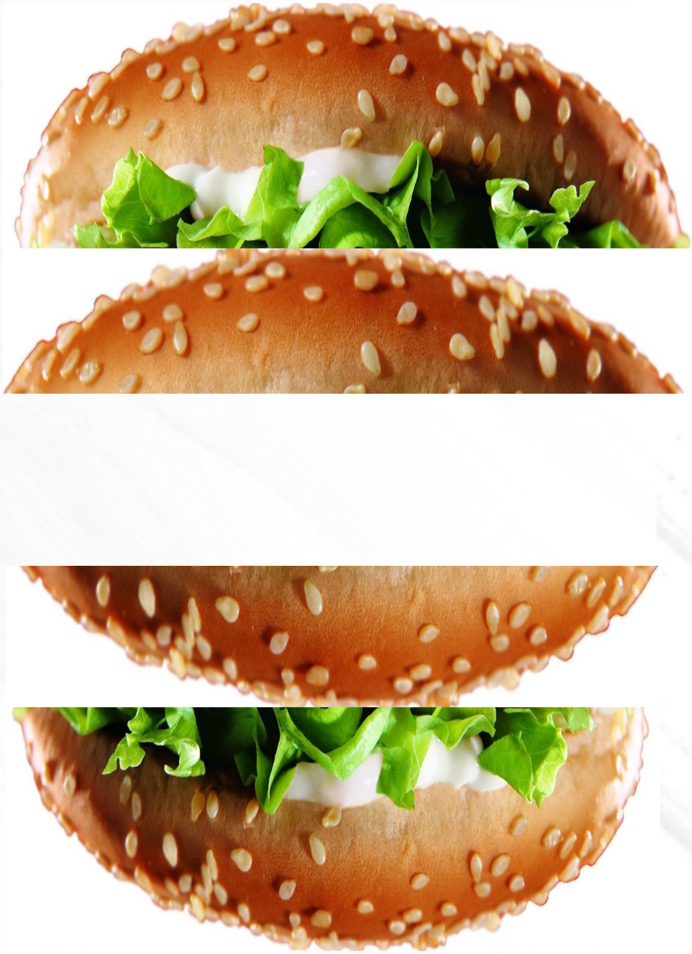
# Battle Between Misuse Resistant Parallelizable Authenticated Ciphers

