Lilliput-AE, a new Encryption Algorithm

Pierre GENARD
Université de Lorraine
January 20, 2024

Lightweight Crypto Competition Candidate

Pierre GENARD
Université de Lorraine
January 20, 2024

Part 1

Block Ciphers

NIST

Part 1

Block Ciphers

Block Cipher

Block Cipher

$\mathbf{E_K} : \{0,1\}^n \Rightarrow \{0,1\}^n$
Family of permutations indexed by a secret key K where n is the block size.

Tweakable Block Cipher : TBC

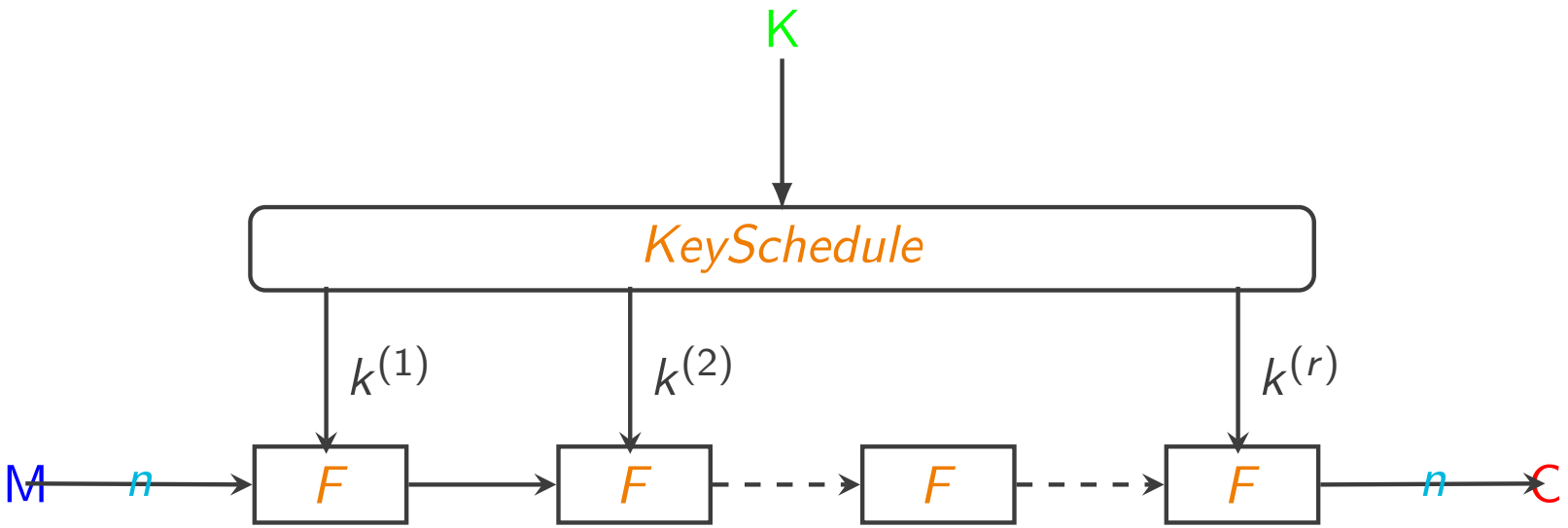
TBC is a family of permutations parametrized by a secret key K and a tweak value T.

Authenticated Encryption : AE

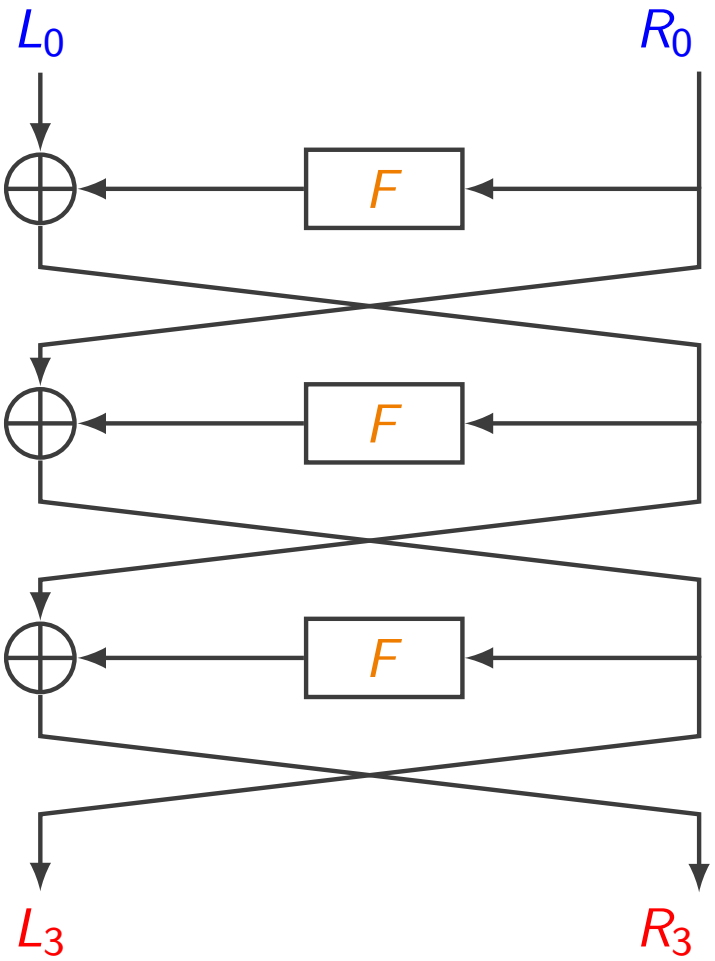
Encryption scheme that assures both data confidentiality and authenticity.

Block Cipher

- Sequence of r iterations (rounds) on n bits blocks.
- There is a need for modes (ECB, CBC, CTR, GCM, etc.).



Feistel Network



Substitution Permutation Network : SPN

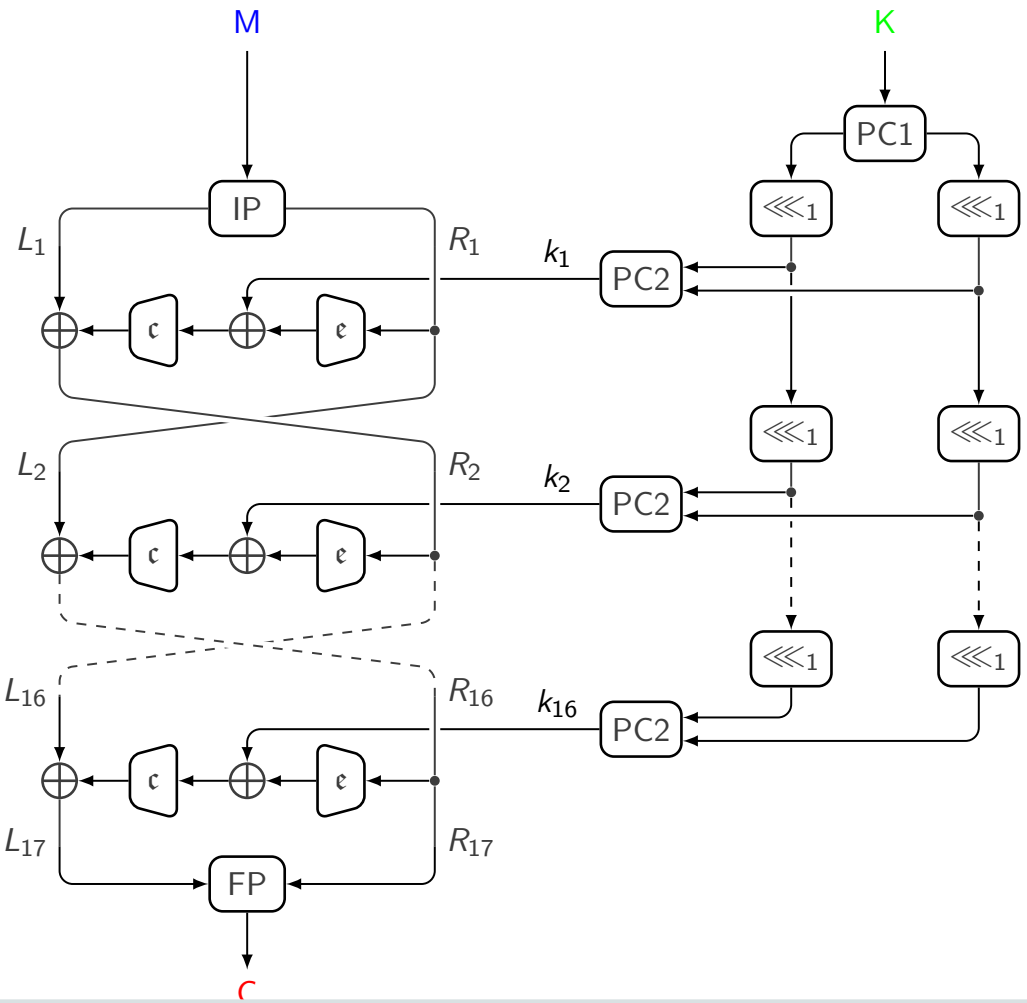
Substitution: S-Boxes
Permutation: P-Boxes
Typical one: DES

