$[x]^A \to [x]^B$ 将 $x \in Z_{2^k}$ 的子秘密

转换为：$\{x[1], x[2] \cdots x[k]\}$，$x[i] \in \{0,1\}$ 的子秘密，并且

$x = \sum_{i=1}^{k} 2^{i-1} x[i]$

(十 与 二 进制转换)

例：仍将秘密 x 以 x_1, x_2, x_3 分享

(x_1, x_2) (x_2, x_3) (x_3, x_1)

A B C

$(x_{1,1}\ x_{1,2} \cdots x_{1,k})$ ----

$(x_{2,1}\ x_{2,2} \cdots x_{2,k})$

x_1、x_2、x_3 第 j 位相加不一定等于 x 的第 j 位

措施：波纹进位全加器 $x = RCFA(RCFA(x_1, x_2), x_3)$

表达式为：$S_i = A_i \oplus B_i \oplus C_{i-1}$

$C_i = A_i B_i + C_{i-1}(A_i + B_i)$

S_i：本位和

A_i、B_i：输入比特

C_{i-1} 低位来的进位

C_i 向高位进位

例：$A_i = 1$，$B_i = 0$，$C_{i-1} = 1$

则：$S_i = 1 \oplus 0 \oplus 1 = 0$

$C_i = 0 + 1(1+0) = 1$