Different Features of ELmD, EME Based Authenticated Encryption Schemes

Nilanjan Datta and Mridul Nandi
Indian Statistical Institute, Kolkata

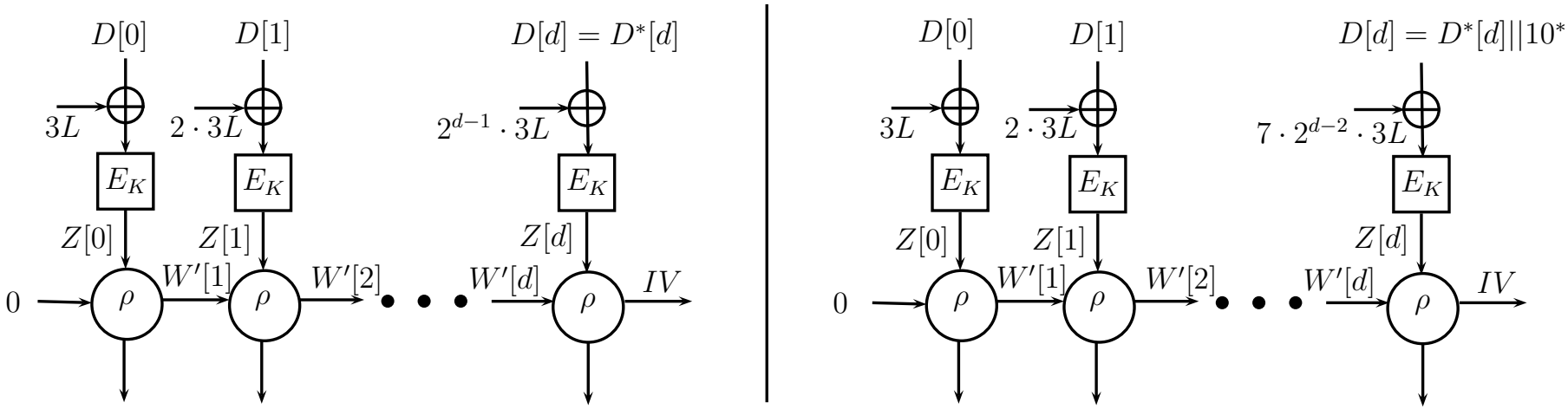
August 24, 2014
DIAC, UCSB

Outline

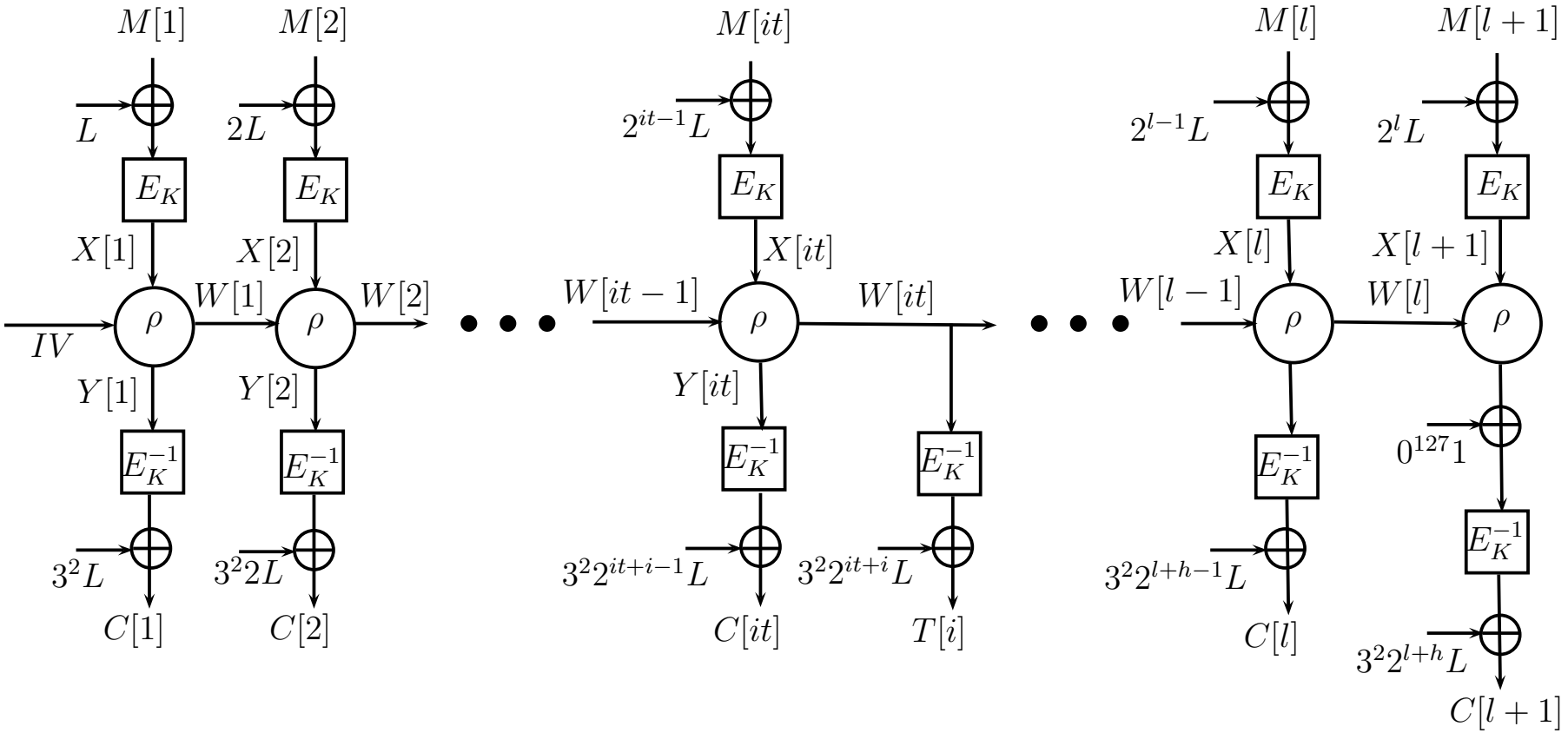
Design Structure of ELmD

1. Process Associated Data in PMAC like structure.
2. Process Message in the paradigm of Encrypt-Mix-Encrypt (e.g., COPA).
3. Expand the plaintext by applying checksum (xor of all message blocks). This leads ciphertext expansion.

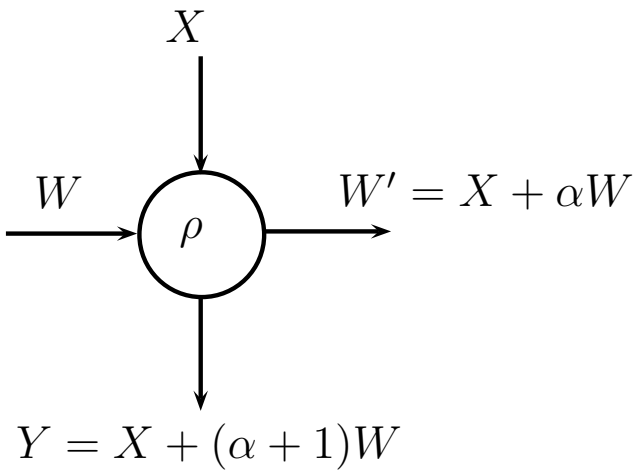
ELmD AE Scheme: Processing of AD



ELmD AE Scheme: Processing of Plaintext



Description of ρ function



Used to provide online linear mix function

$$Y[j] = X[j] + (\alpha+1)X[j-1] + \ldots + \alpha^{j-2}(\alpha+1)X[1] + \alpha^{j-1}(\alpha+1)IV$$

Parameters of ELmD

1. We use AES as a blockcipher E_K in the second layer. However, we make a choice of 5 or ten rounds of AES in the first layer.
2. We have provisions of intermediate tag (if required).
3. Instead of having exactly 128 bit final tags, we can provide up to 255 bits tag (so that ciphertext size is multiple of 128). This helps in faster decryption and verification in hardware.

