Parallelizable and Authenticated Online Ciphers[1]

Atul Luykx

COSIC
KU Leuven and iMinds

December 3, 2013

[1] Joint work with E. Andreeva, A. Bogdanov, B. Mennink, E. Tischhauser, and K. Yasuda.

Motivation: Authenticated Encryption

Authenticated Encryption (AE) = Privacy + Authenticity

1. Applications: SSH, IPsec, TLS, IEEE 802.11
2. CAESAR competition

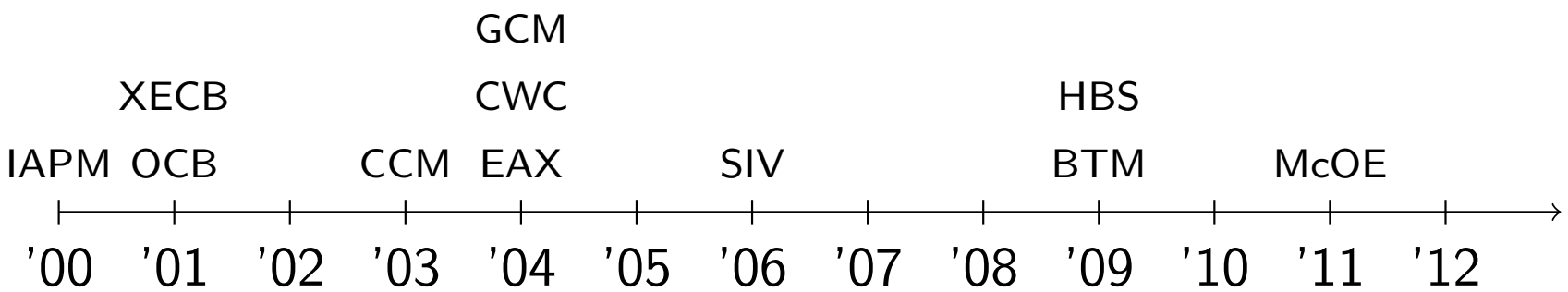


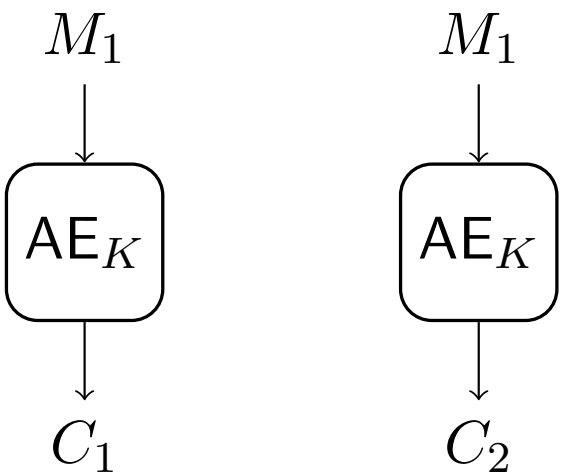
Figure : AE schemes

Motivation: Nonce Misuse

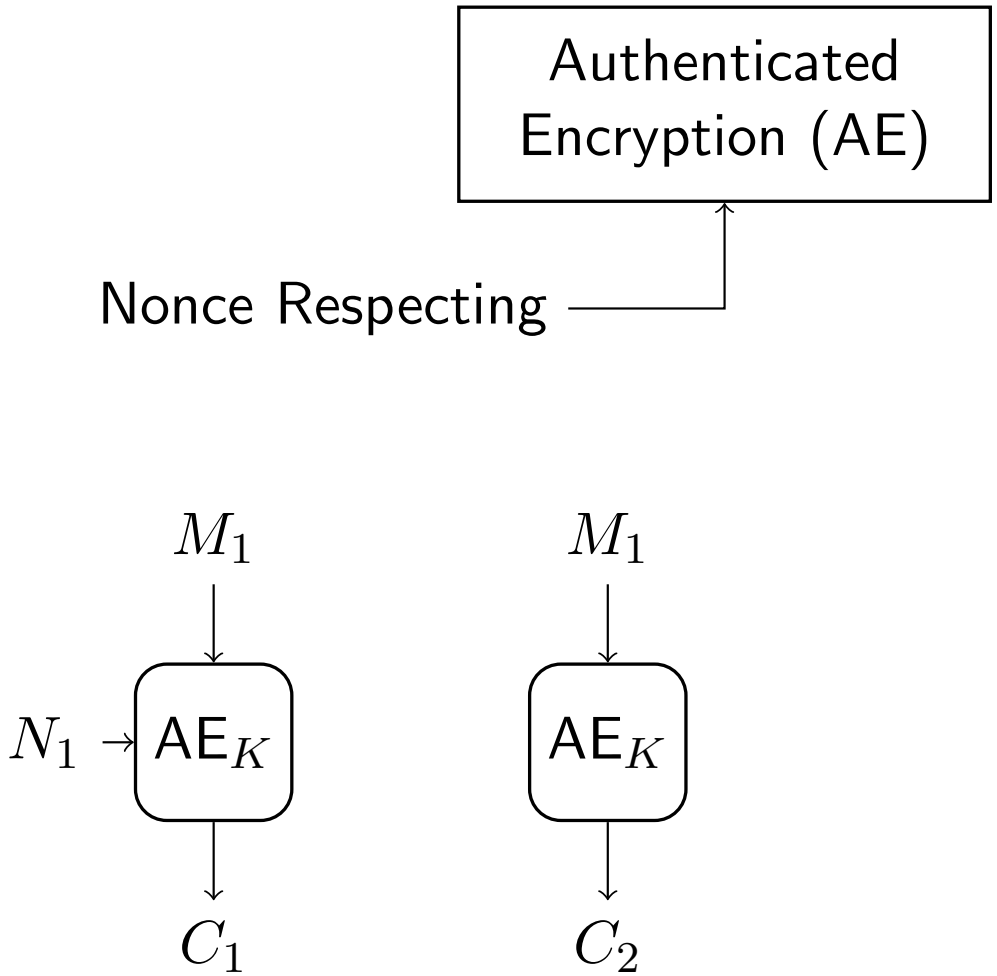
Authenticated Encryption (AE)