$$L_{i+1} = R_i \qquad R_{i+1} = L_i \oplus F(R_i)$$

Attacks

Linear cryptanalysis
Differential cryptanalysis

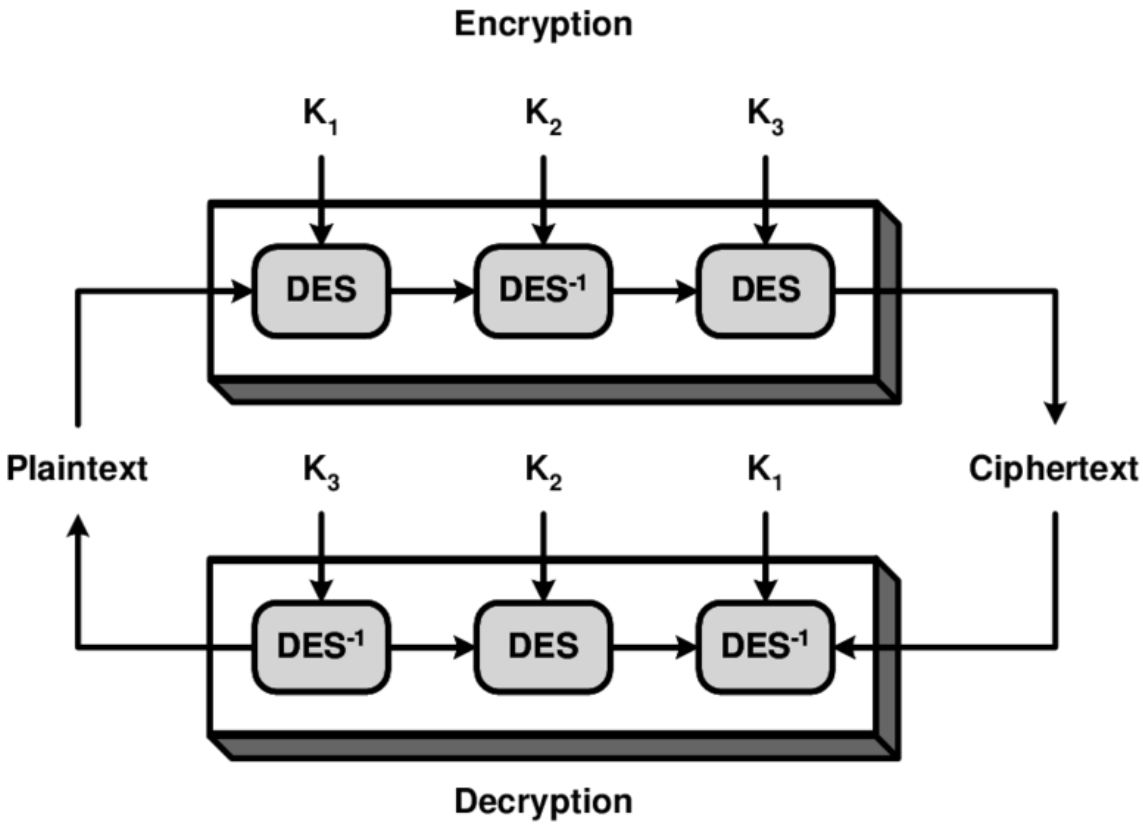
Data Encryption Standard : DES



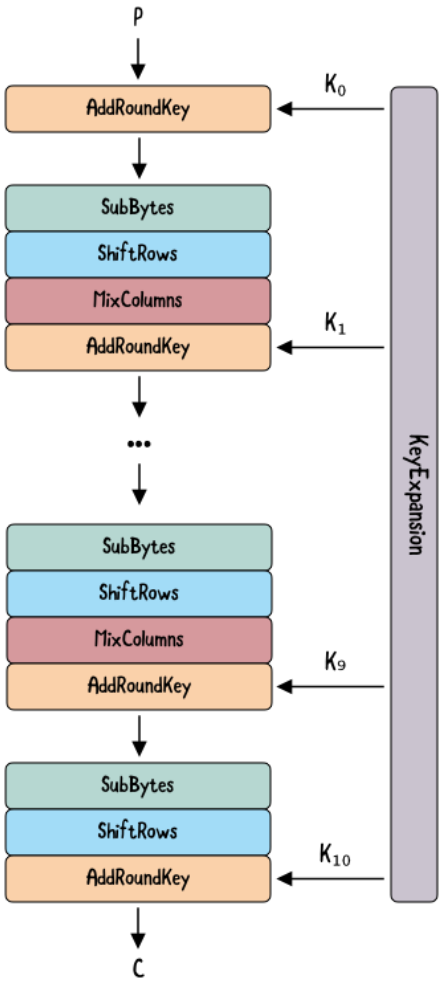
- Key size : 56 bits
- Blocks size : 64 bits
- Feistel network
- 16 rounds
- Triple-DES

$$\mathbf{C} = \mathbf{E}_{\mathbf{K}_3}(\mathbf{D}_{\mathbf{K}_2}(\mathbf{E}_{\mathbf{K}_1}(\mathbf{M})))$$

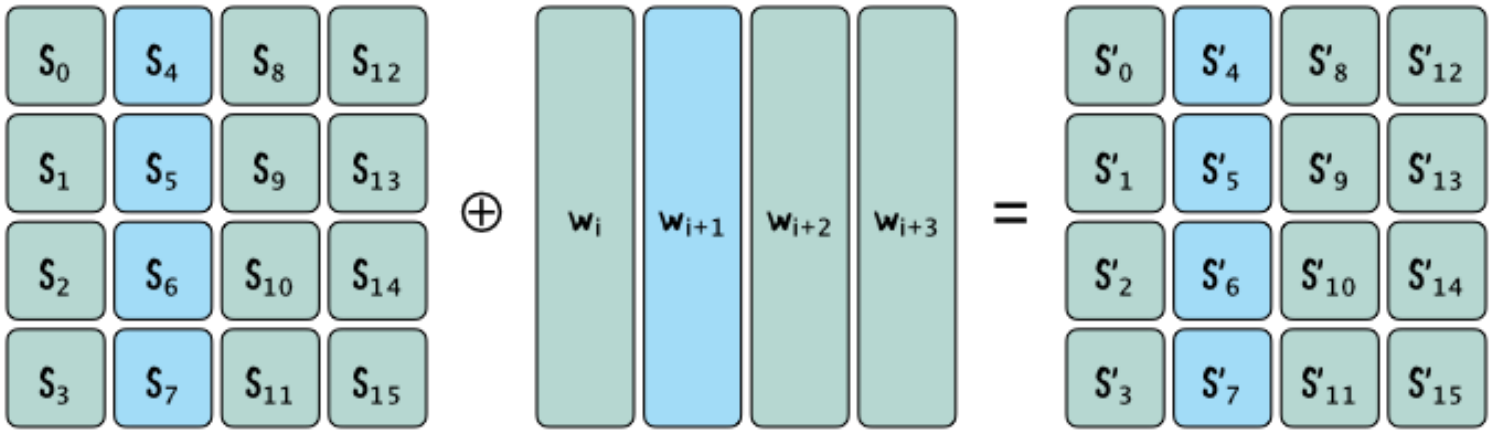
Triple DES : Overview



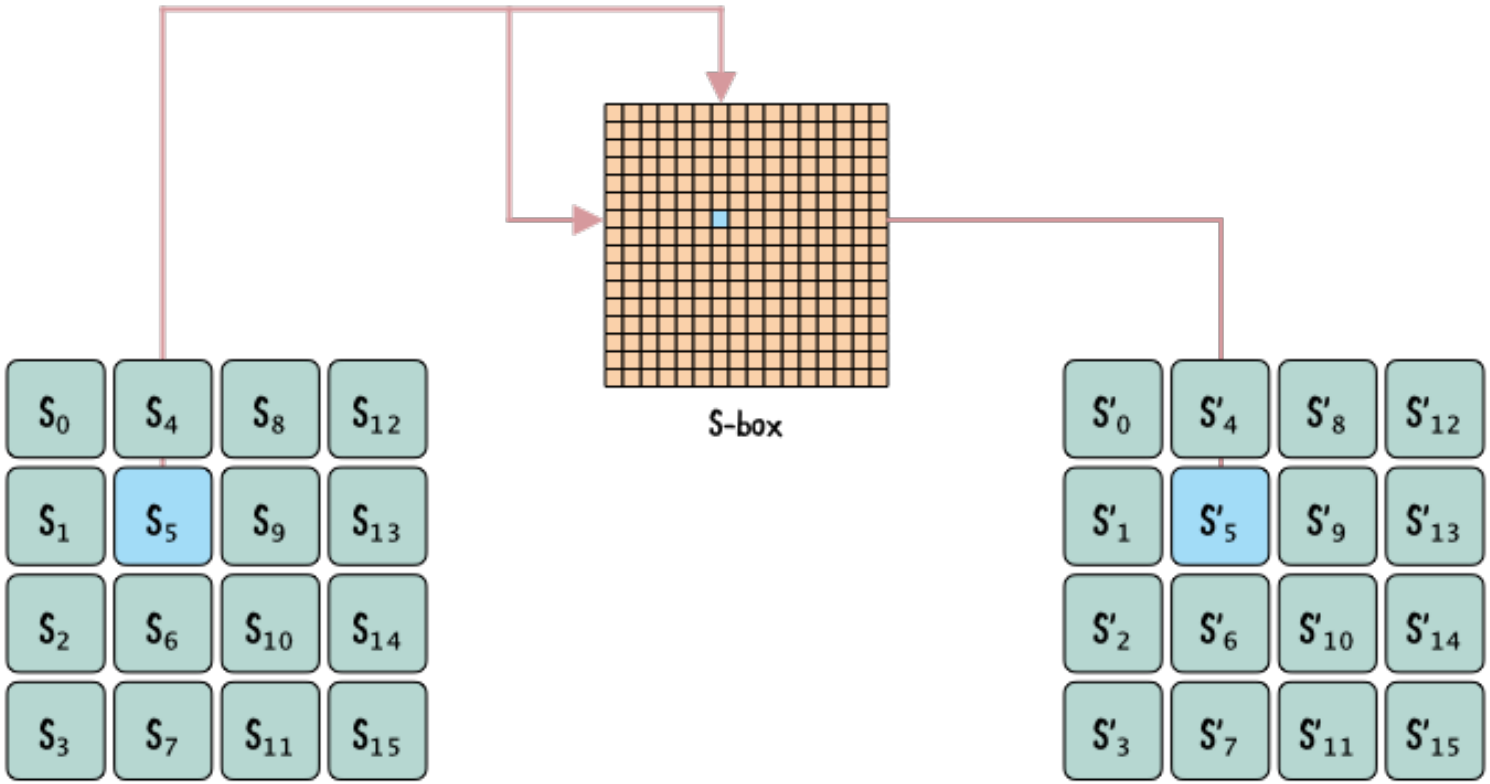
Advanced Encryption Standard : AES Encryption



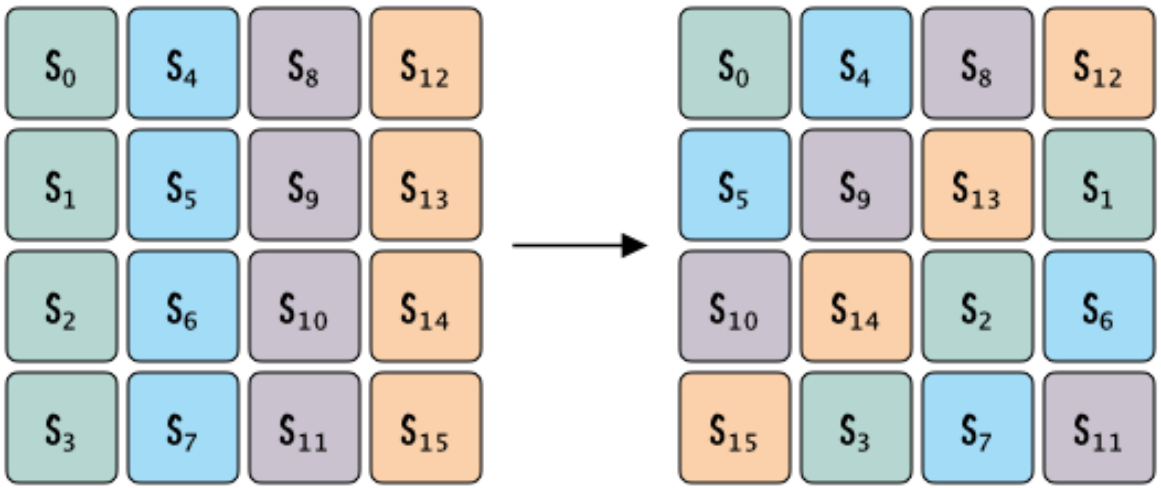
Advanced Encryption Standard : AddRoundKey