Nilanjan Datta, Mridul Nandi

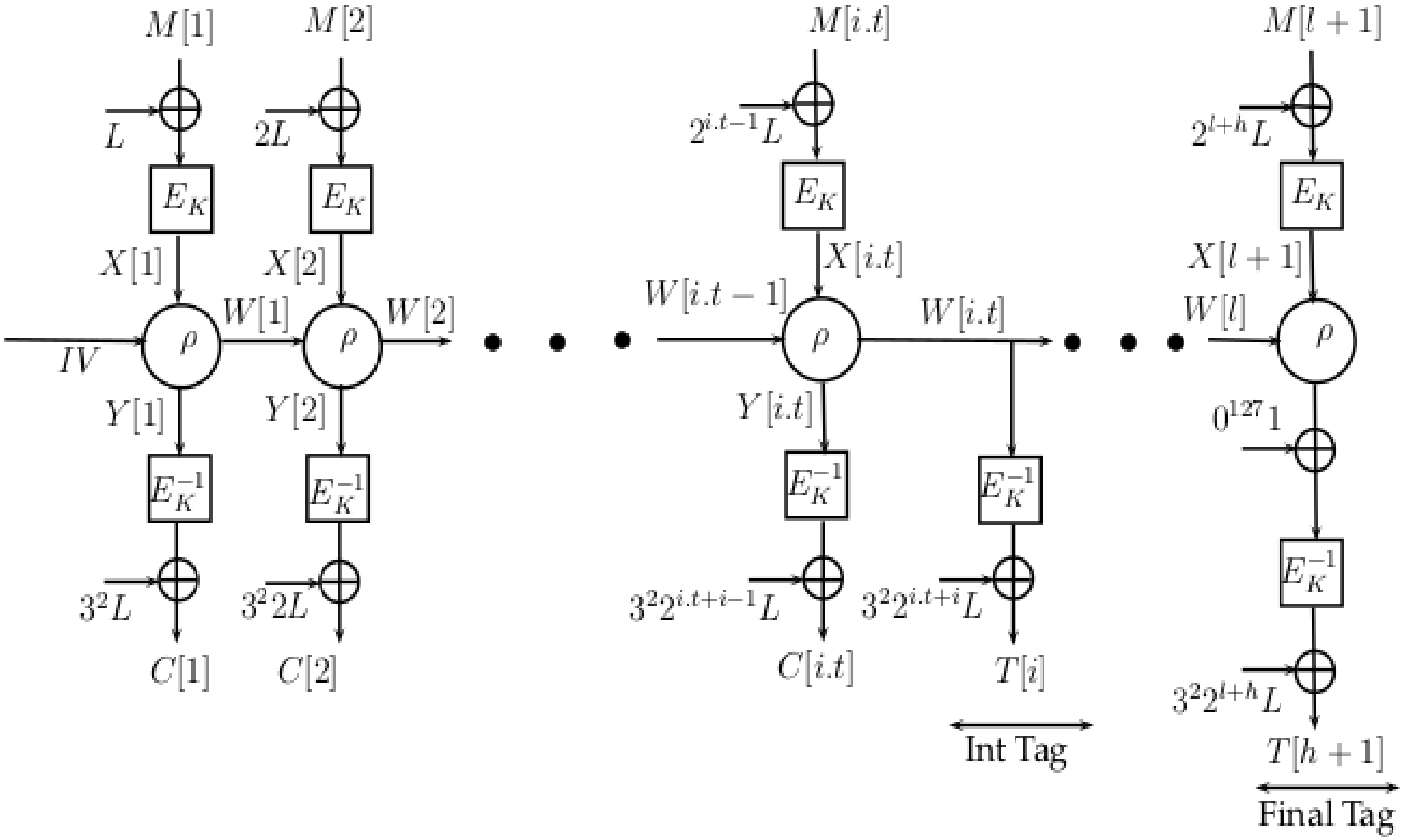
Indian Statistical Institute

# Issue 1 : Area of combined implementation



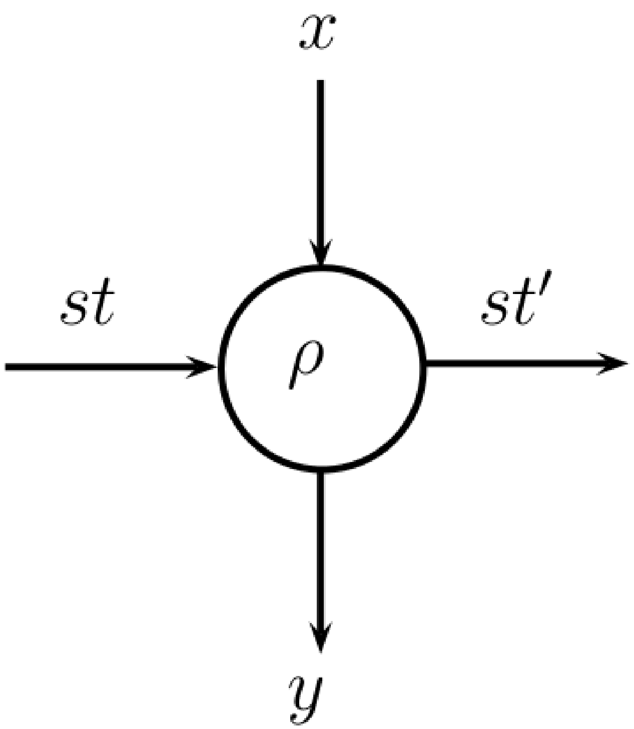
Which Burger will you choose ??