Motivation: Nonce Misuse

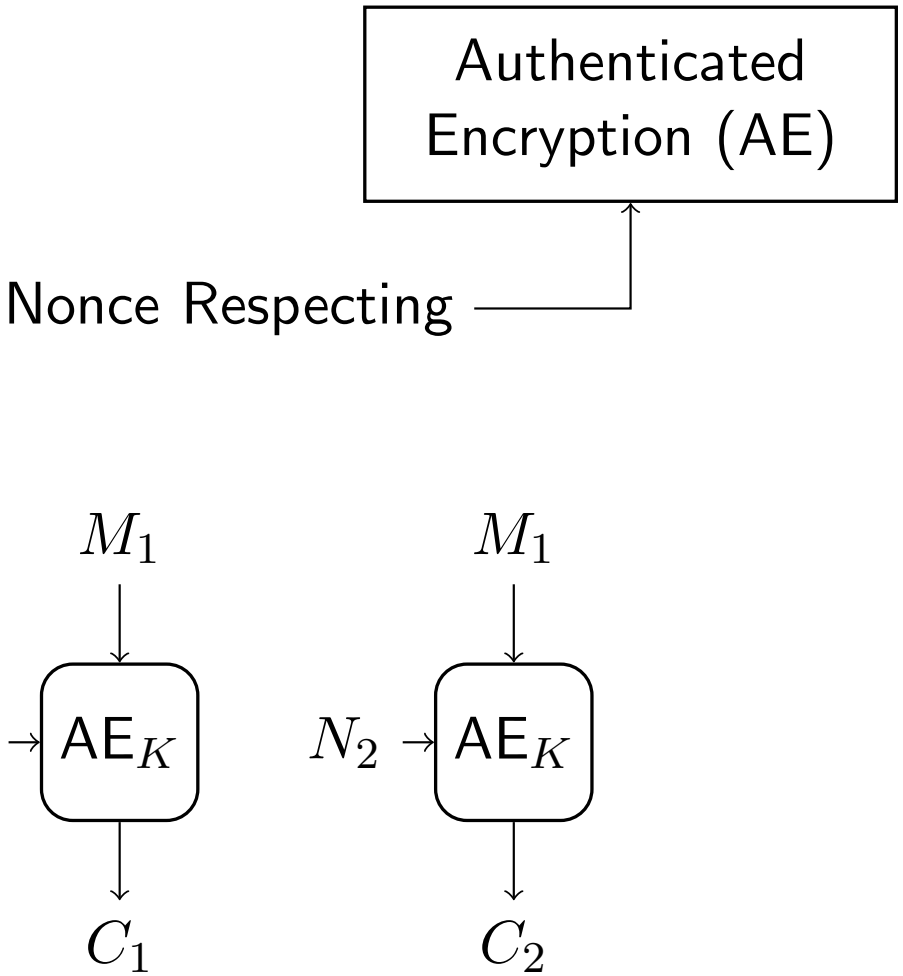
Authenticated Encryption (AE)



