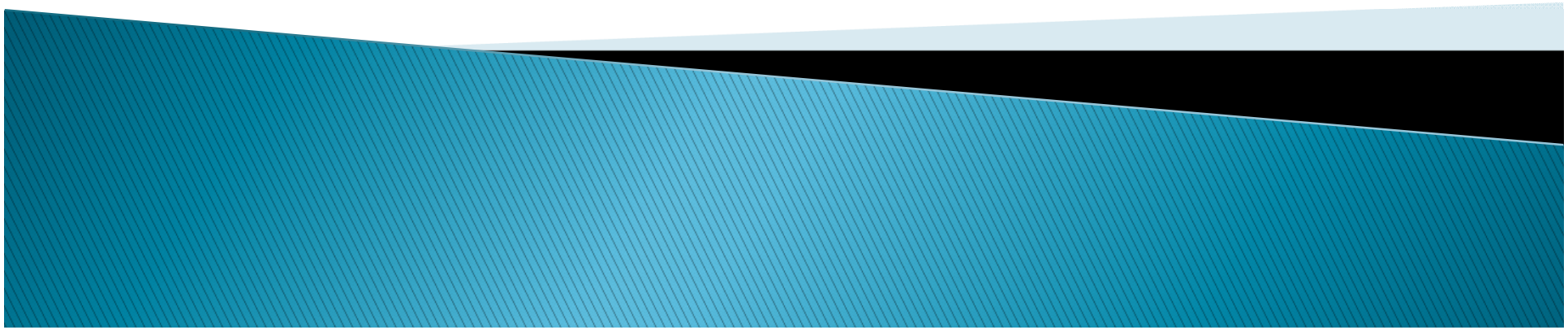
Institute of Software
Chinese Academy of Sciences

