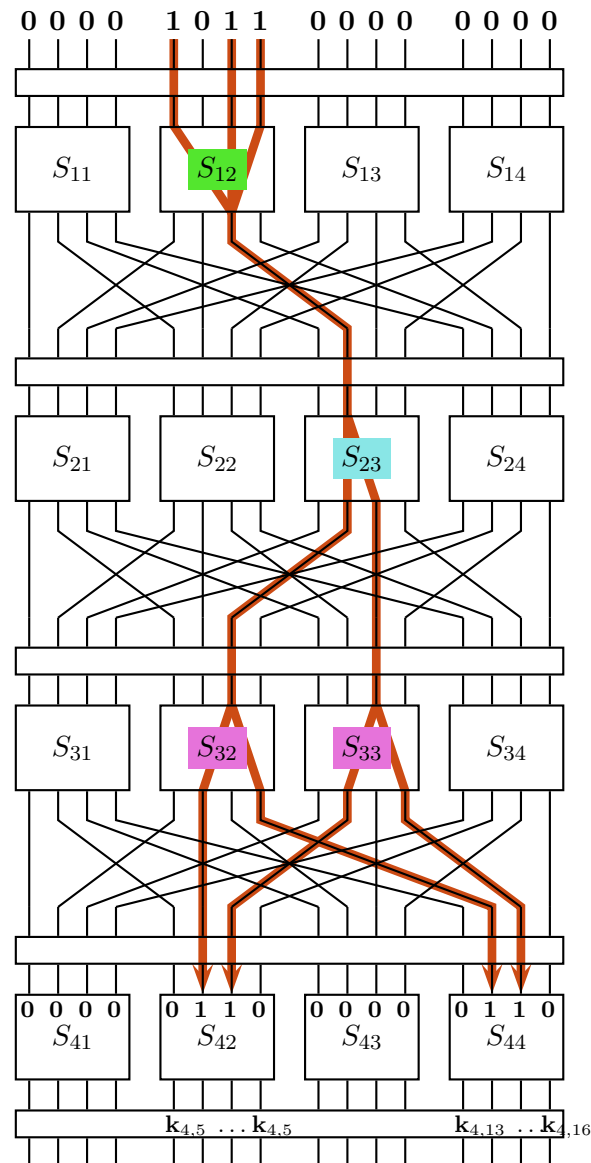


FIGURE 4 – Un exemple de caractéristique différentielle

		Somme en sortie															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Somme en entrée	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
	2	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
	3	0	0	0	0	0	0	0	0	2	-6	-2	-2	2	2	-2	-2
	4	0	2	0	-2	-2	-4	-2	0	0	-2	0	2	2	-4	2	0
	5	0	-2	-2	0	-2	0	4	2	-2	0	-4	2	0	-2	-2	0
	6	0	2	-2	4	2	0	0	2	0	-2	2	4	-2	0	0	-2
	7	0	-2	0	2	2	-4	2	0	-2	0	2	0	4	2	0	2
	8	0	0	0	0	0	0	0	0	-2	2	2	-2	2	-2	-2	-6
	9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	2	0	4	2	-2
	a	0	4	-2	2	-4	0	2	-2	2	2	0	0	2	2	0	0
	b	0	4	0	-4	4	0	4	0	0	0	0	0	0	0	0	0
	c	0	-2	4	-2	-2	0	2	0	2	0	2	4	0	2	0	-2
	d	0	2	2	0	-2	4	0	2	-4	-2	2	0	2	0	0	2
	e	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
	f	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

FIGURE 5 – Table des approximations linéaires

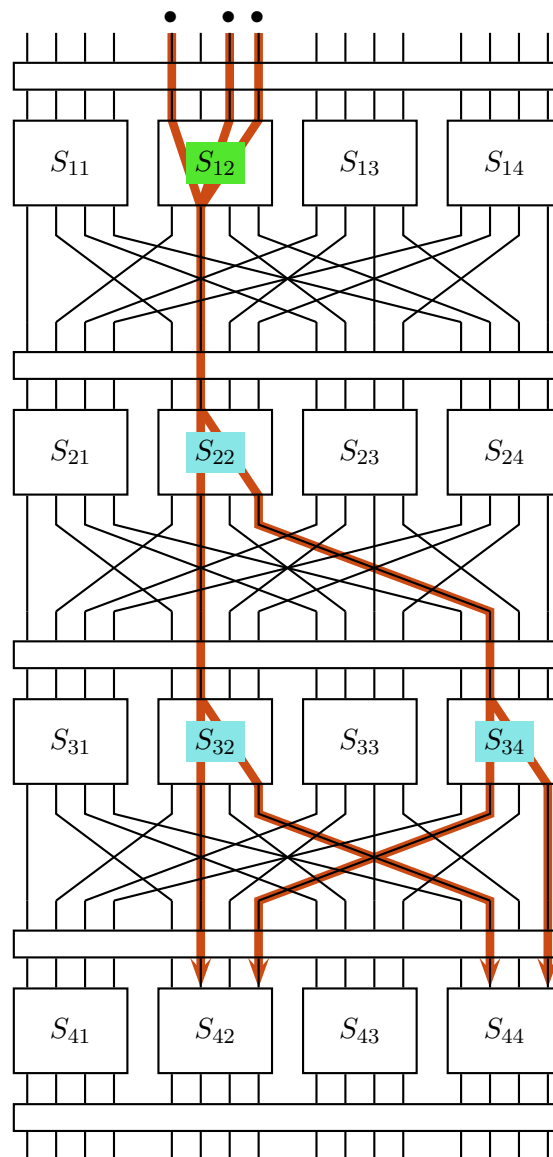


FIGURE 6 – Un exemple d'approximation linéaire (à compléter)