• (5.2). Attaque avec clair / chiffré.

supposons donc que la clé $k = (p_{m-1}, \dots, p_0)$ servant de base pour le calcul de la s-clé $(\Delta_i)_i$.

Hypothèse : { clair $x_0, \dots, x_{2m-1}$ connu par Oscar. ainsi que son chiffré $y_1, \dots, y_{2m-1}$.

Oscar calcule $\Delta_i = x_i + y_i \pmod 2$ $i = 0, 1, \dots, 2m-1$.

on a : $(*)$ $\Delta_{i+m} = \sum_{j=0}^{m-1} p_j \Delta_{i+j} \pmod 2$ $i \geq 0$.

L'eq. $(*)$ peut servir pour déduire les (p_i) :

$$(S)\begin{cases} i=0, & \Delta_m = p_{m-1}\Delta_{m-1} + \dots + p_0 p_0 \pmod 2. \\ i=1, & \Delta_{m+1} = p_{m-1}\Delta_m + \dots + p_0 \Delta_1 \\ \dots & \\ i = m-1, & \Delta_{2m-1} = p_{m-1}\Delta_{2m-2} + \dots + p_0 \Delta_{m-1} \end{cases}$$

Donc Oscar résout (S) pour trouver (p_i).

Remarque. Malgré l'attaque ci-dessus, on peut renforcer le système (ex. Trivium vir ...).