Proposed Modification on Padding Rule

Submitted Padding Rule

$$M[l] = \begin{cases} (M^*[l] \,||\, 10^*) & \text{if } |M^*[l]| \neq 128 \\ M^*[l] & \text{else} \end{cases}$$

$$M[l+1] = \oplus_{i=1}^{l} M[i]$$

Proposed Modification

$$M[l] = \begin{cases} (M^*[l] \,||\, 10^*) \oplus (\oplus_{i=1}^{l-1} M[i]) & \text{if } |M^*[l]| \neq 128 \\ M^*[l] \oplus (\oplus_{i=1}^{l-1} M[i]) & \text{else} \end{cases}$$

$$M[l+1] = M[l]$$

Security Claim

Goal	$\mathsf{ELmD}_{(\mathsf{rd}_1,\mathsf{rd}_2),0,\mathsf{f}}$	$\mathsf{ELmD}_{(\mathsf{rd}_1,\mathsf{rd}_2),127,\mathsf{f}}$
confidentiality	62.8	62.8
integrity	62.4	62.3

Table: Table quantifying, for each of the recommended parameter sets, the intended number of bits of security : Here $((\mathsf{rd}_1, \mathsf{rd}_2), \mathsf{f}) \in \{((10, 10), 0), ((10, 10), 1), ((5, 10), 0), ((5, 10), 1)\}$.

Security Claim

- Theorem 3.1 : $\mathbf{Adv}^{\mathrm{opriv}}_{\mathsf{ELmD}_{(10,10),0,\mathsf{f}}}(A) \leq \eta(\sigma_{\mathrm{priv}}) + \frac{5\sigma^2_{\mathrm{priv}}}{2^n}$.
- Theorem 3.2 : $\mathbf{Adv}^{\mathrm{opriv}}_{\mathsf{ELmD}_{(10,10),127,\mathsf{f}}}(A) \leq \eta(\sigma_{\mathrm{priv}}) + \frac{6\sigma^2_{\mathrm{priv}}}{2^n}$
- Theorem 3.3 : $\mathbf{Adv}^{\mathrm{auth}}_{\mathsf{ELmD}_{(10,10),0,\mathsf{f}}}(A) \leq \eta(\sigma_{\mathrm{auth}}) + \frac{9\sigma^2_{\mathrm{auth}}}{2^n}$.
- Theorem 3.4 : $\mathbf{Adv}^{\mathrm{auth}}_{\mathsf{ELmD}_{(10,10),127,\mathsf{f}}}(A) \leq \eta(\sigma_{\mathrm{auth}}) + \frac{11\sigma^2_{\mathrm{auth}}}{2^n}$

Here $\eta(i)$ denotes the maximum AES advantage over all adversaries, making at most i queries. As full rounds of AES is used, we can assume $\eta(i)$ to be negligible.

Properties of EME based AE Schemes

Online

i^{th} block of ciphertext only depends on the first i blocks of plaintext.

Nonce Misuse Resistant

Cipher provides online security even if nonce is repeated.

Pipeline Implementable

As EME is parallel, the ciphers are expected to have the parallel nature and hence pipeline implementable.

Examples of other AE Schemes with EME Structure

- AES-COPA
- Marble
- NMR-Deoxys
- NMR-Joltik
- NMR-KIASU
- PRØST-COPA
- SHELL

No. of primitives used

d-block associated data Processing

ELmD requires d many block-cipher invocations.

l-block message Processing

ELmD requires $2l + 2$ many block-cipher invocations.

l-block message Processing (final block incomplete)

- Doesn't use of XLS or tag splitting.
- Similar treatment for incomplete, complete blocks and even when the number of blocks is one.

Parallelism and Uniformity

Processing of Message

Similar processing of message for full and incomplete final block messages.

Processing of Message and Ciphertext

Similar processing for both encryption and decryption. It would help to have low area combined implementation in hardware.