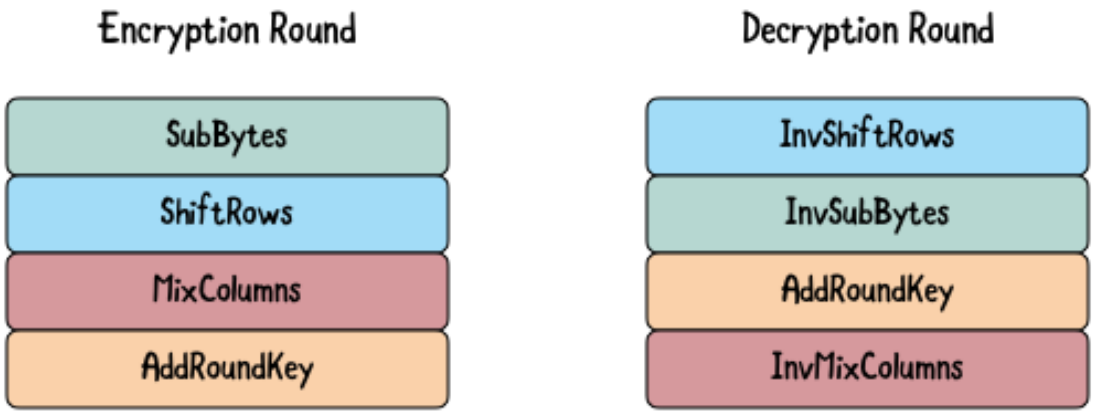
Advanced Encryption Standard : SubBytes



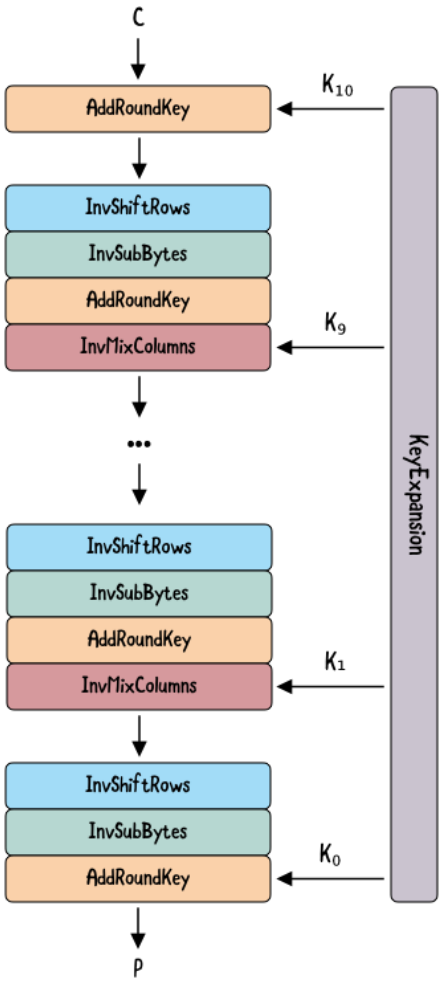
Advanced Encryption Standard : ShiftRows



Advanced Encryption Standard : AES Round



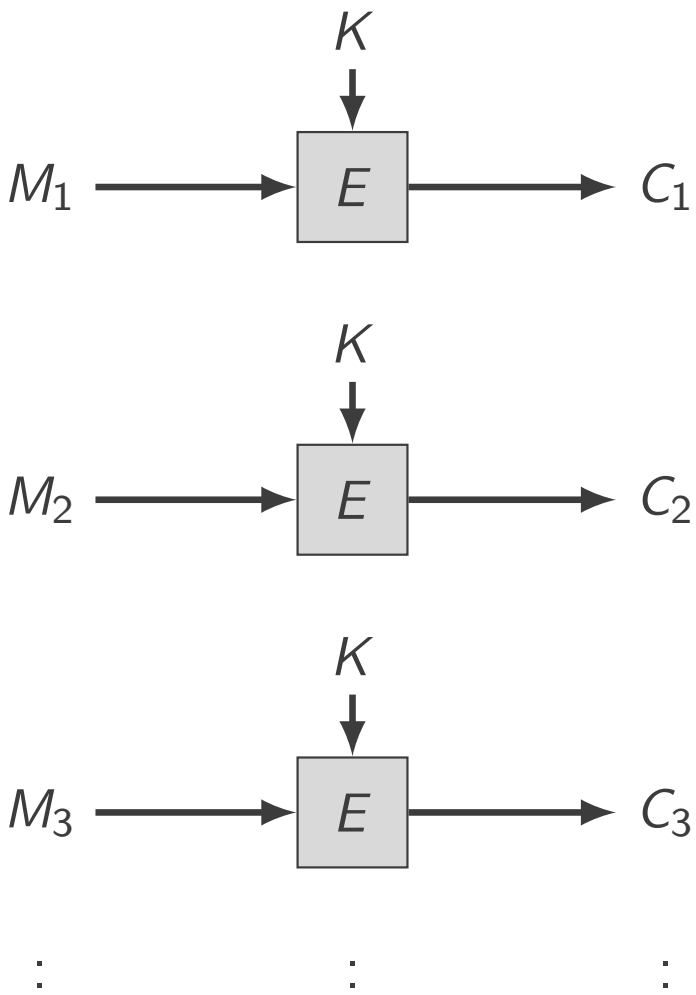
Advanced Encryption Standard : AES Decryption



Part 1

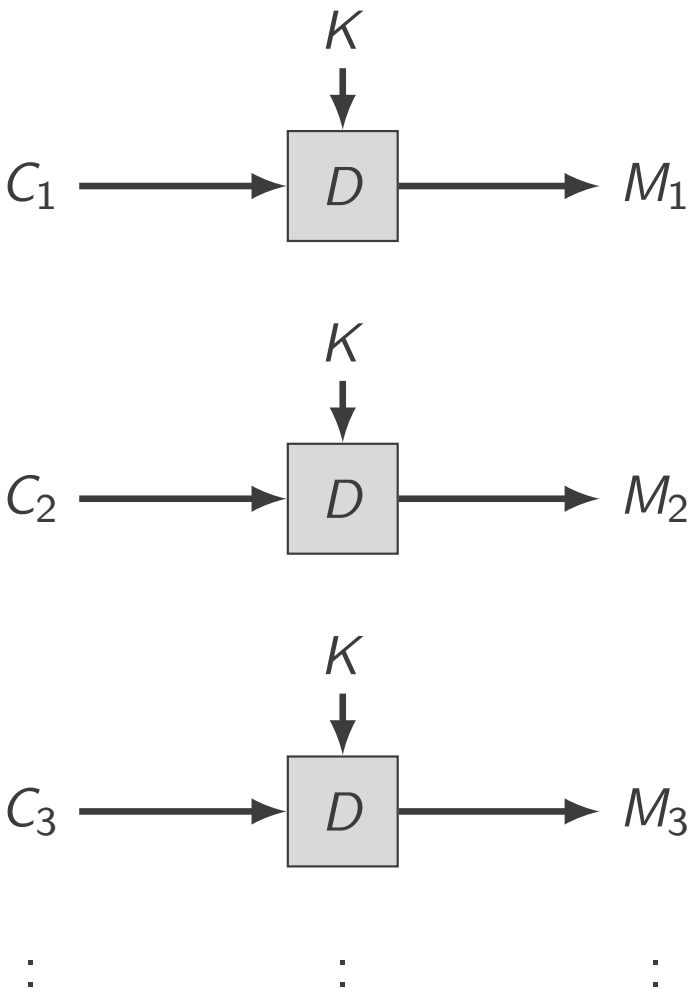
Block Ciphers

Electronic Code Book : ECB Encryption



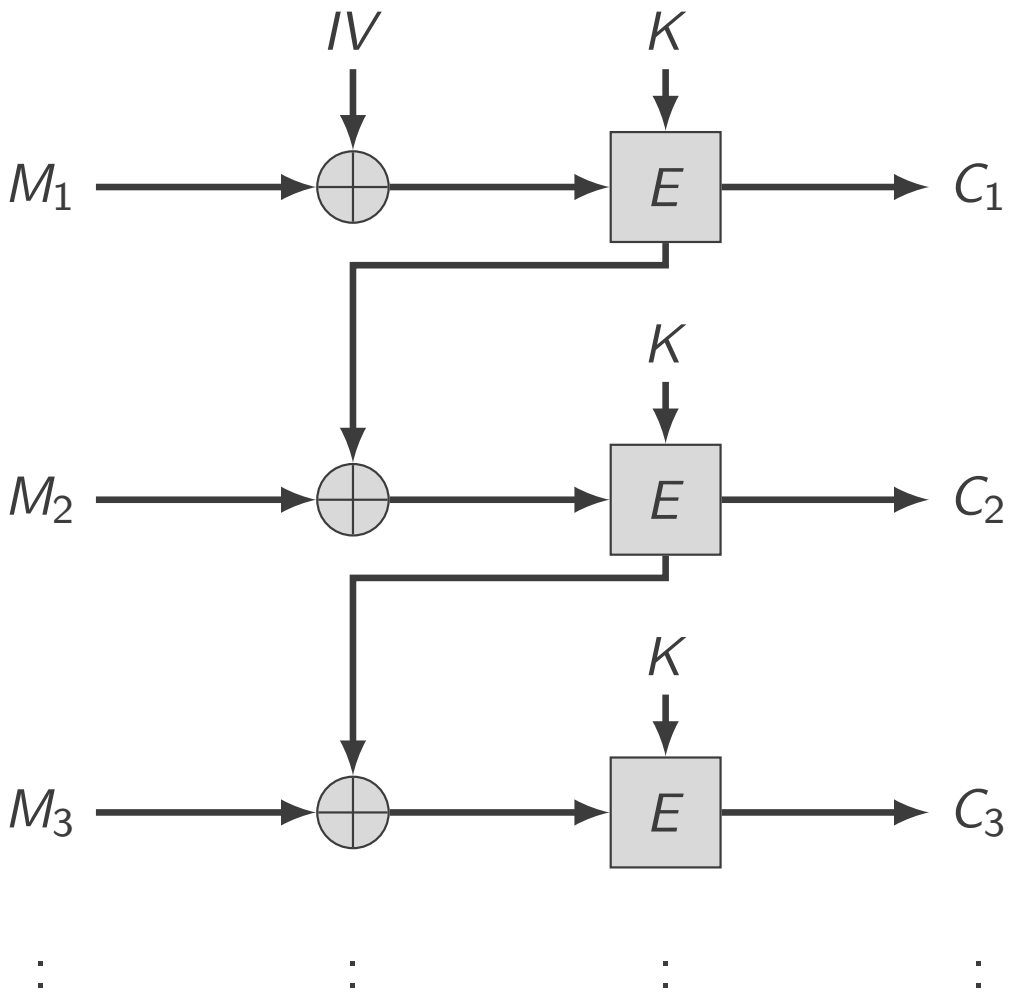
- Never use this !
- Parallel
- Random access