# ElmE



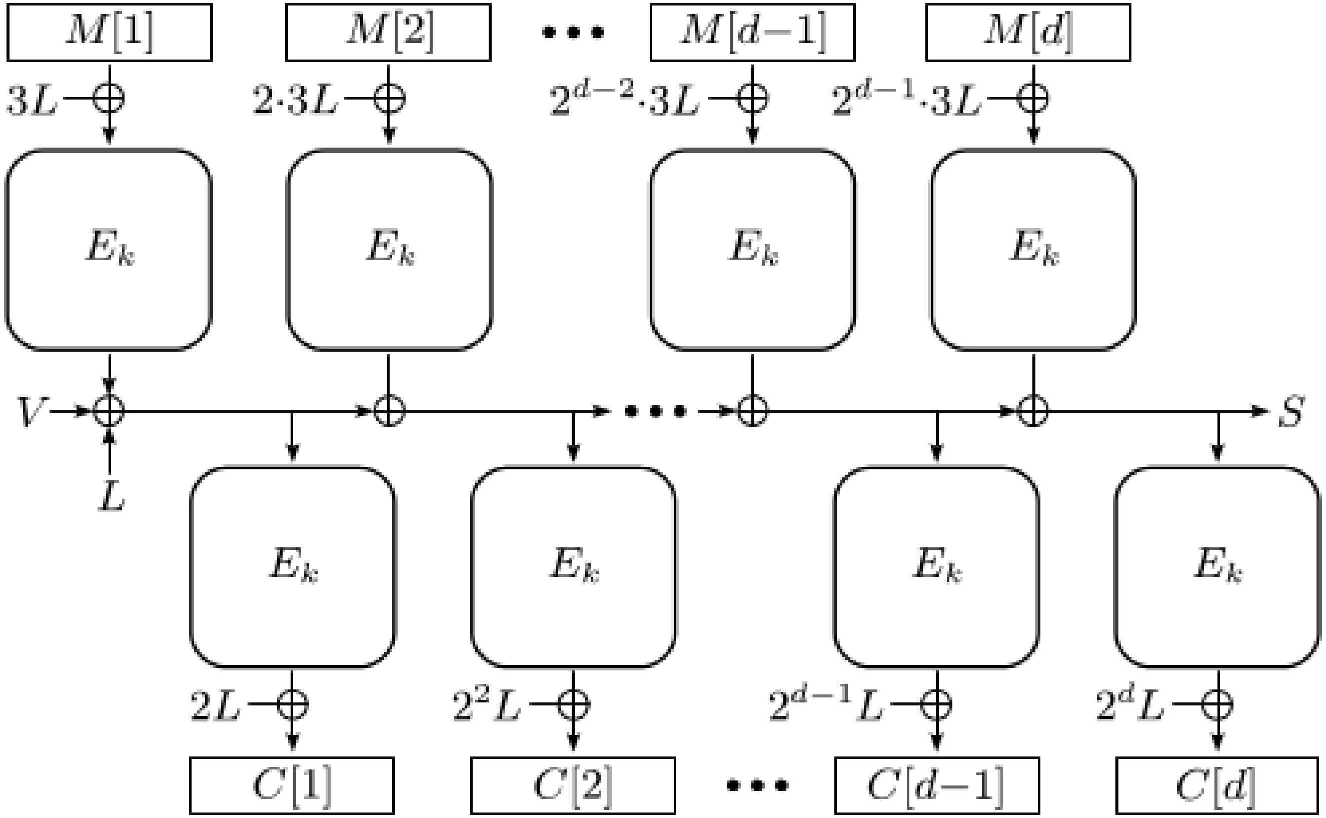
$M[1]$
$M[2]$
$M[i.t]$
$M[l+1]$
$L$
$2L$
$2^{i.t-1}L$
$2^{l+h}L$
$E_K$
$X[1]$
$X[2]$
$X[i.t]$
$X[l+1]$
$W[1]$
$W[2]$
$W[i.t-1]$
$W[i.t]$
$W[l]$
$IV$
$\rho$
$Y[1]$
$Y[2]$
$Y[i.t]$
$0^{127}1$
$E_K^{-1}$
$3^2L$
$3^22L$
$3^22^{i.t+i-1}L$
$3^22^{i.t+i}L$
$3^22^{l+h}L$
$C[1]$
$C[2]$
$C[i.t]$
$T[i]$
Int Tag
$T[h+1]$
Final Tag