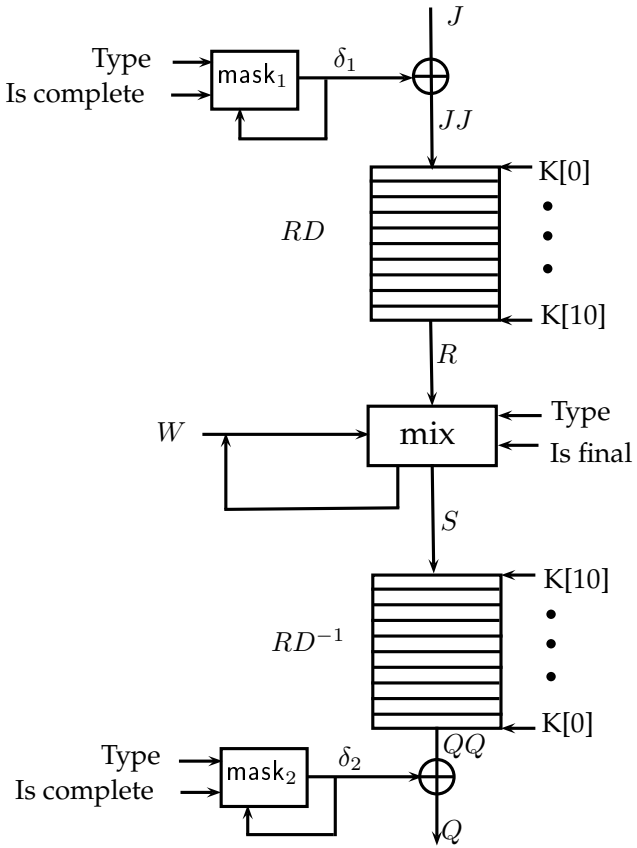
Processing of Associated Data

Similar processing of associated data. No bottleneck for the last block.

Performance of ELmE

Hardware Implementation

Enc-Dec Combined hardware implementation area is minimized.



Limited Buffer Scenario

Issues of Limited Buffer

- Low end devices has limited buffer.
- It may has to release unverified plaintext during decryption.

