

5

mdsmp ( $\overline{U, P}$ )<sup>type 2</sup>  
 $|P| \neq 0, 1$

U: forme factorisée  
 $u_1 \cdot u_2 \dots u_k$

poly à un littéral x

Soit V forme "factorisée" illégale  $V = \frac{v_1 \dots v_k}{1}$   
telle que  $\sum_{i=1}^k \frac{v_i}{u_i} \equiv \frac{1}{u_1 \dots u_k} \pmod{p}$  car a peut  
 $\deg(v_i) < \deg(u_i)$

```
YMD SMP: BSR XMF BEZC
BSR WCALMB3
SUBQ #2, A0
MOVE.L AS, -(SP)
ADDQ #6, A6
BSR XMF BEZ
MOVE.L (SP)+, A5
BRA POPNEW
```

telle U  
 $[A3] = |p| \neq 0, 1$  décodé  
 $\text{var}_{A0} = U$