# ElmE Linear Mixing



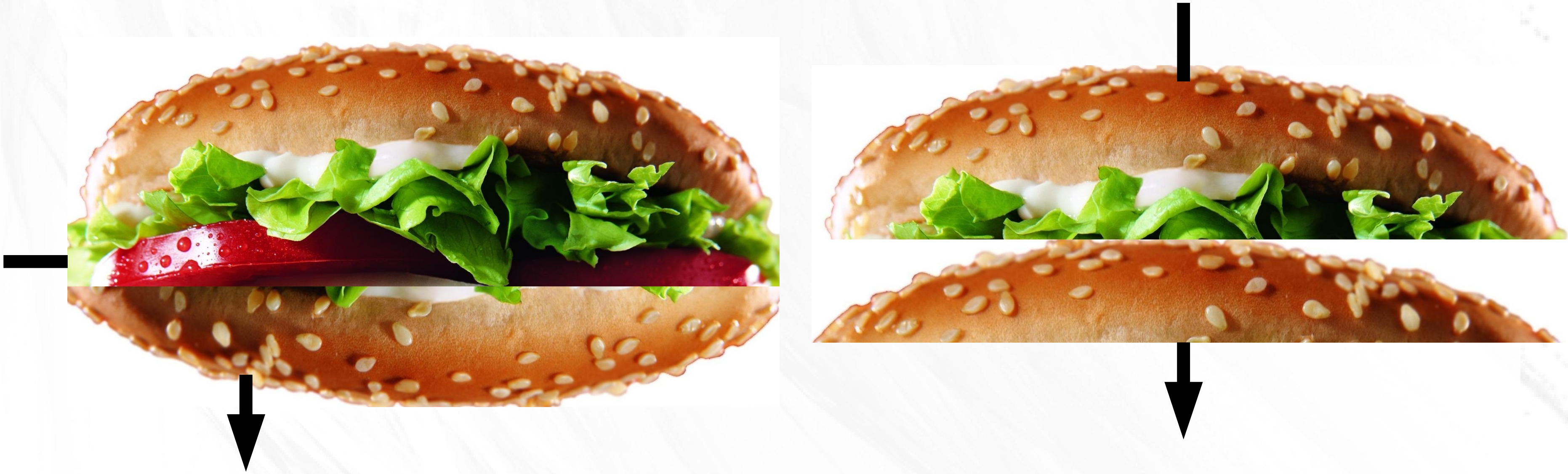
$$\begin{aligned} y &= x \oplus 3 \cdot st \\ st' &= x \oplus 2 \cdot st \end{aligned}$$

# CoPA



$M[1]$
$M[2]$
$M[d-1]$
$M[d]$
$3L$
$2 \cdot 3L$
$2^{d-2} \cdot 3L$
$2^{d-1} \cdot 3L$
$E_k$
$V$
$L$
$S$
$2L$
$2^2 L$
$2^{d-1} L$
$2^d L$
$C[1]$
$C[2]$
$C[d-1]$
$C[d]$