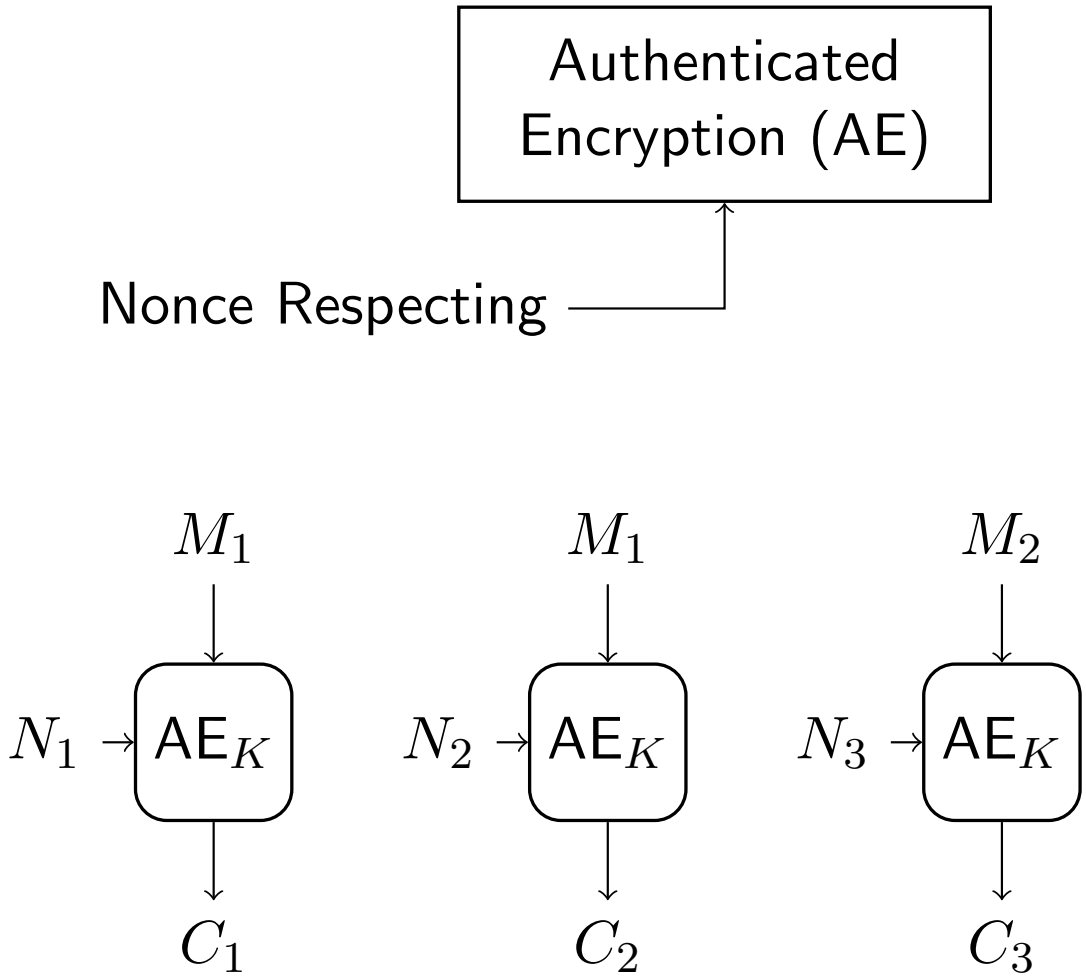
Motivation: Nonce Misuse



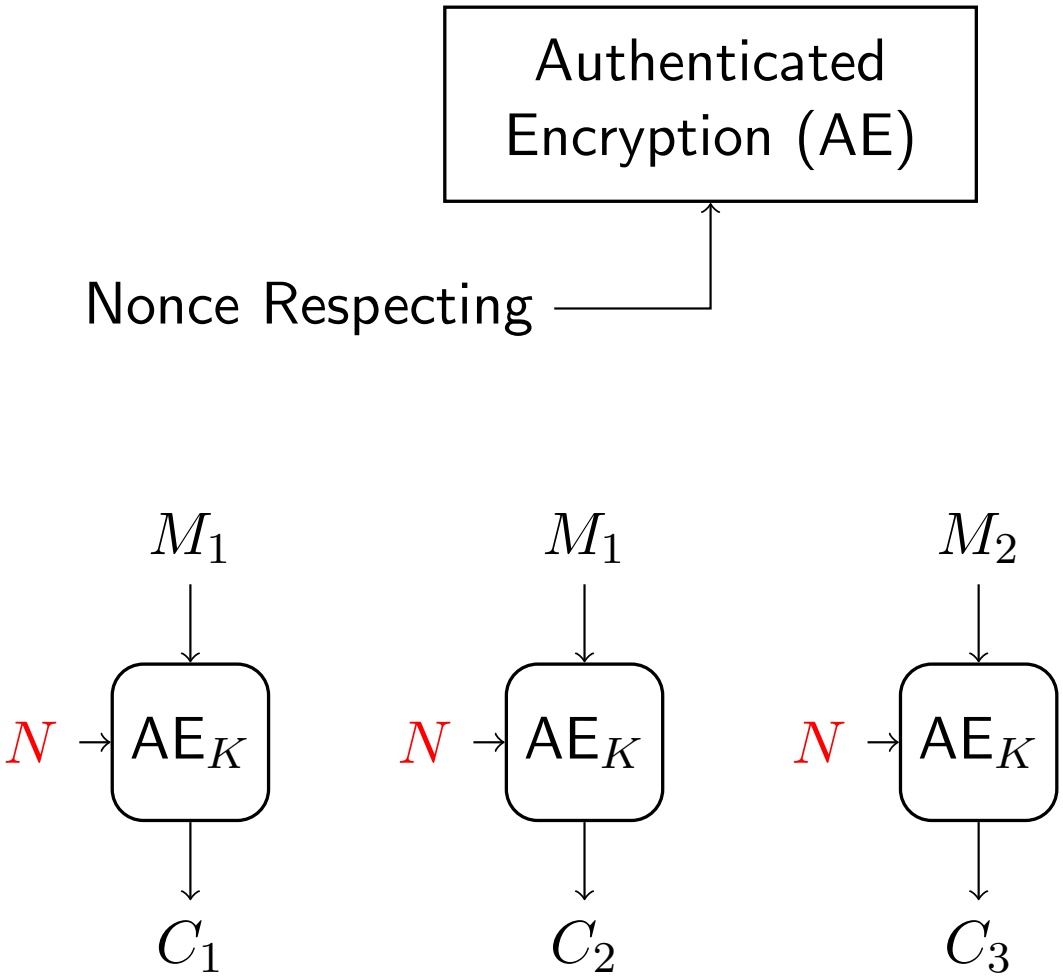
Motivation: Nonce Misuse



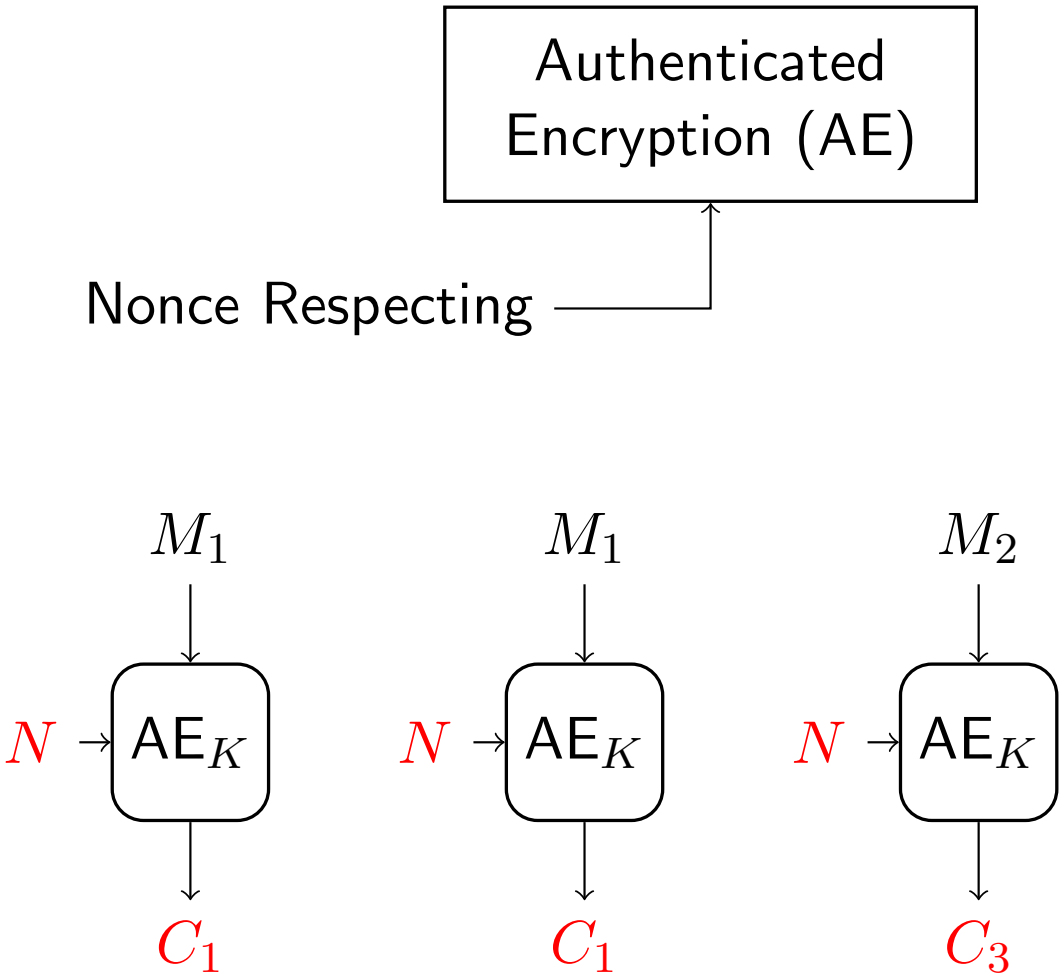
Motivation: Nonce Misuse



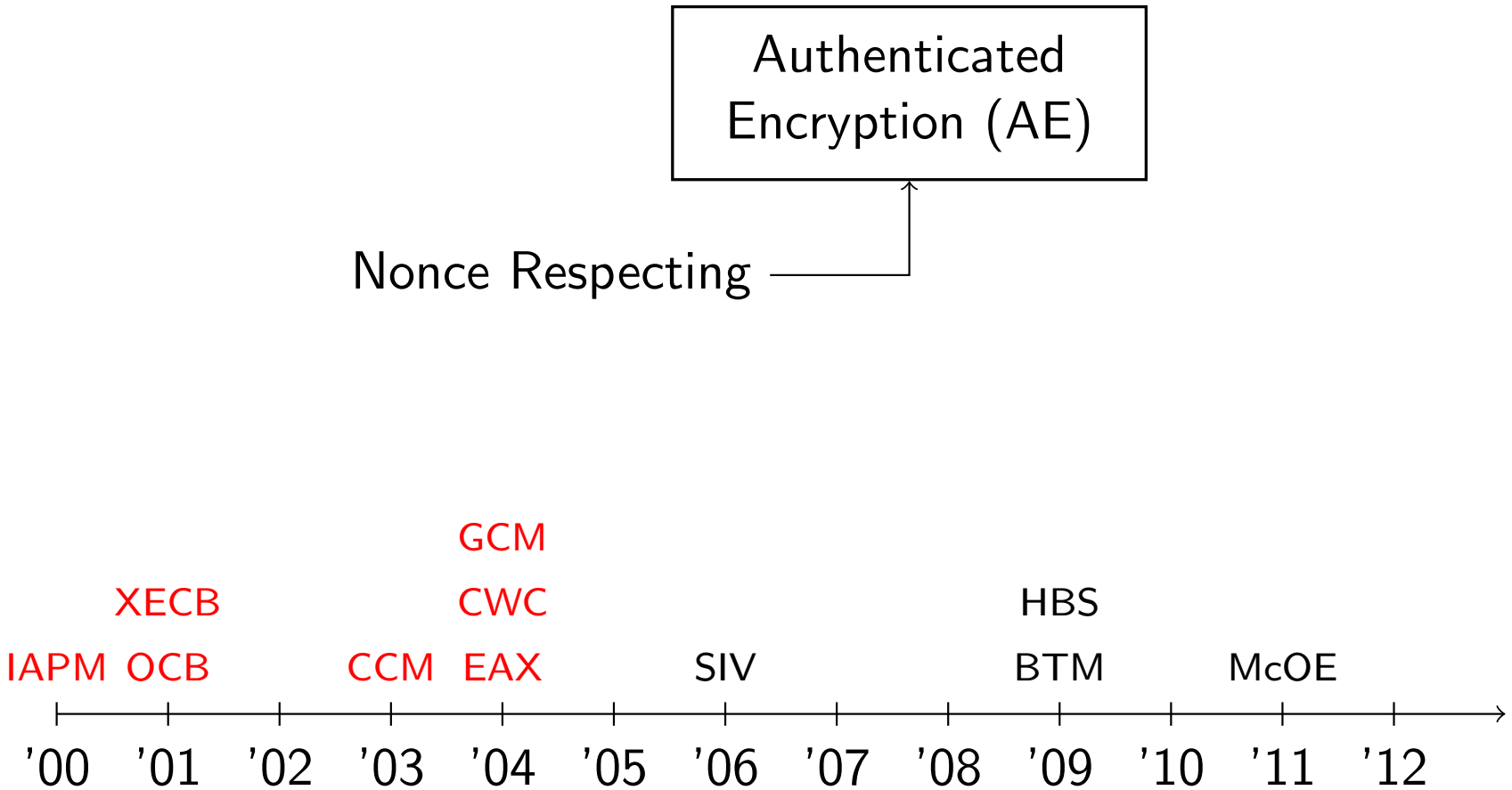
Motivation: Nonce Misuse



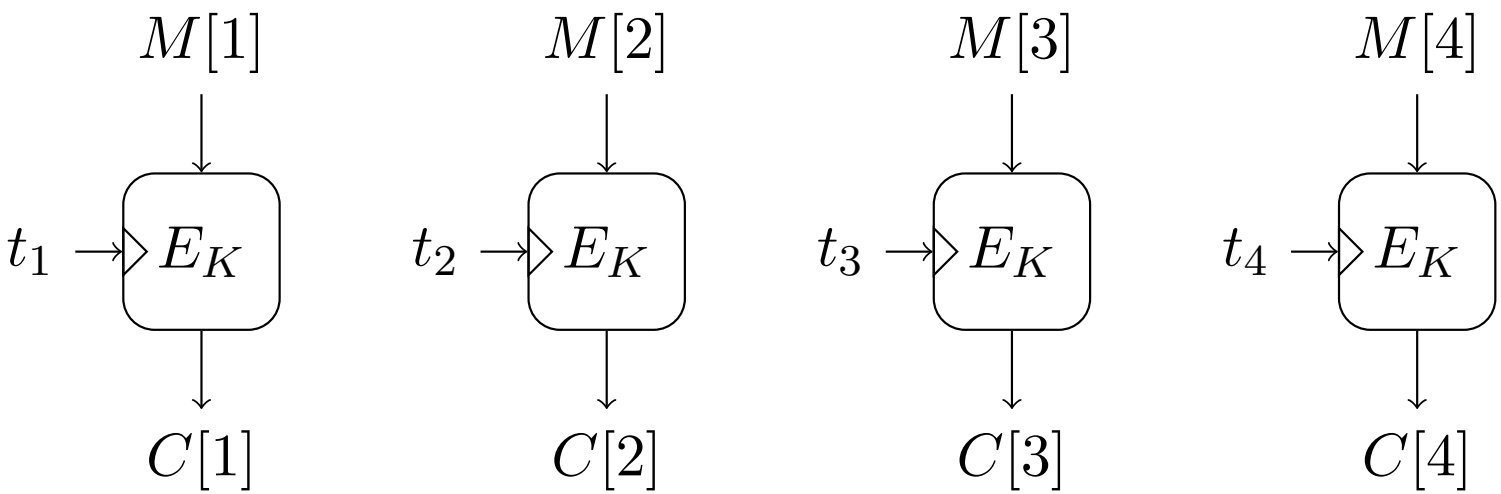