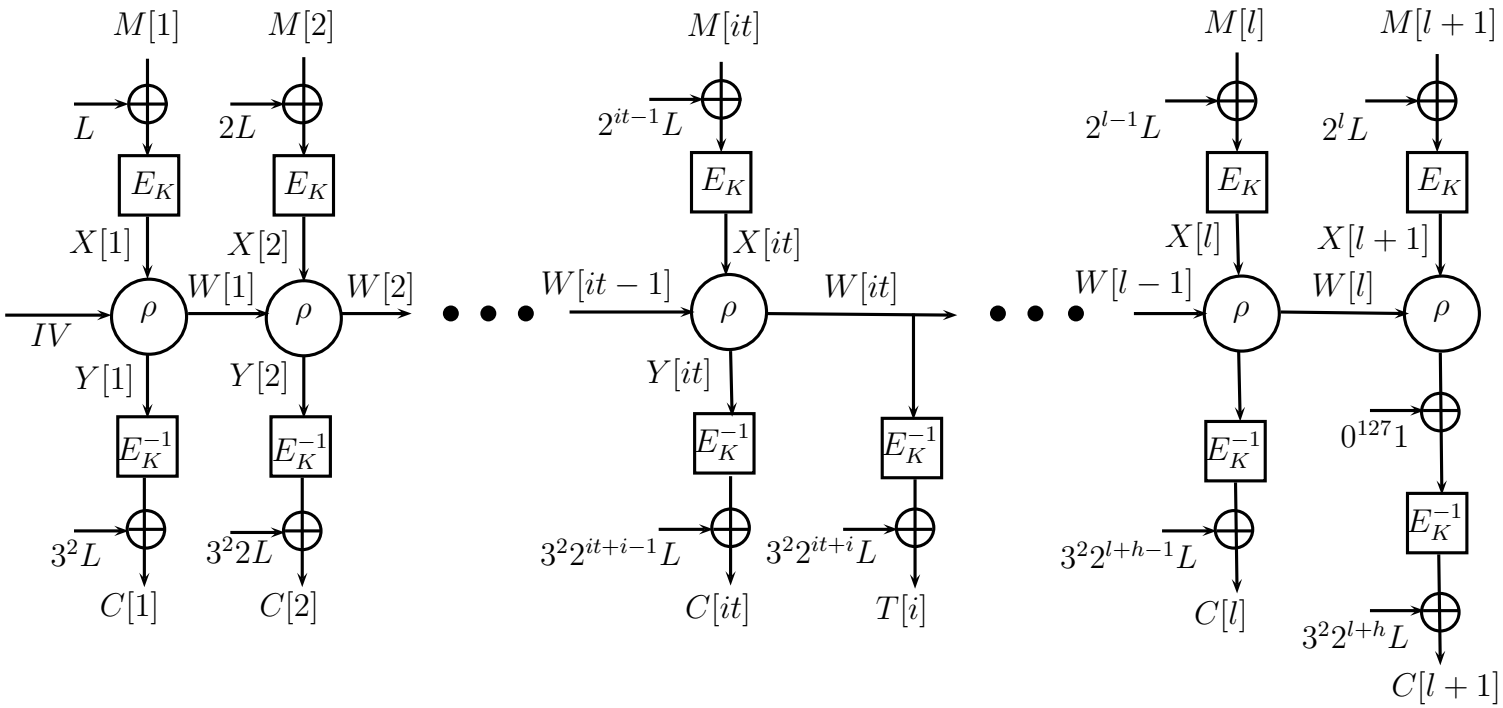
INT-RUP Security

- Adversary has access to unverified decryption oracle.
- OCB, AES-COPA: INT-RUP insecure. Does not work in straightforward manner for ELmD.

Solution: Intermediate Tag

stops releasing unverified plaintext.

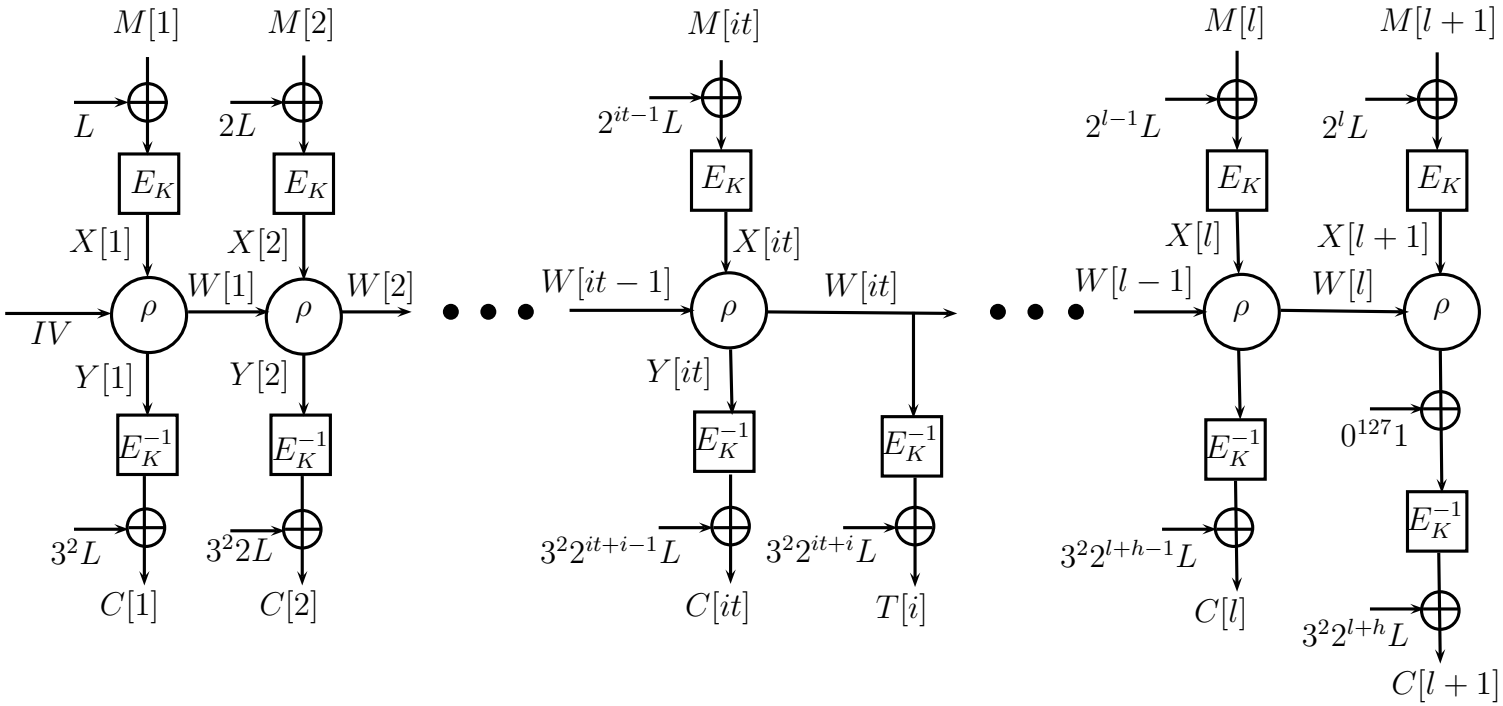
ELmD: Flexibility



Use as Online Encryption/Decryption only Scheme

- Set associated data as empty and $IV = 1$.
- Return $C[1..e]$.