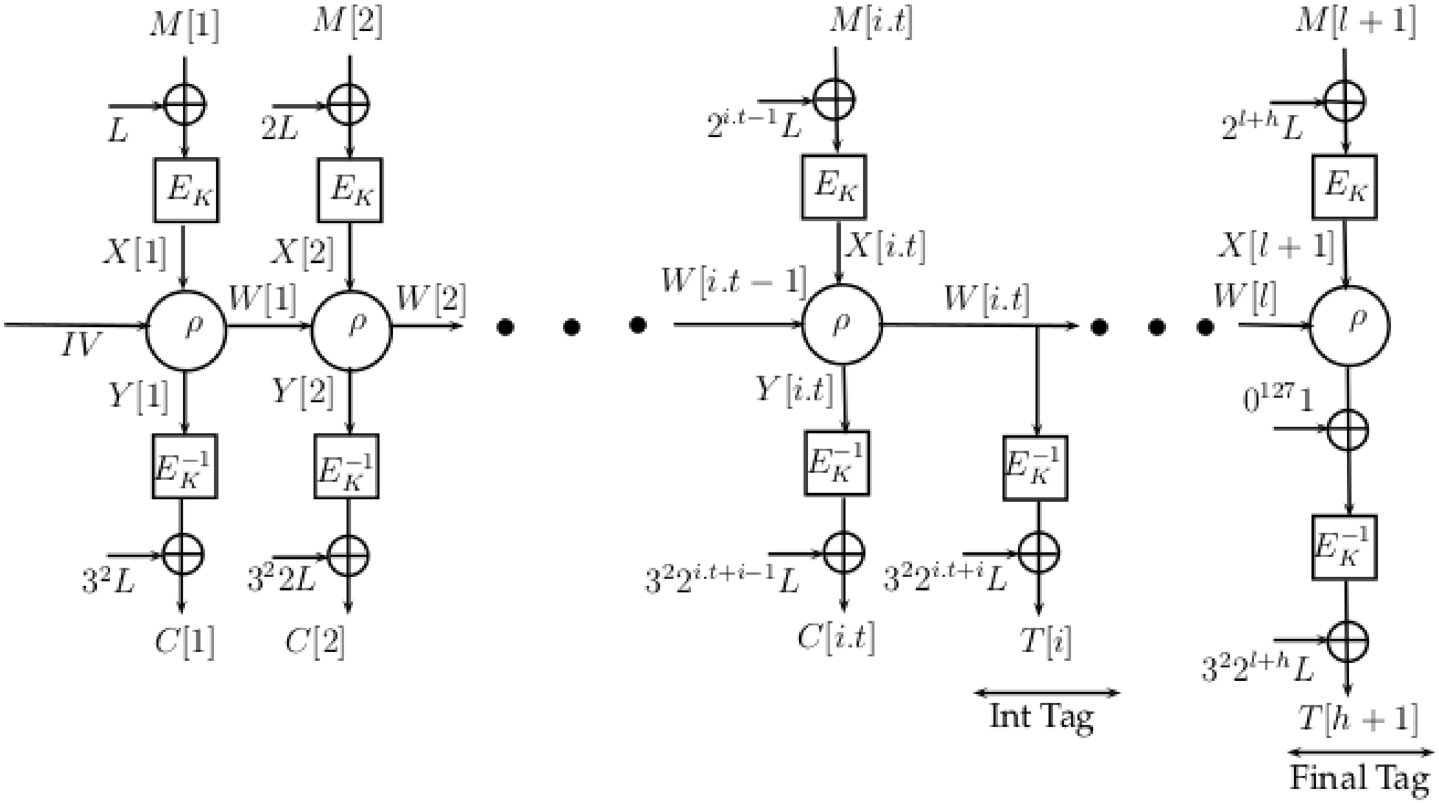
# Issue 2 : Intermediate Tag Generation