iFeed: the Input-Feed AE Modes

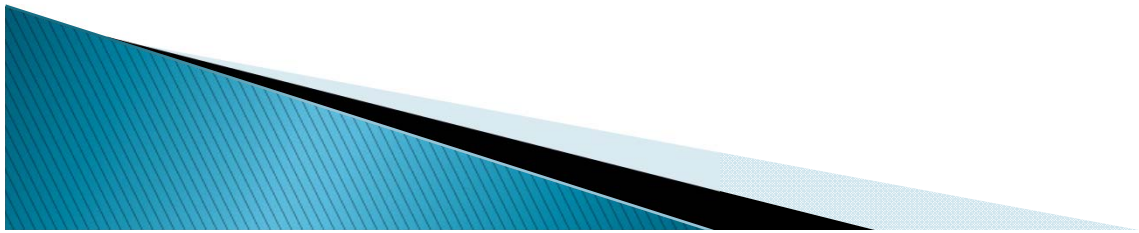
Liting Zhang

FSE 2013, Rump Session

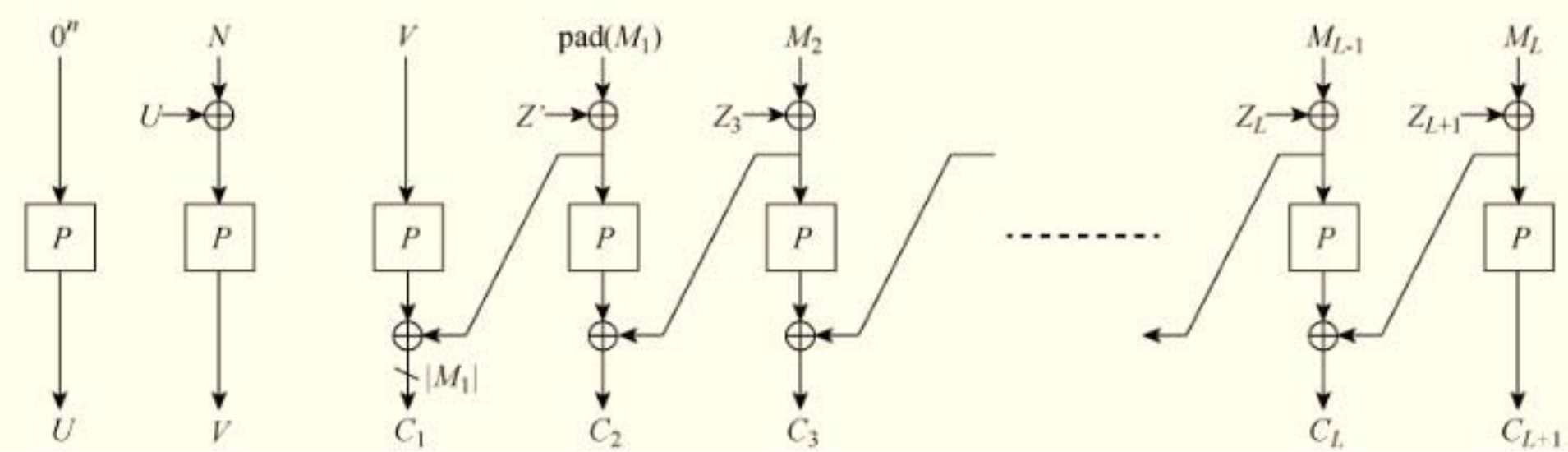


Basic Idea

- Aim – avoid P^{-1} in the one-pass AE modes
- Method – feed the inputs to BCs forward or backward to the outputs of BCs
- iFeed family includes iForward and iBackward