Motivation: Nonce Misuse



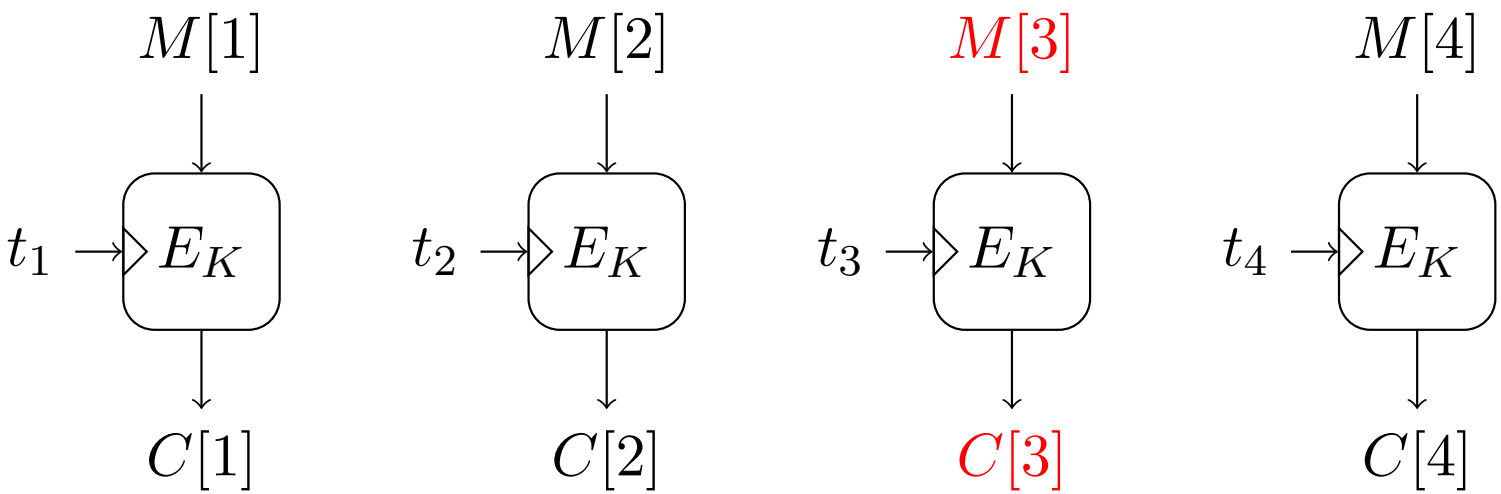
Motivation: Nonce Misuse



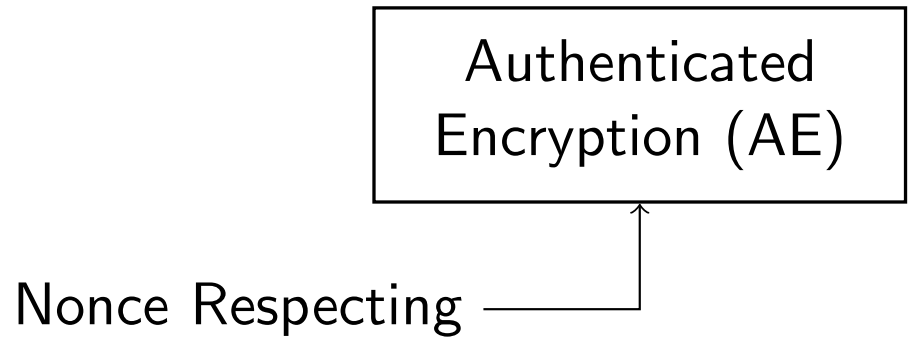
Motivation: OCB With Nonce Repeated

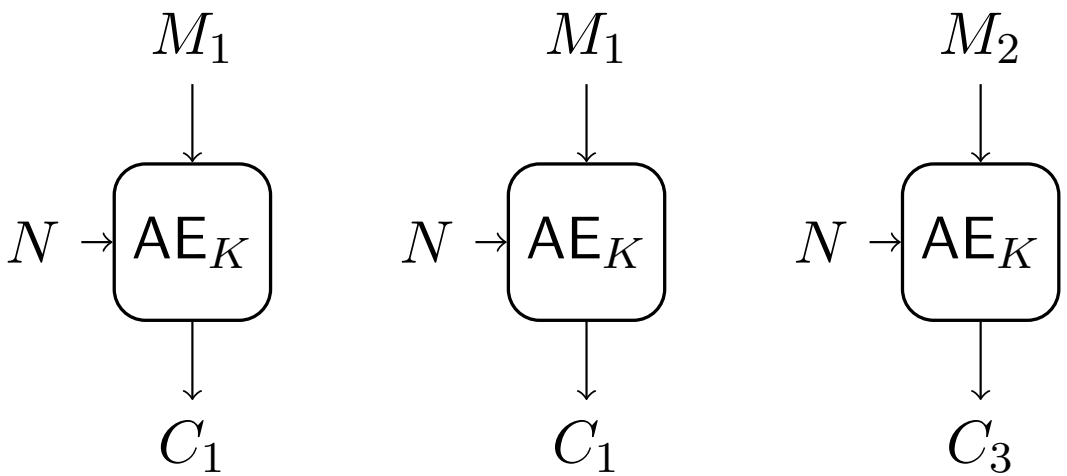


Motivation: OCB With Nonce Repeated

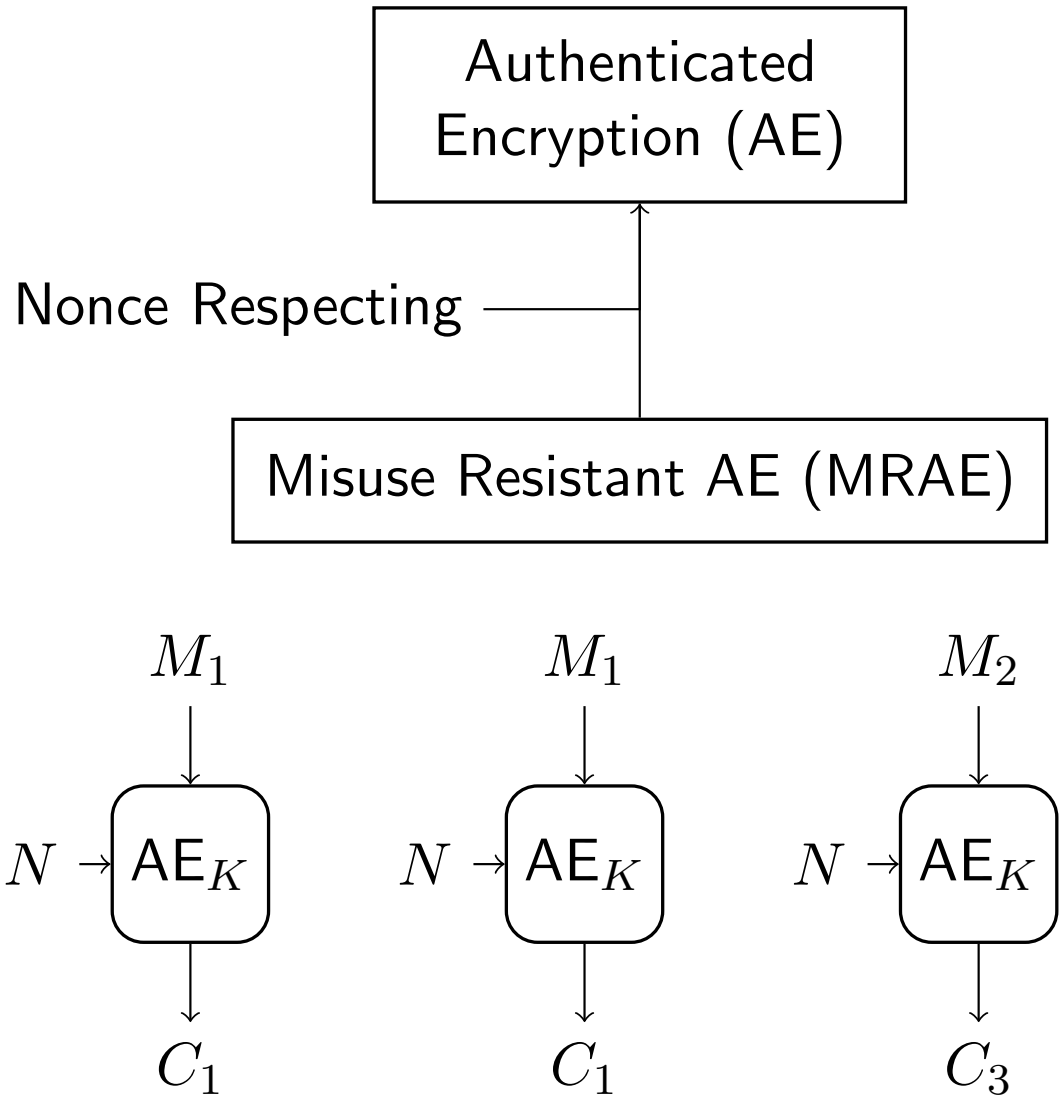


Motivation: Nonce Misuse