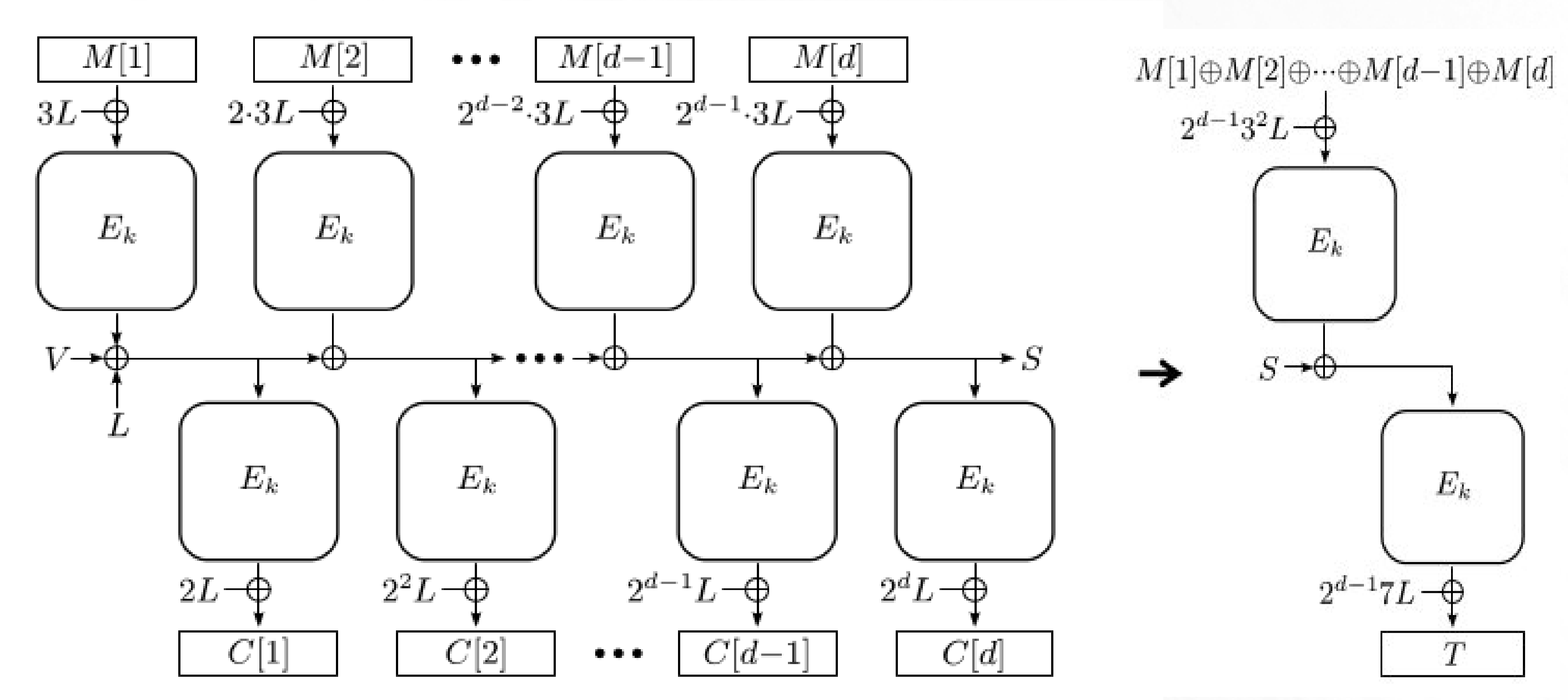
ElmE : Easily Done due to rho mixing.