iForward: AEnc(N,M)=$C_1 \ldots C_{L+1}$



Nonce-based

- One-Pass
- Single-Keyed
- Parallel Calling to P

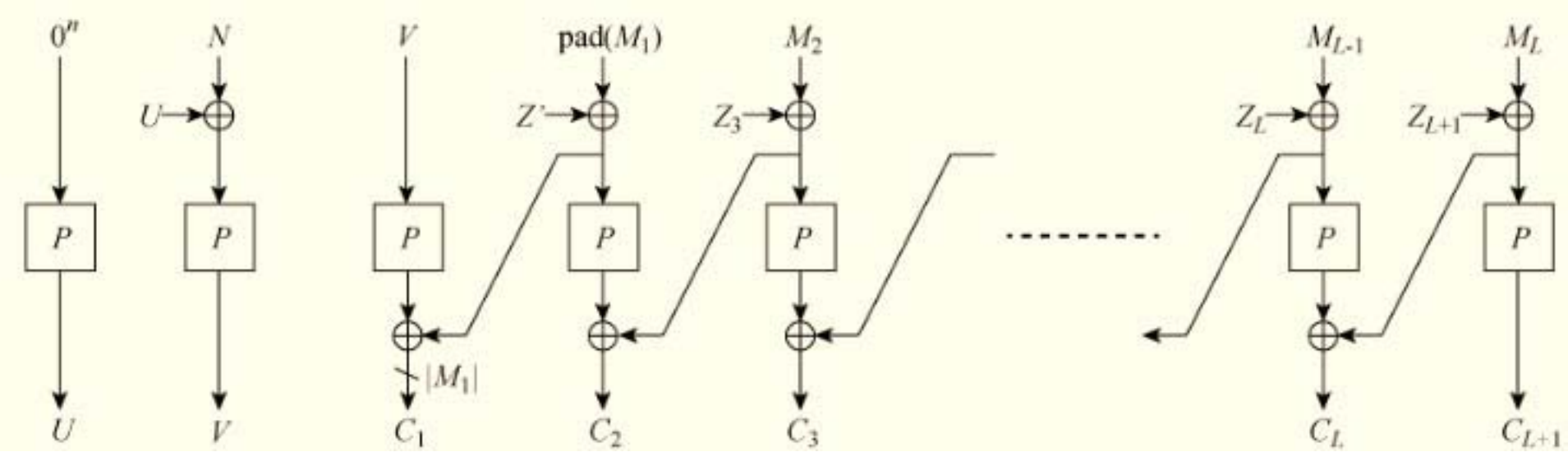
Not on-line

Length-Preserving

Z_i = MaskGen(U,V), like OCB

Z' = Z_1 or Z_2

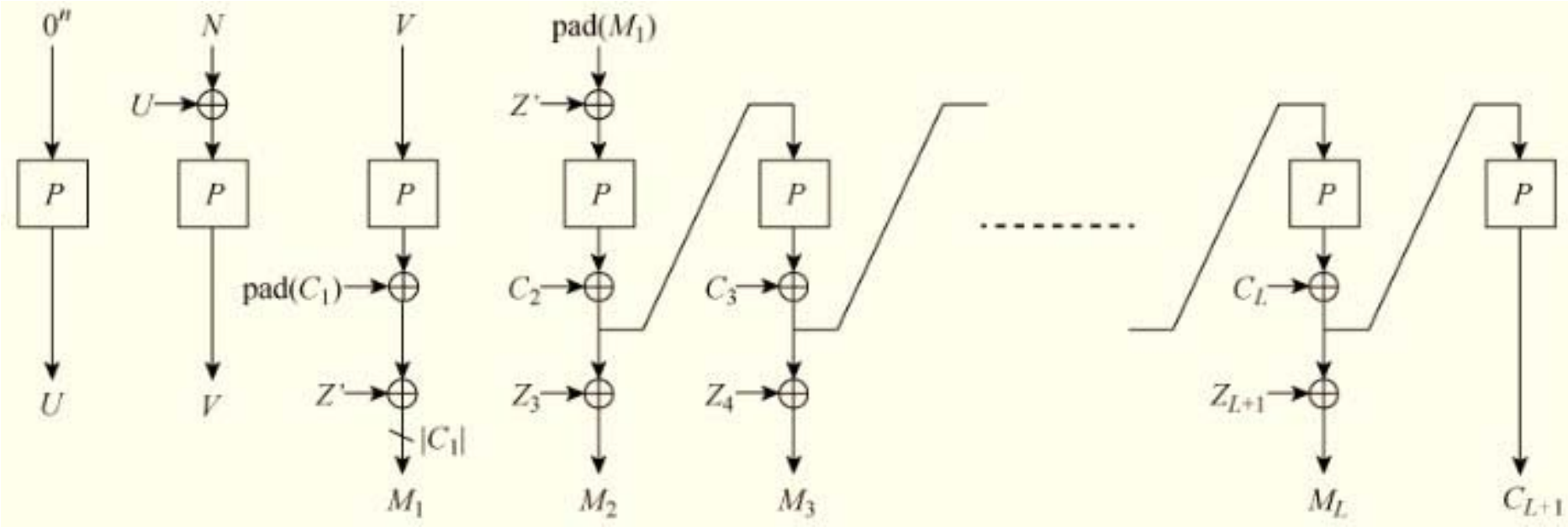
iForward: AEnc(N,M)=$C_1 \ldots C_{L+1}$