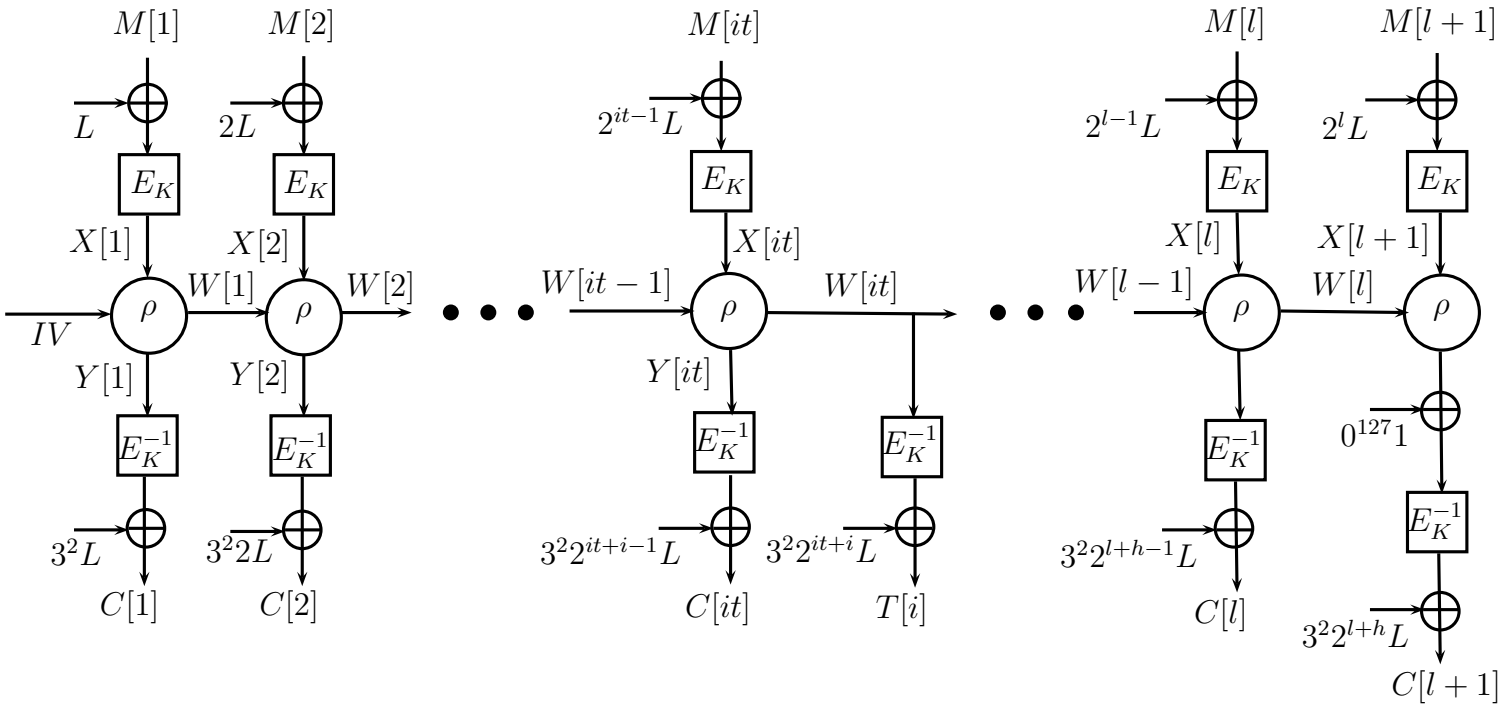
ELmD: Flexibility



Use as MAC only

- Set Associated data empty and $IV = 1$.
- Return (M, T).

ELmD: Flexibility



Use to check integrity of associated data only

- Set message as empty and checksum $M[1] = 0$.
- Return (D, T).

Questions and Comments