Electronic Code Book : ECB Decryption



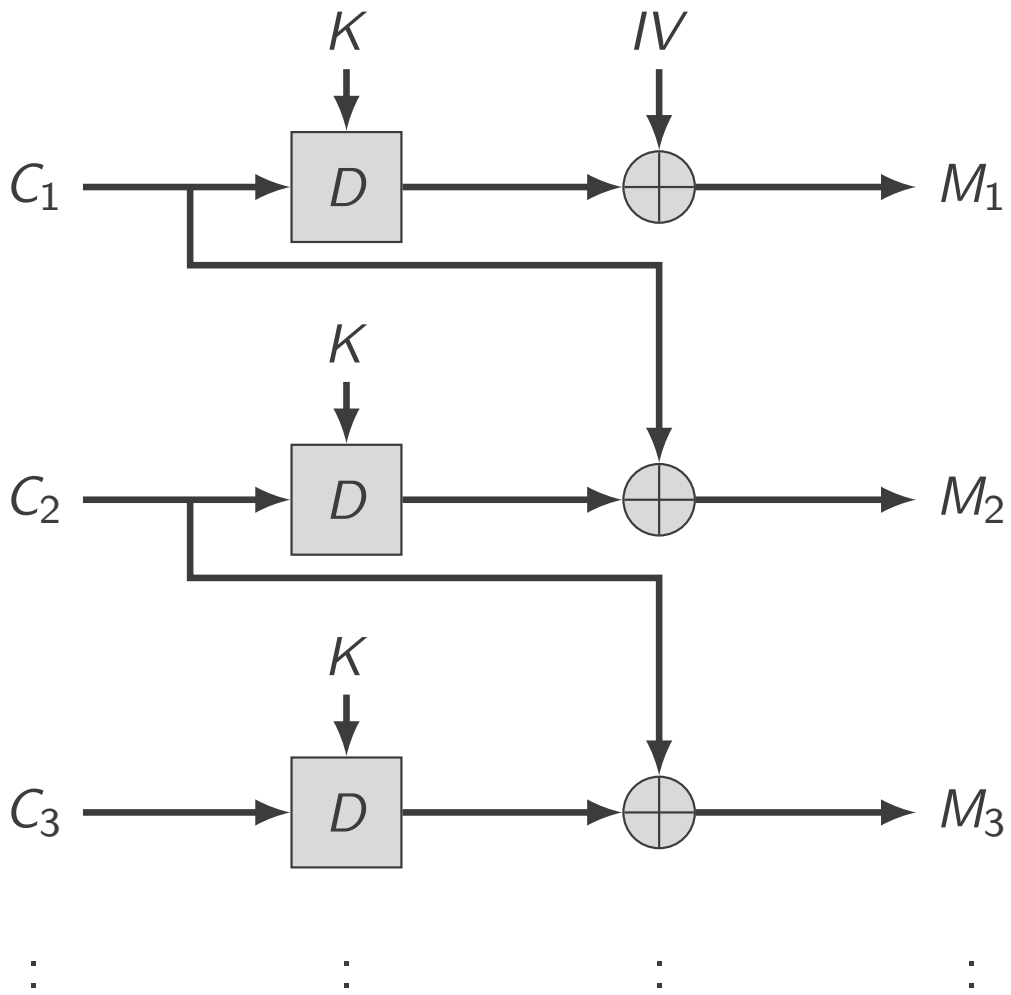
- Parallel
- Random access

Cipher Block Chaining : CBC Encryption



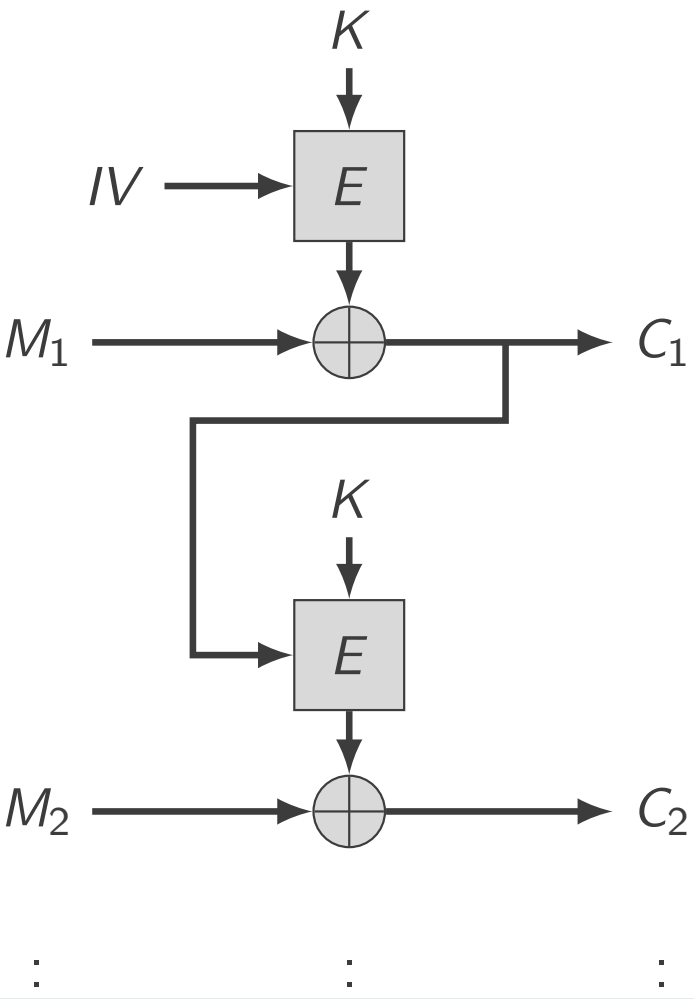
- Sequential
- Padding flaws

Cipher Block Chaining : CBC Decryption



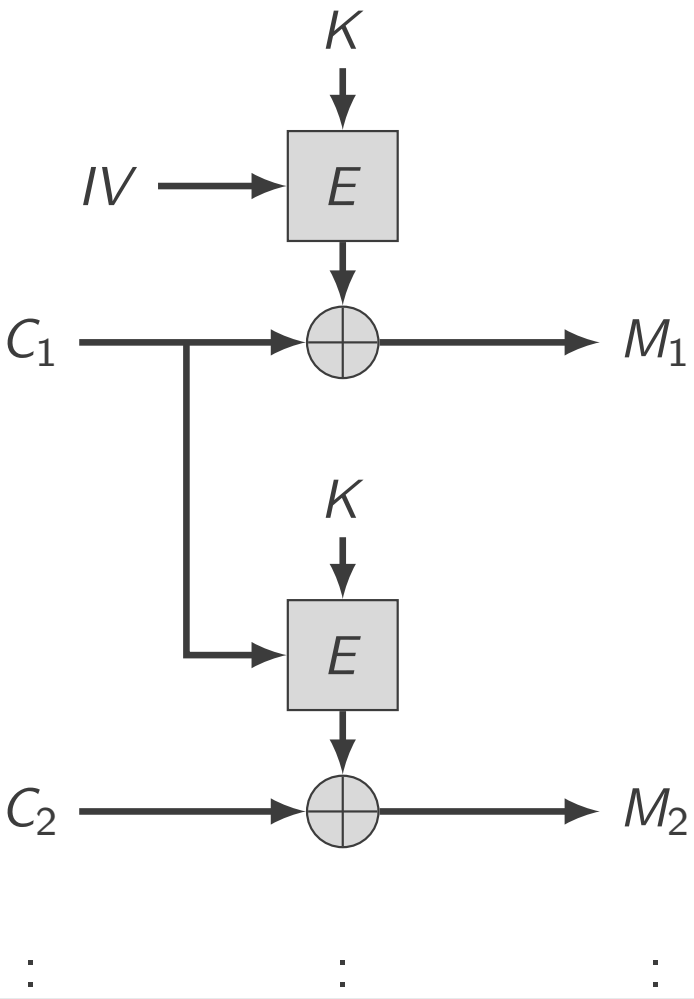
- Parallel

Cipher Feed Back : CFB Encryption



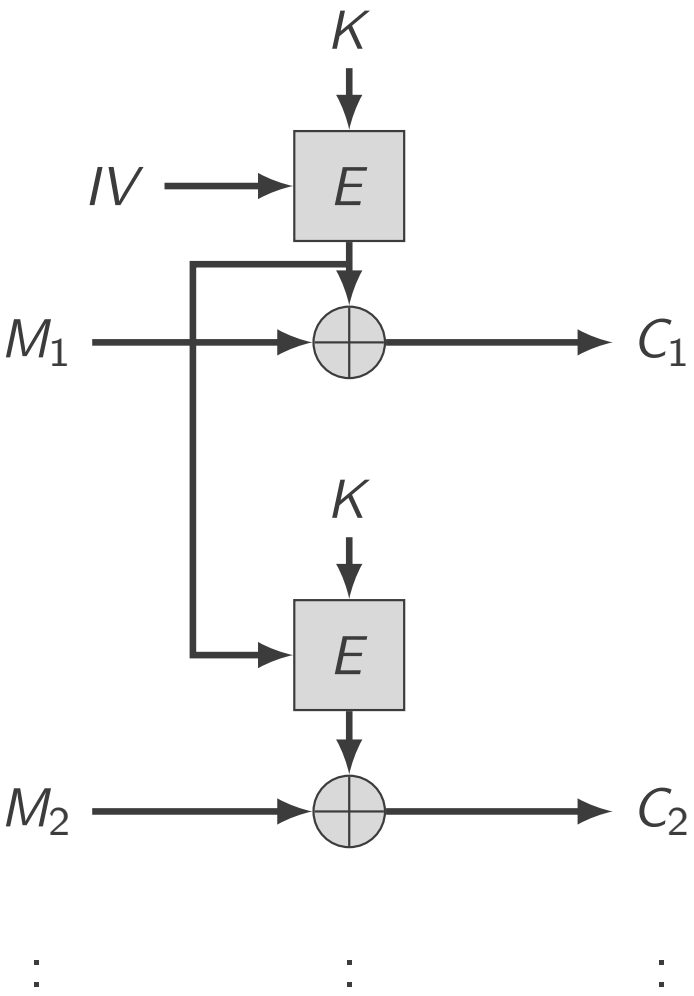
- Sequential
- Random access

Cipher Feed Back : CFB Decryption



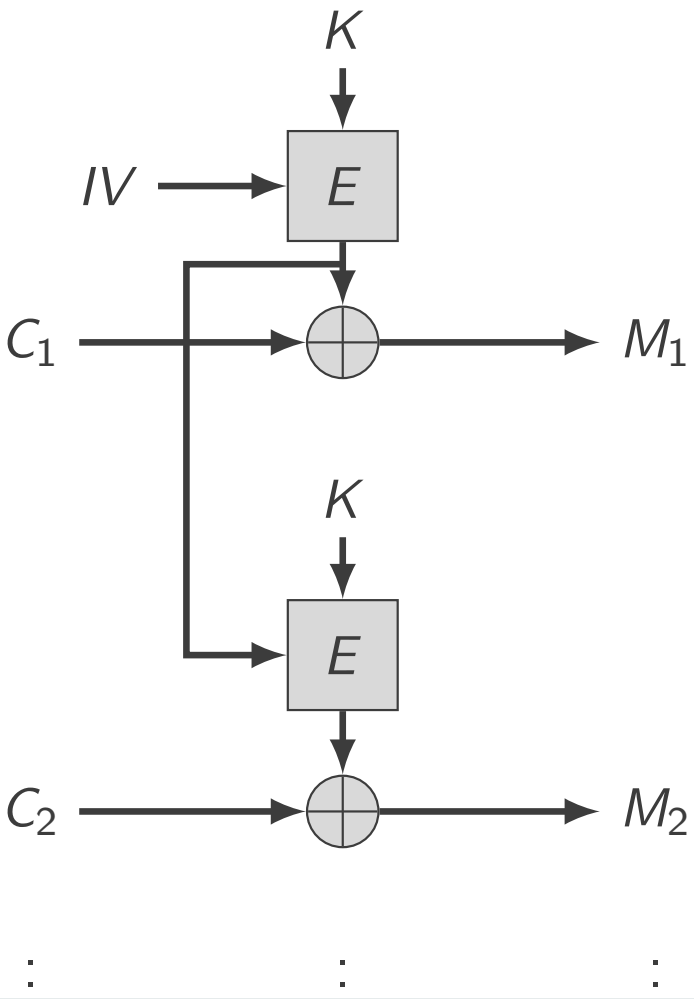
- Parallel
- Random access

Output Feed Back : OFB Encryption



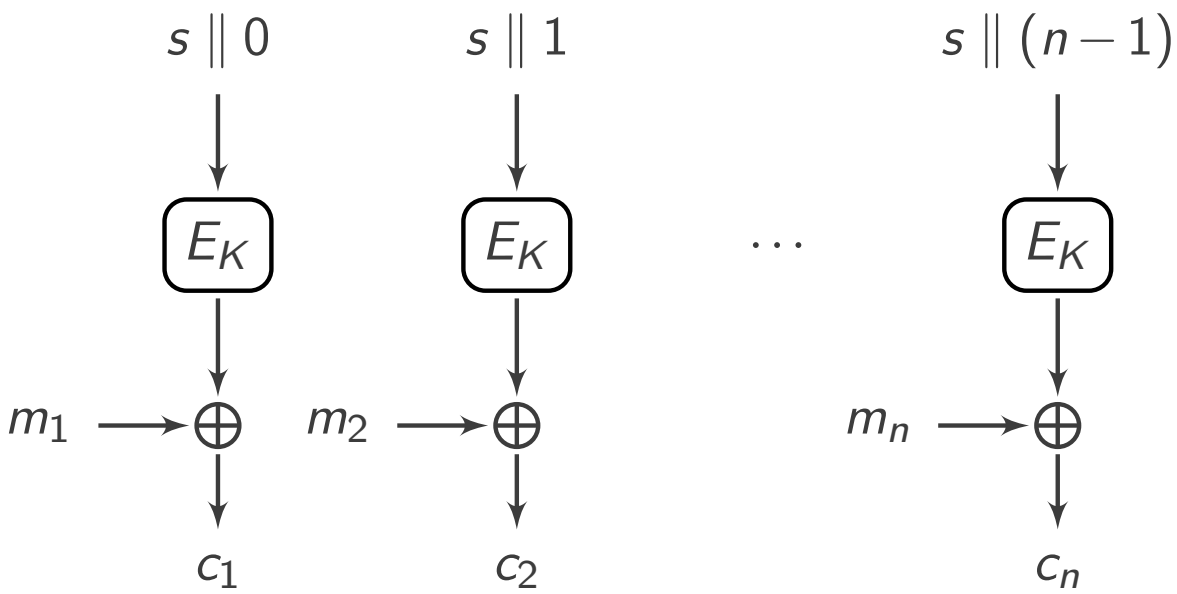