- Priv for M_1 M_2 M_3 M_L
- Auth for M_1 M_2 M_{L-1} M_L

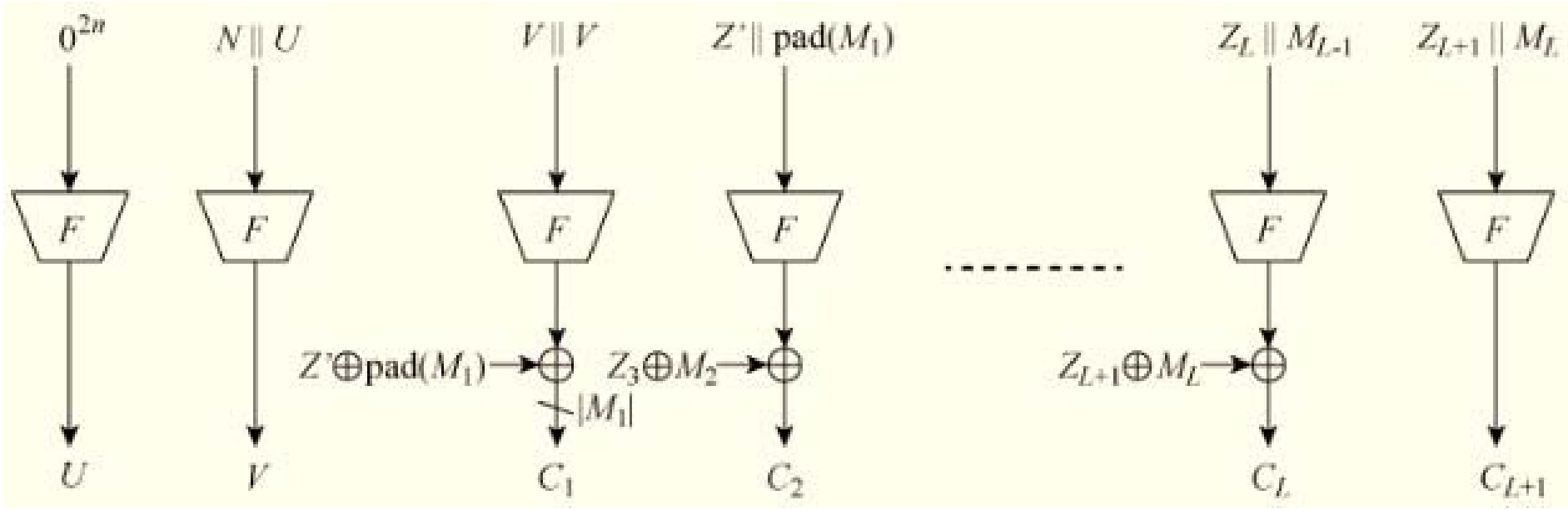
New method to combine Priv and Auth

iForward: ADec(N,C)=M or ⊥



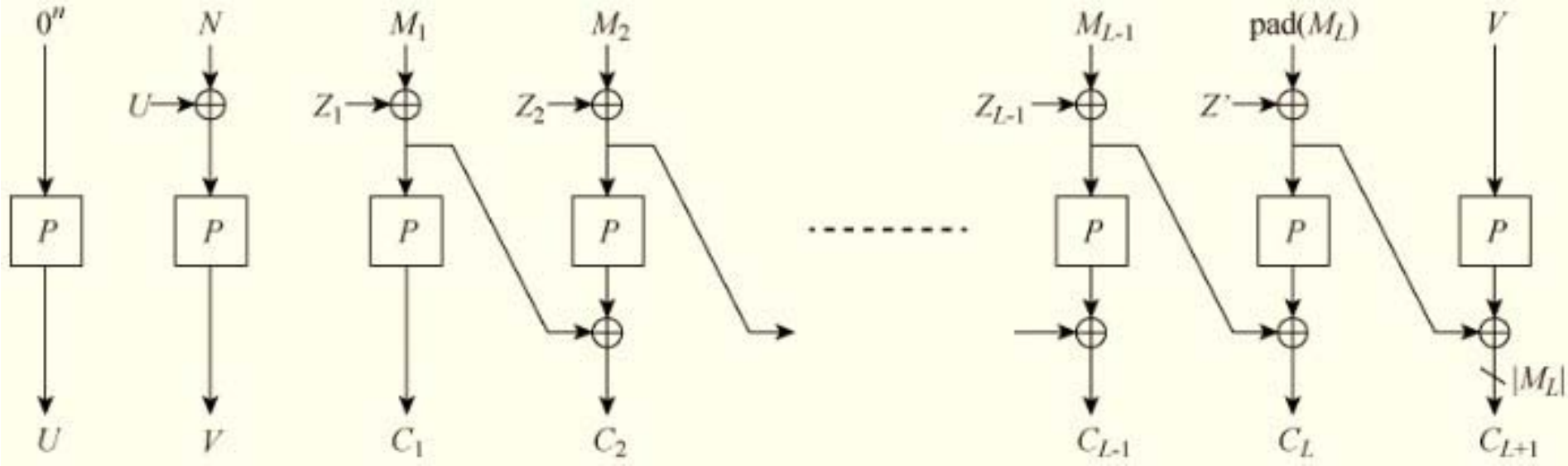
- No need for P^{-1} → Requiring No SPRP
- Sequential Calling to P

