

(10) mult mod p mod v(x)

entre  $P_{A_0}$  } à 1 littéral x  
 $P_{A_1}$

$[A_3] = p$   
 $P_{A_4} = v(x)$

Pose à libre  $P_{A_2} = P_{A_0} * P_{A_1} \begin{matrix} \text{mod } p \\ \text{mod } v(x) \end{matrix}$

conservé A3/A4

XMM MUL : MOVEM.L A3/A4/A6, -(SP)

BSR XMULP  $P_{A_0} * P_{A_1}$

MOVE.L A2, A0

MOVE.L (SP)+, A3

MOVE.L (SP), A1

BSR XMPMOD  $\begin{matrix} \text{conservé } A3 \\ \text{met le reste modulo } v(x) \text{ et } p \end{matrix}$

MOVE.L (SP)+, A4

BRA KL860