- Sequential

Output Feed Back : OFB Decryption



- Sequential

Counter : CTR Encryption



Part 2

Lilliput-AE

Part 2

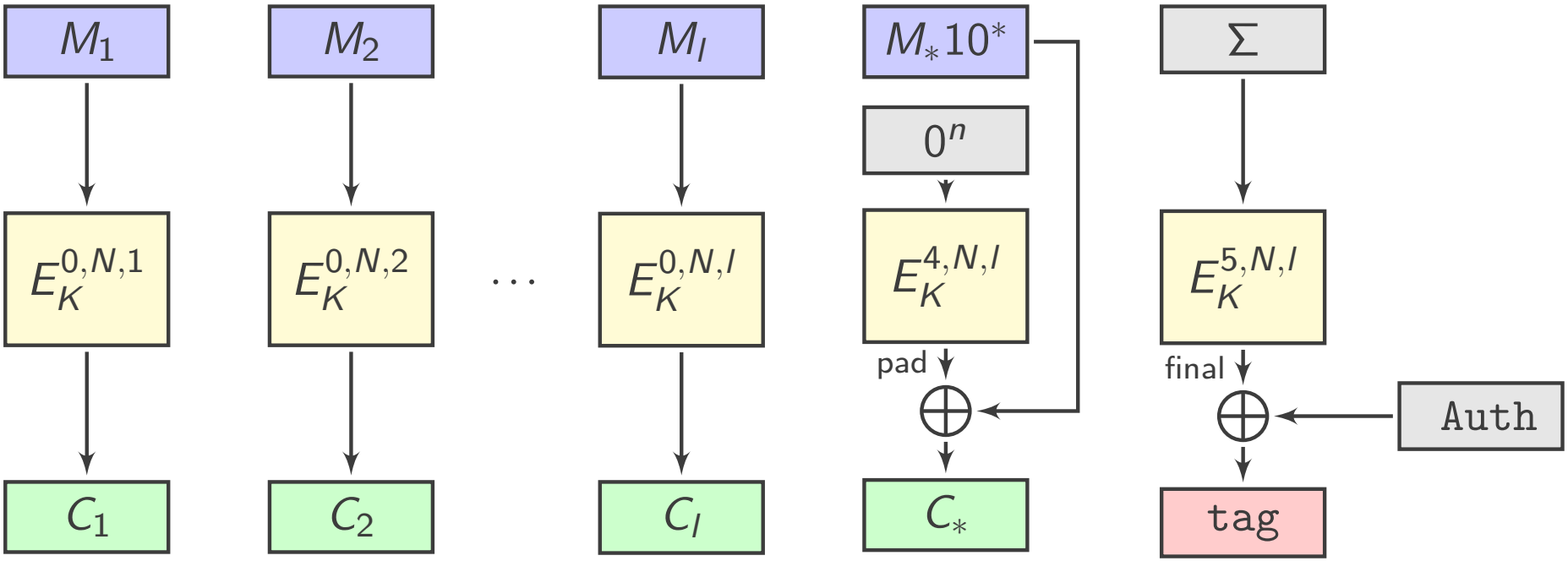
Lilliput-AE

Two Authenticated Encryption Modes

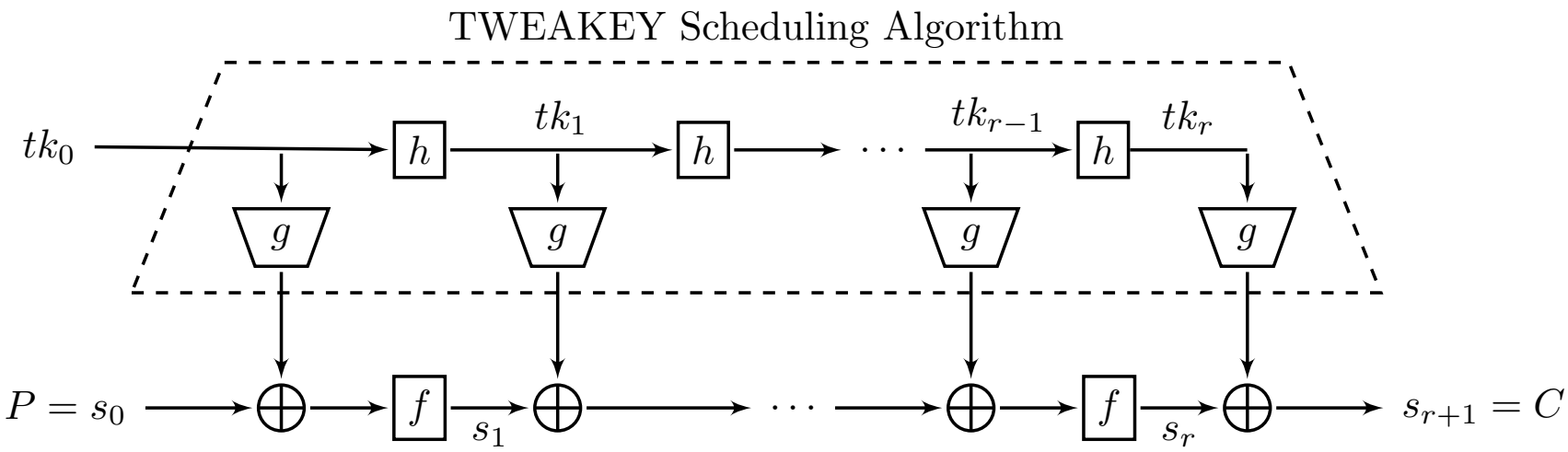
- Lilliput-I: nonce-respecting mode corresponding with ΘCB3.
- Lilliput-II: nonce-misuse resistant mode corresponding with SCT-2.

Name	k	t	n	|N|	τ
Lilliput-I-128	128	192	128	120	128
Lilliput-I-192	192	192	128	120	128
Lilliput-I-256	256	192	128	120	128
Lilliput-II-128	128	128	128	120	128
Lilliput-II-192	192	128	128	120	128
Lilliput-II-256	256	128	128	120	128