CoPA : Hard to generate from lightweight mixing

# ElmE : Easy to Generated Intermediate Tags



# CoPA : Hard to Generate Intermediate tags



- Can't generate Tag from mixing layer.
- Intermediate Tag generation must be similar to Final Tag Generation

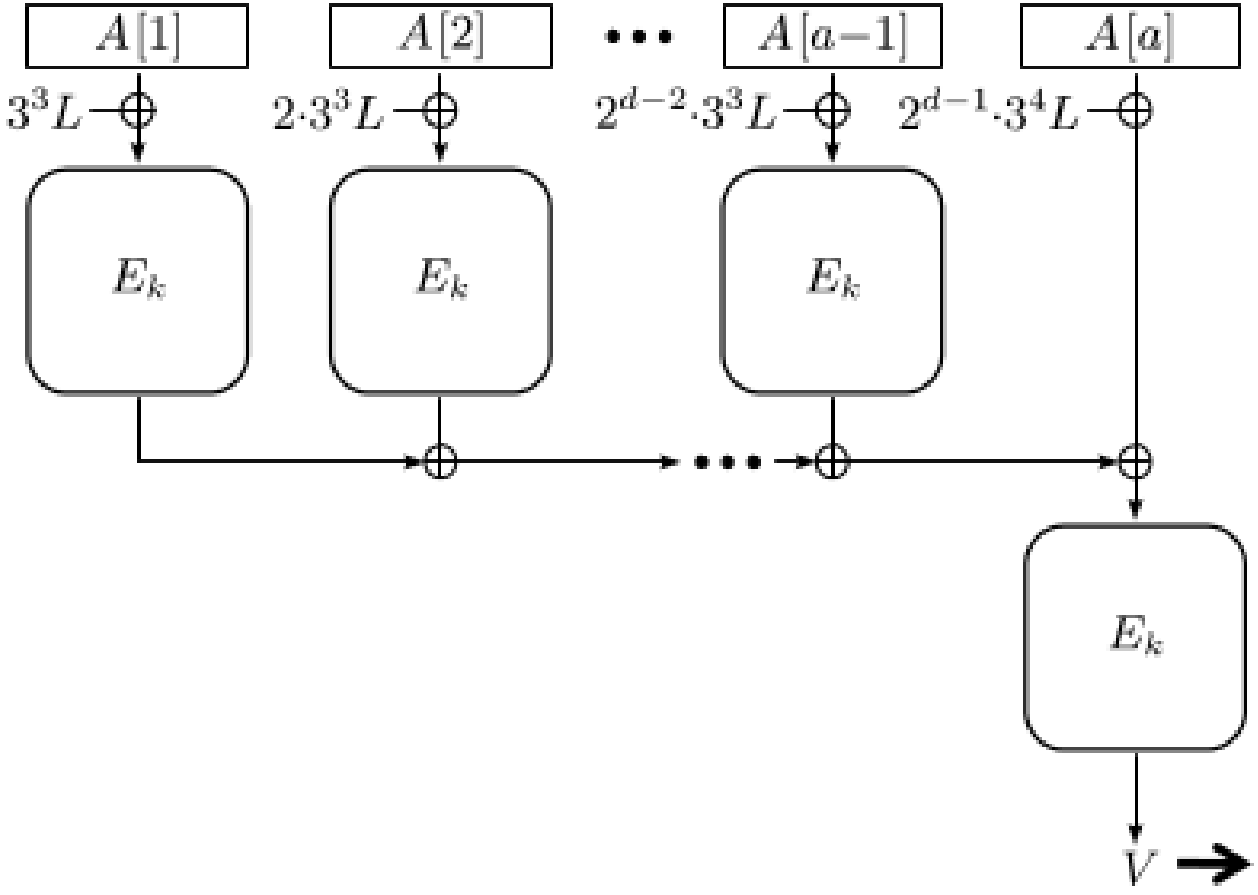