Generalizing iForward



- Using compression functions

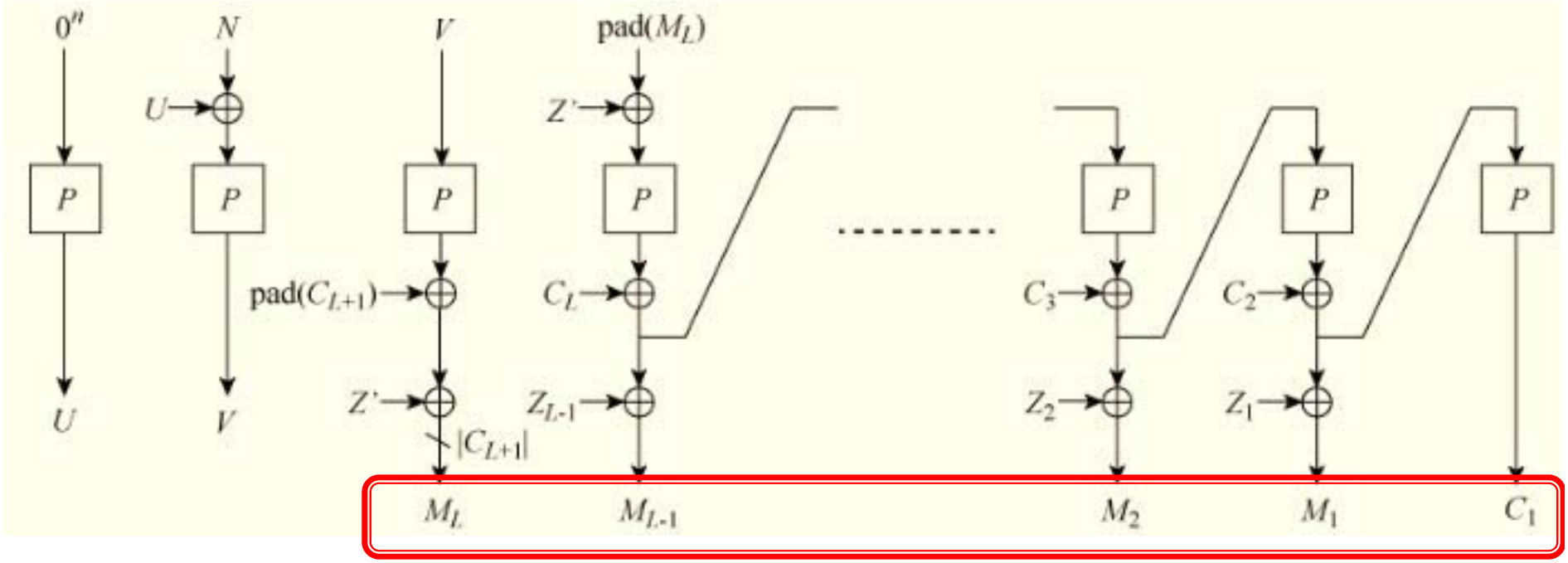
iBackward: Another iFeed Mode



- On-line and length-preserving

Z_i = MaskGen(U,V), like OCB
Z' = Z_L or Z_{L+1}

iBackward: Another iFeed Mode



- But inverse order in ADec(N,C)= M or $\perp$

Thanks

- The modes are still in adjusting
- All comments are welcome
-  liting.zhang@hotmail.com

Institute of Software
Chinese Academy of Sciences