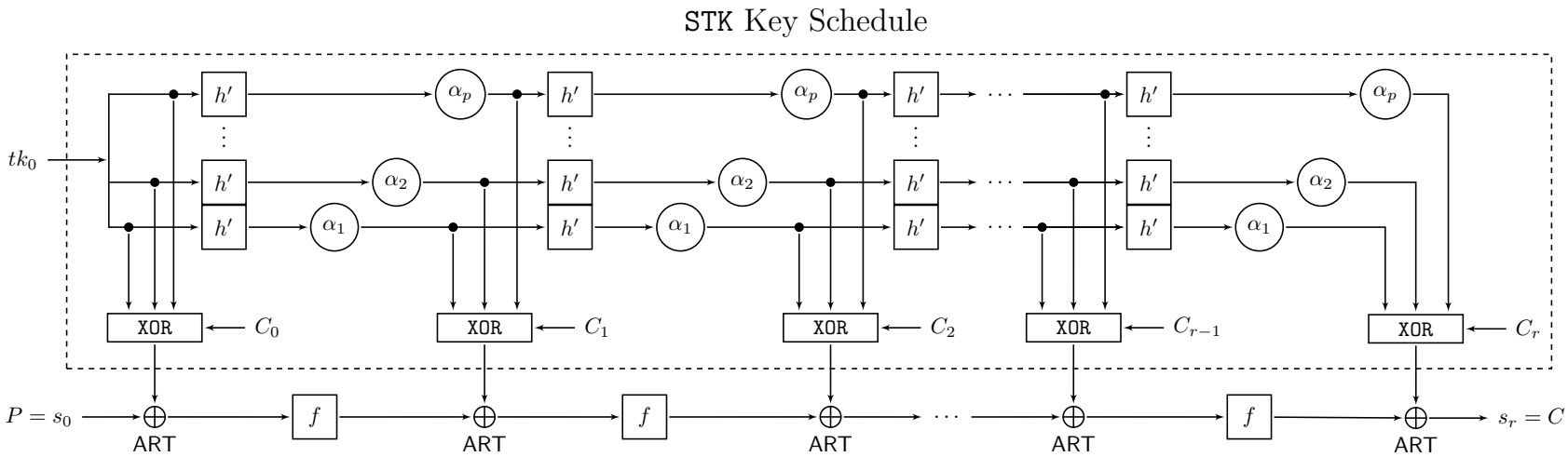
AE with a Tweakable Block Cipher



TWEAKEY Schedule



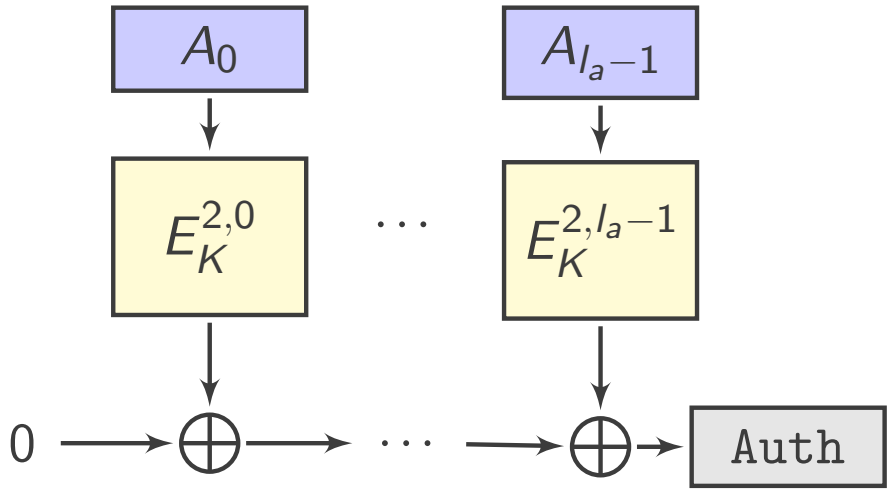
STK Key Schedule



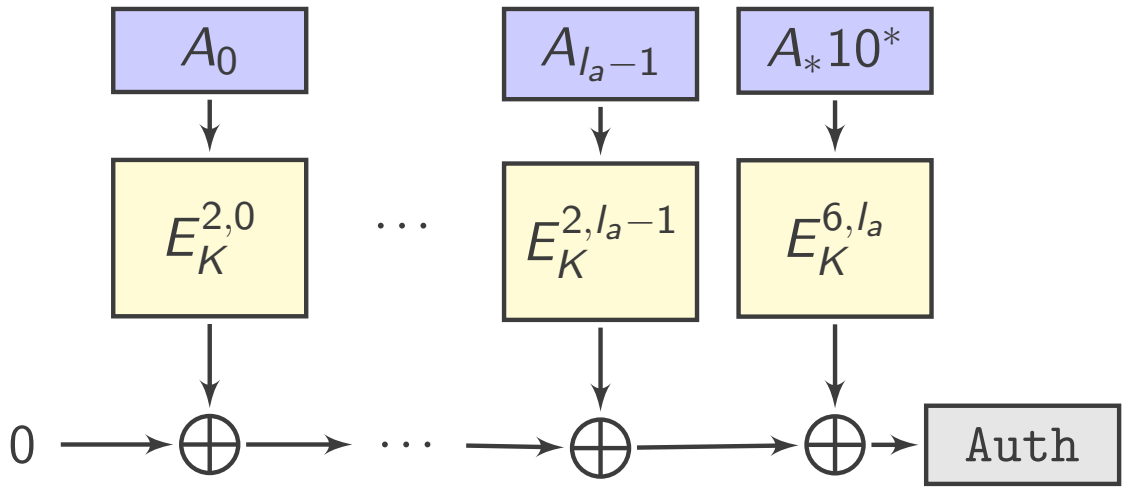
Part 2

Lilliput-AE

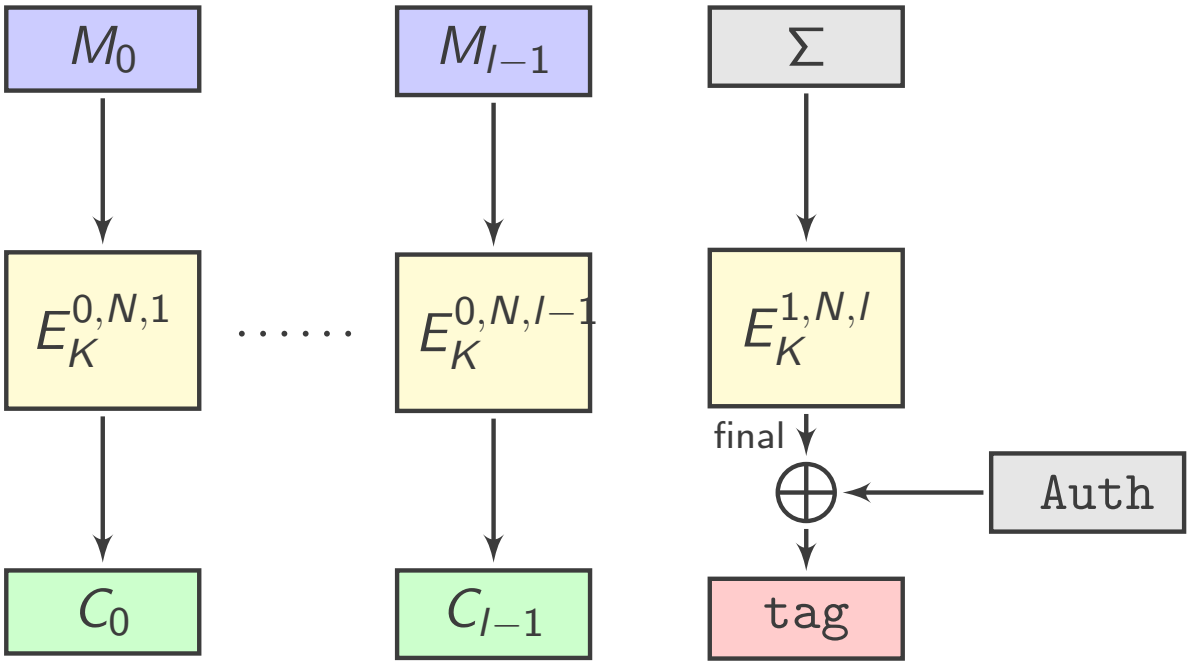
Associated Data : Without Padding



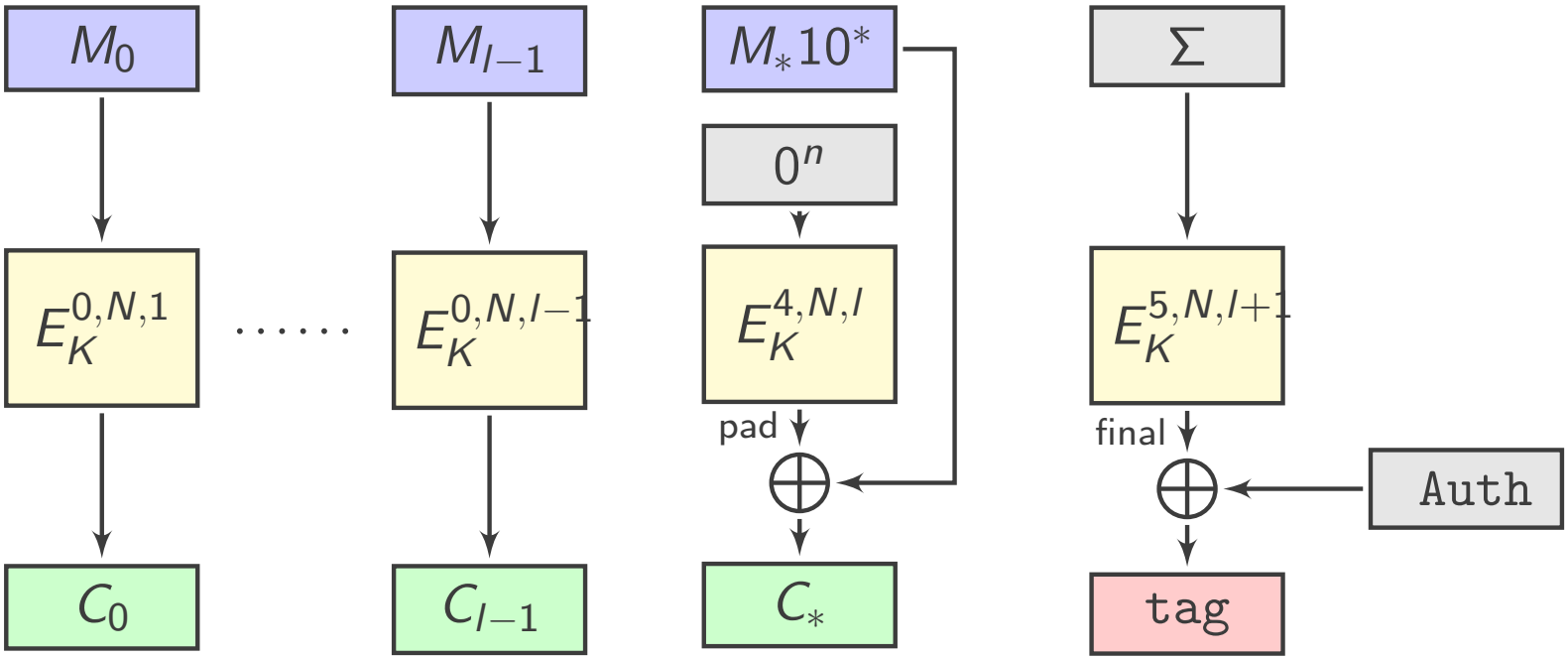
Associated Data : With Padding



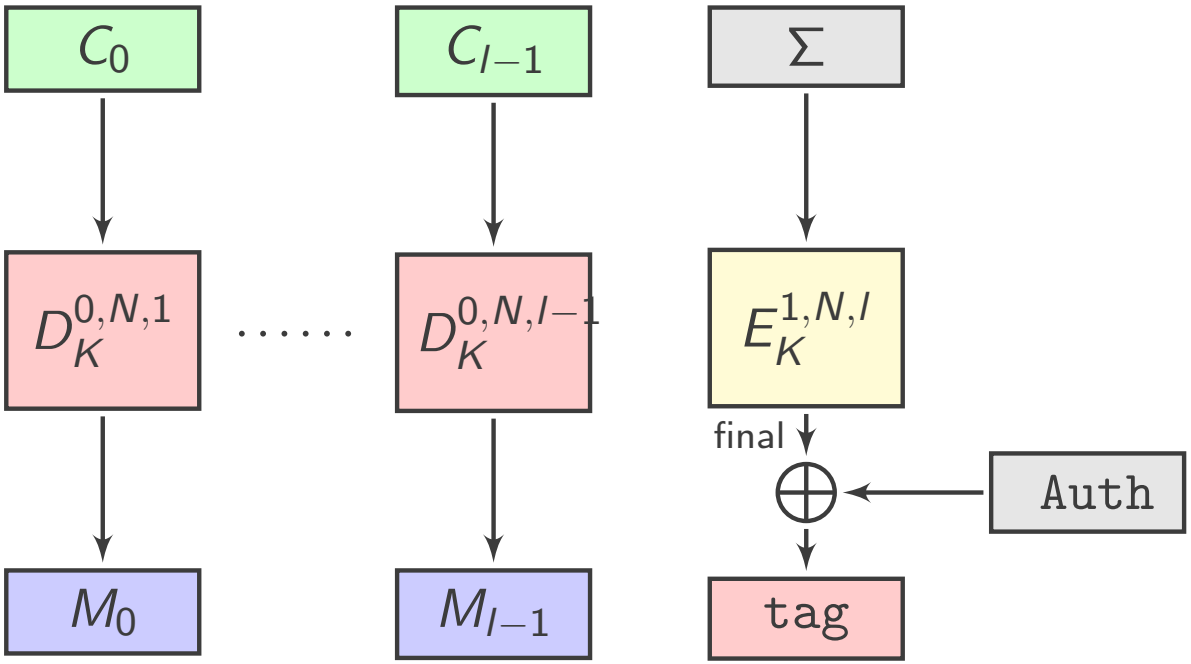
Message Encryption : Without Padding