# Issue 3 : Associated Data Processing

Eat, Digest and then take bread

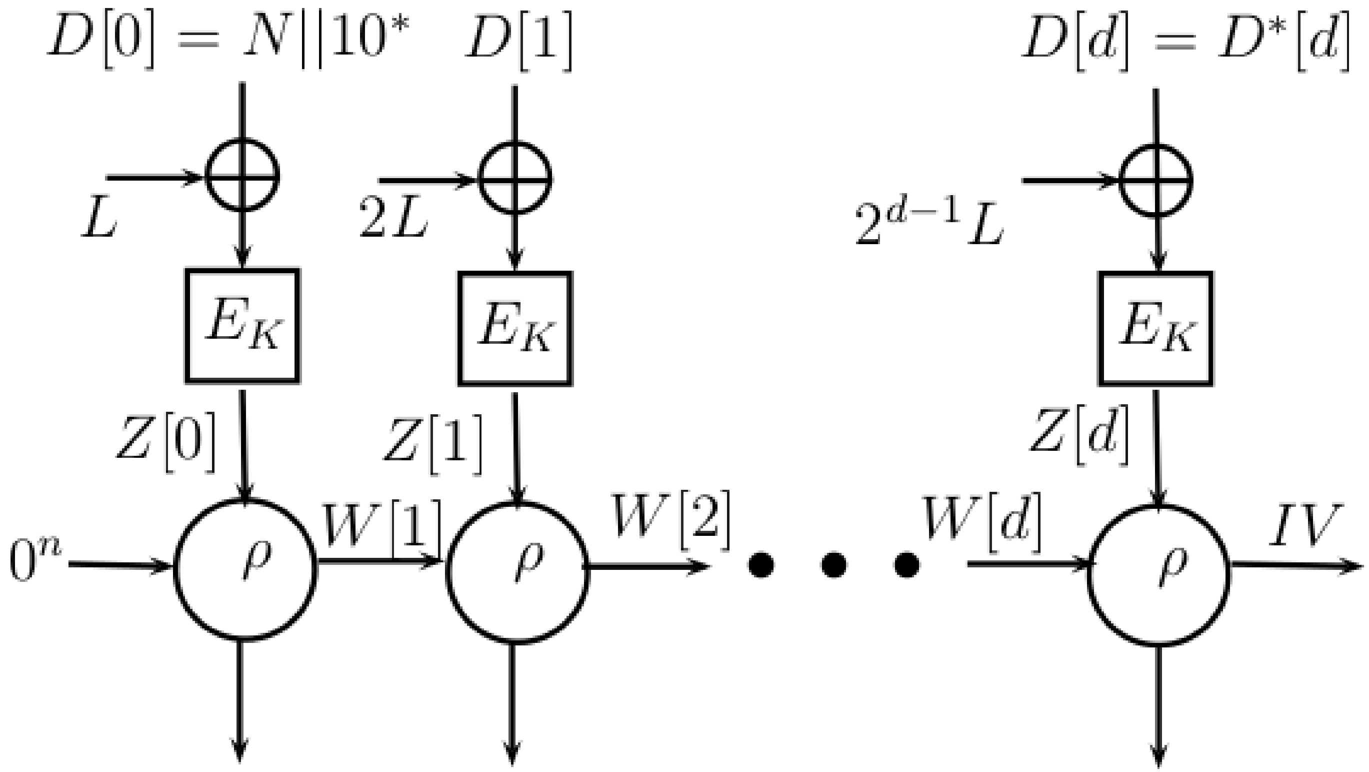
ElmE : Fully Parallel

COPA : Sequential for one block

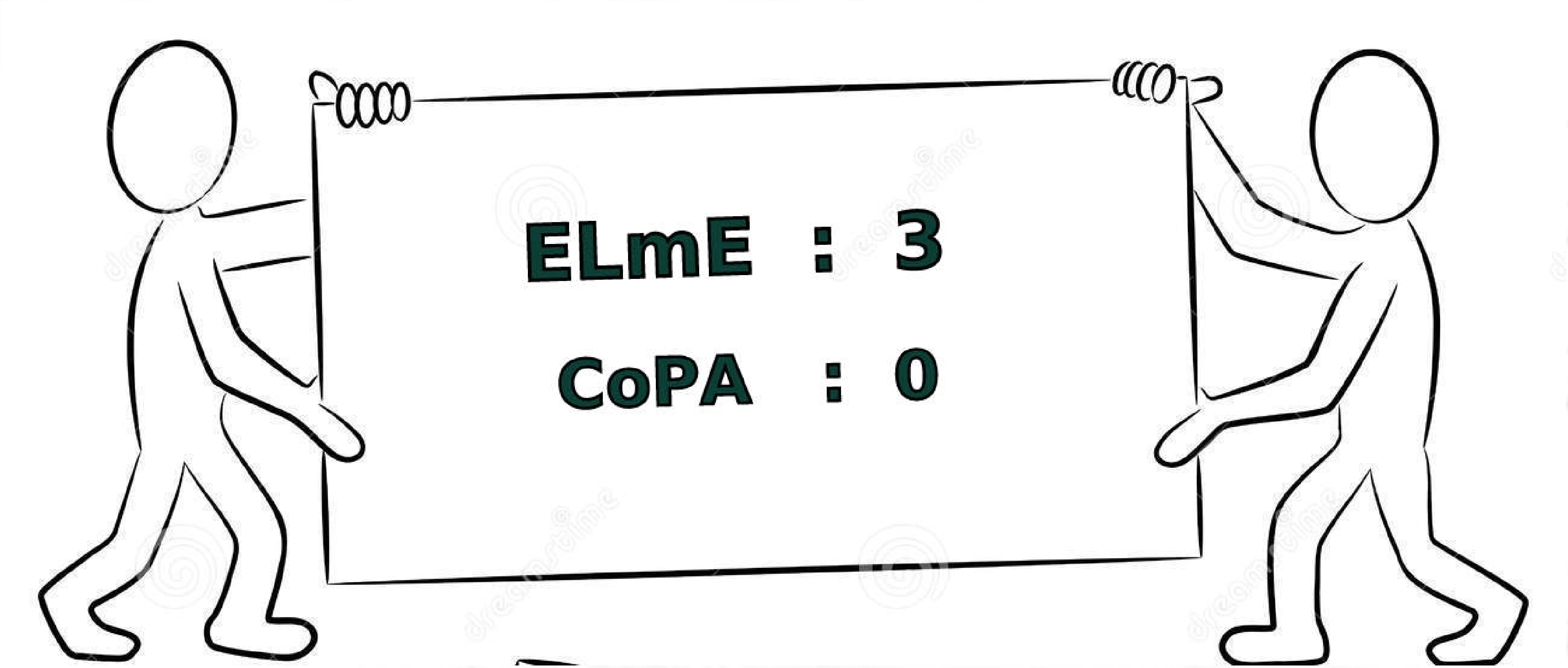
# CoPA : Associated Data Processing



# ElmE : Associated Data Processing



# Final Result


ELmE : 3
CoPA : 0