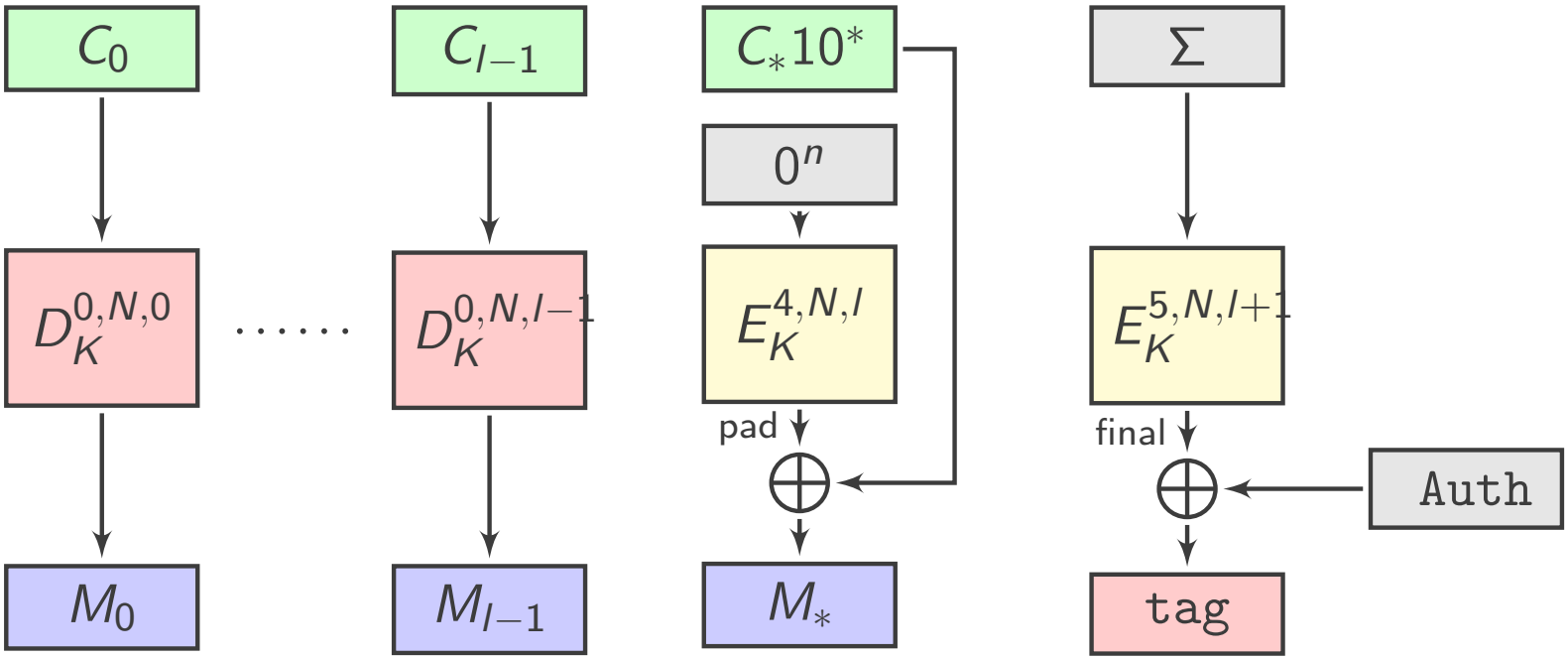
Message Encryption : With Padding



Message Decryption : Without Padding



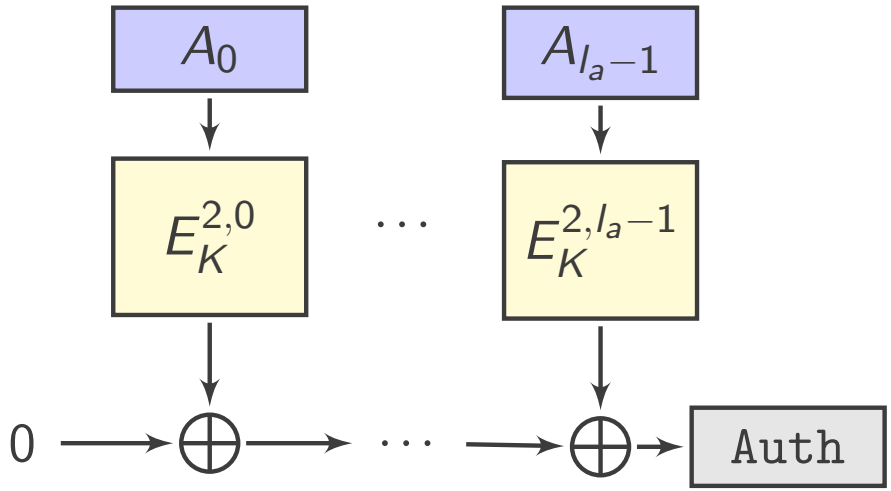
Message Decryption : With Padding



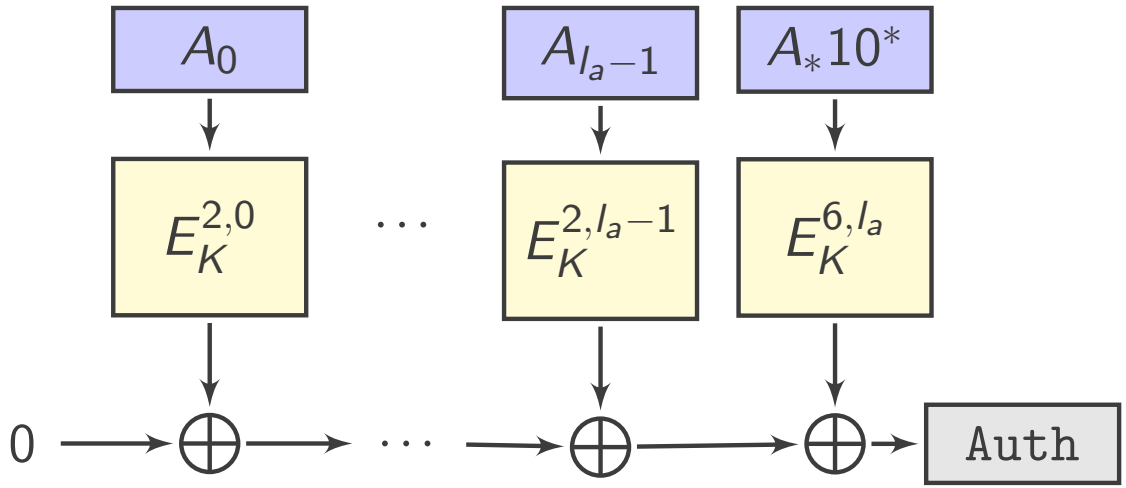
Part 2

Lilliput-AE

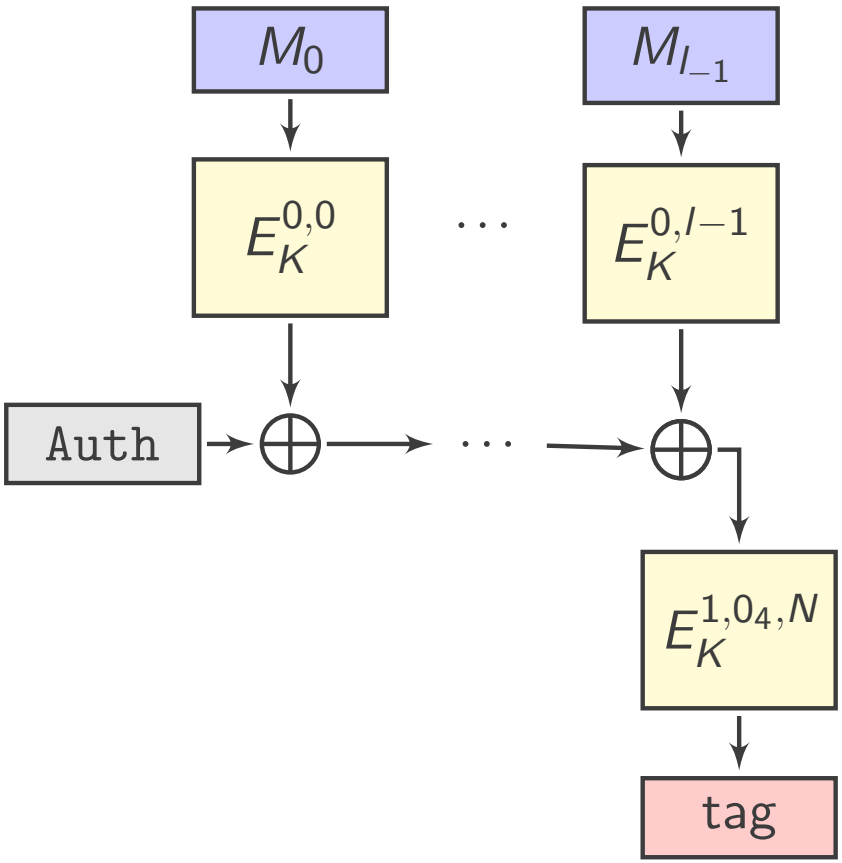
Associated Data : Without Padding



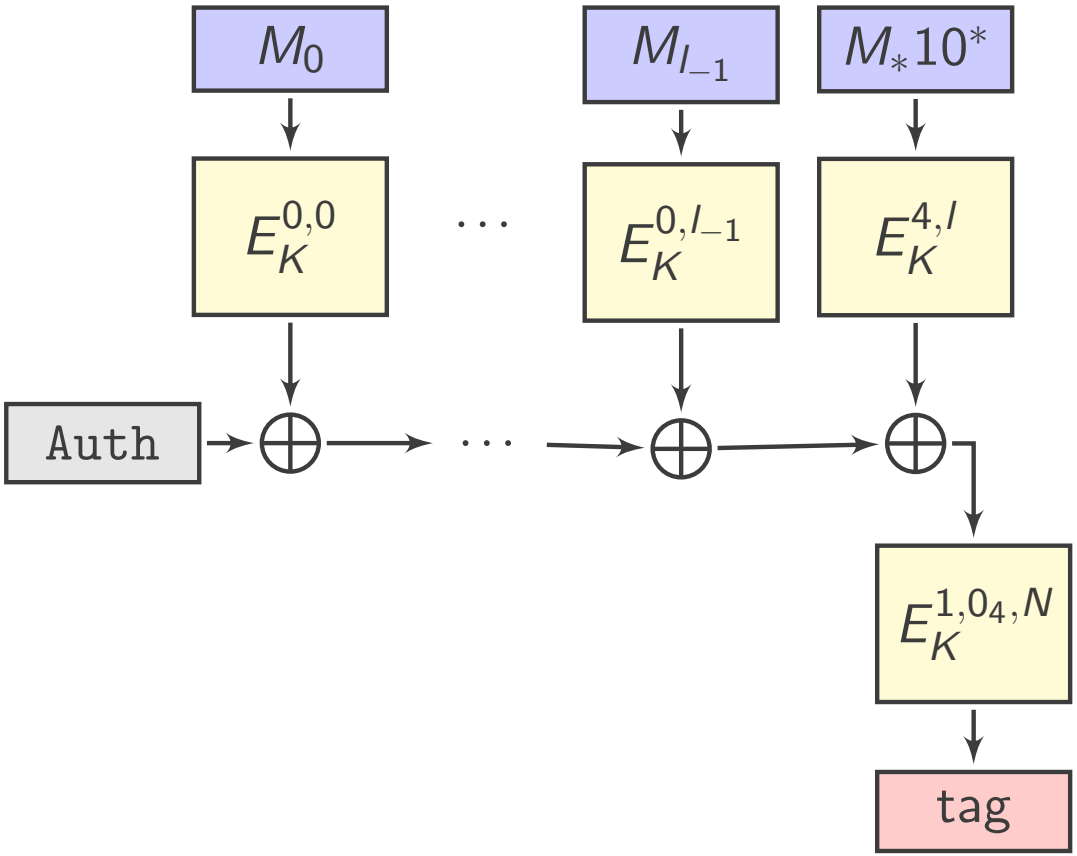
Associated Data : With Padding



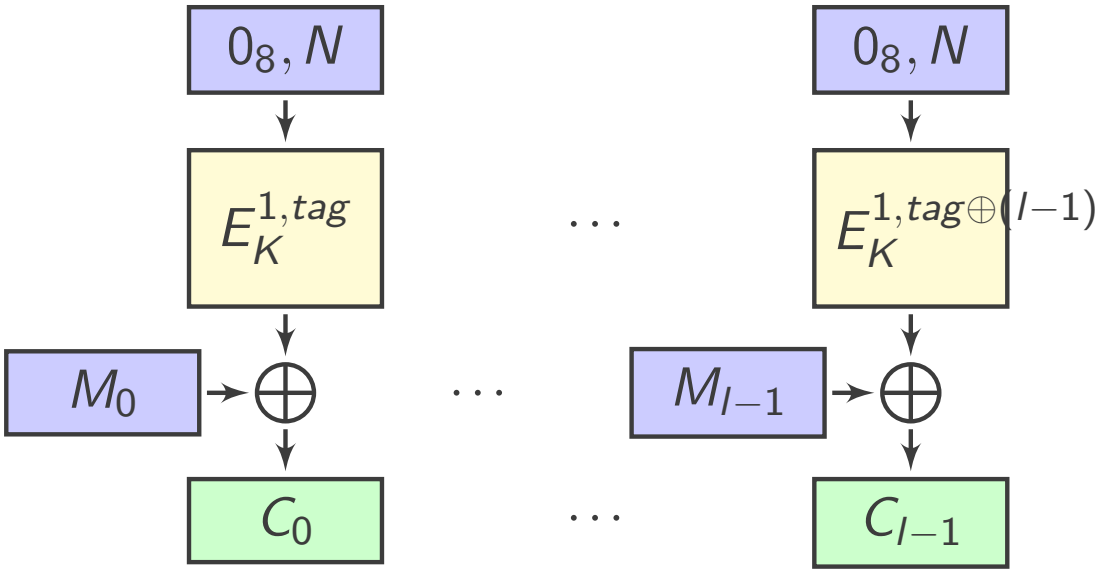
Tag Generation : Without Padding



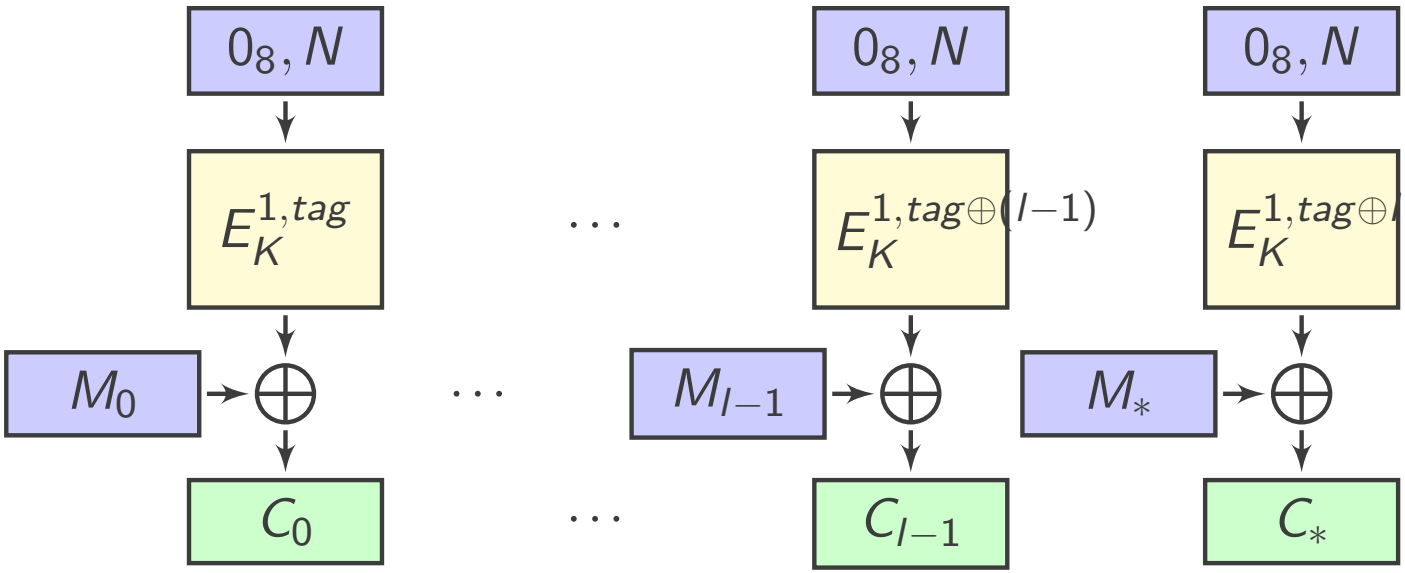
Tag Generation : With Padding



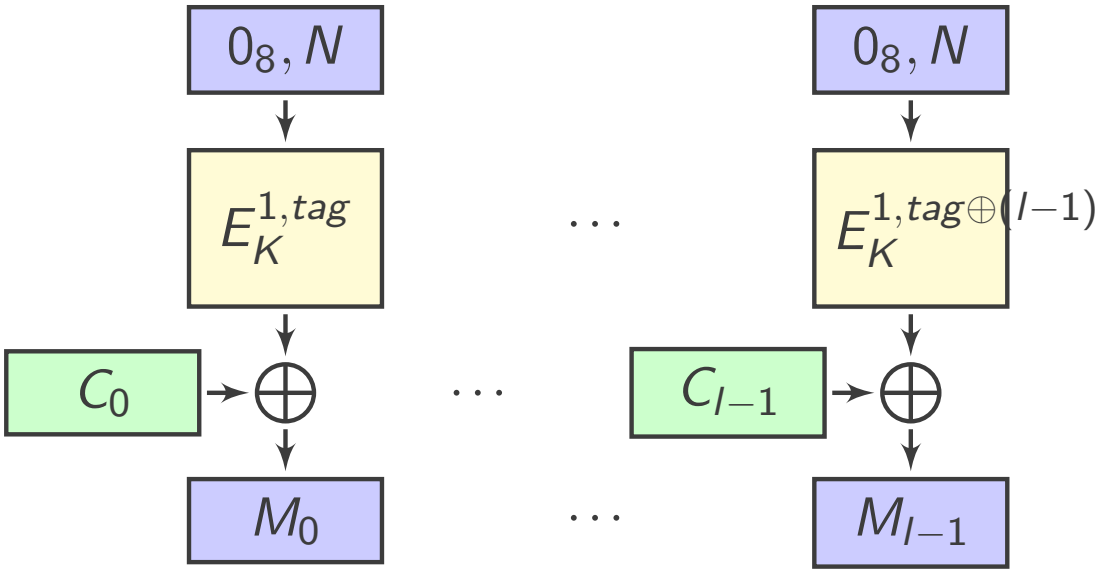
Message Encryption : Without Padding



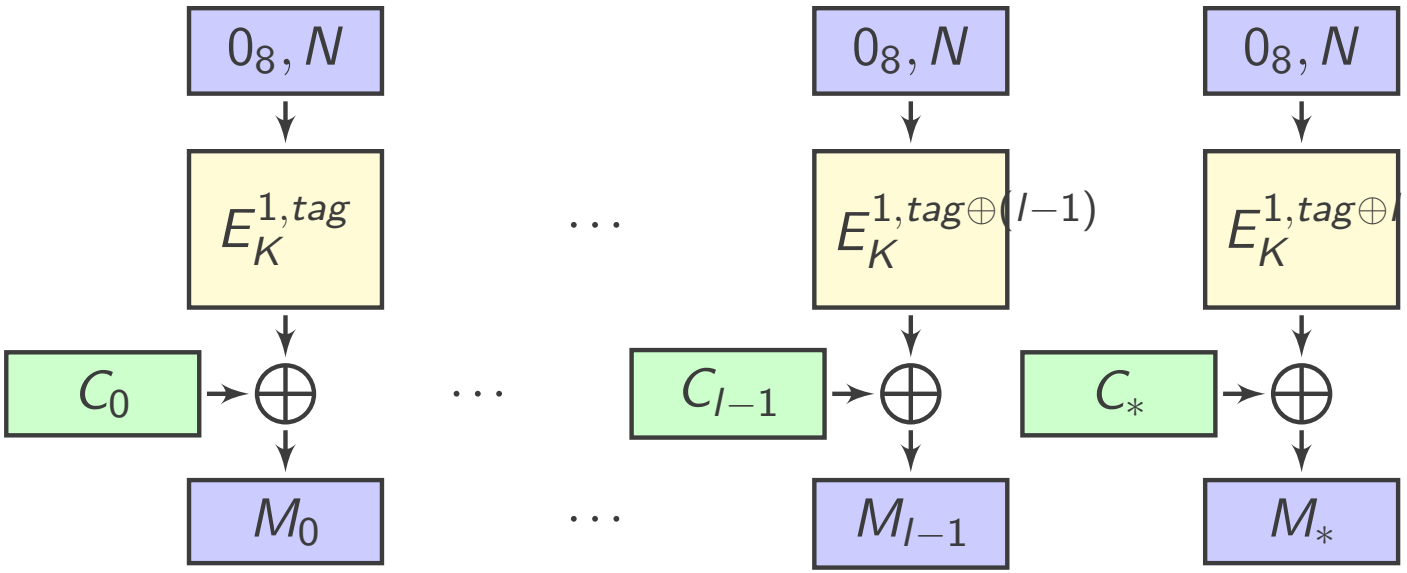
Message Encryption : With Padding



Message Decryption : Without Padding



Message Decryption : With Padding



Thanks for your attention!

Questions ?

References

 Intro to Cryptography

 Joy of Cryptography

 Salad of Block Ciphers