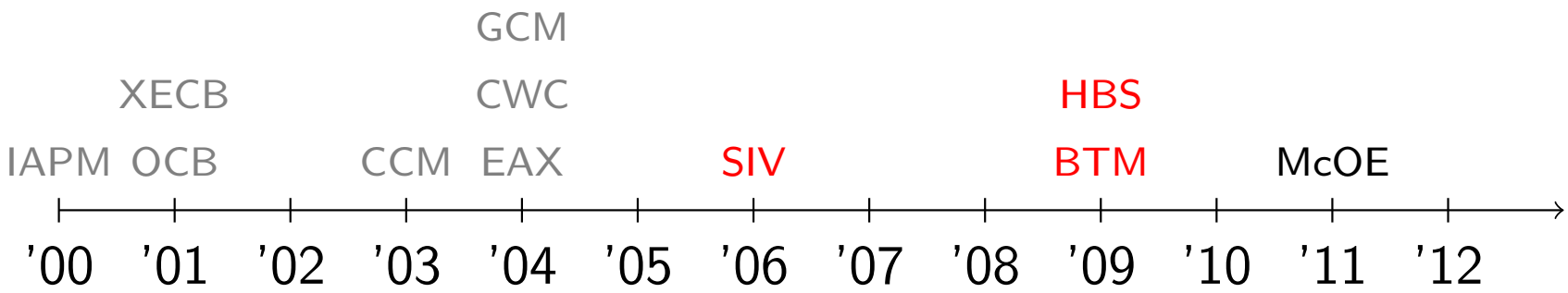




Motivation: Nonce Misuse



Motivation: Efficiency

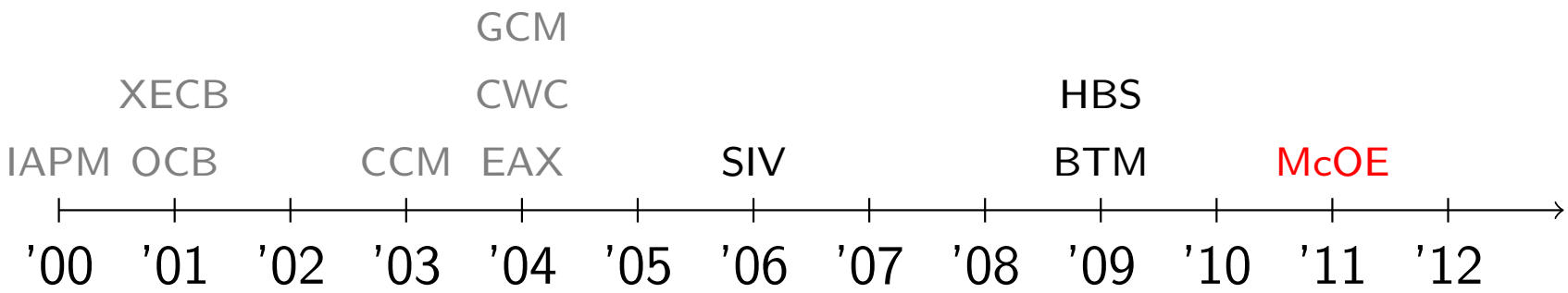


SIV, BTM, HBS:

1. High latency (receive full message before first output)
2. Storage issues (large internal state)

McOE: inherently sequential

Motivation: Efficiency



SIV, BTM, HBS:

1. High latency (receive full message before first output)
2. Storage issues (large internal state)

McOE: inherently sequential

Motivation: Our Goal

Design an AE scheme that is

- Online
- Parallelizable
- Misuse Resistant

Motivation: Our Goal

Design an AE scheme that is

- Online
- Parallelizable
- Misuse Resistant

Our method:

1. Create the first parallelizable online cipher: COPE
2. Add authenticity efficiently: COPA

Motivation: Our Goal

Design an AE scheme that is

- Online
- Parallelizable
- Misuse Resistant

Our method:

1. Create the first parallelizable online cipher: COPE
2. Add authenticity efficiently: COPA

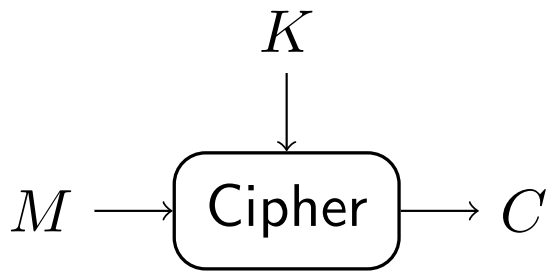
Our desired AE scheme: COPA

Background: Cipher Definition

$$M \in \{0,1\}^*$$

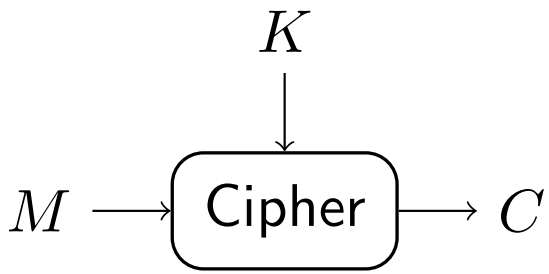
Background: Cipher Definition

$M \in \{0,1\}^*$



Background: Cipher Definition

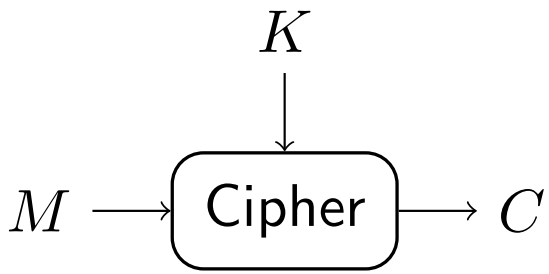
$M \in \{0,1\}^*$



$|M| = |C|$

Background: Cipher Definition

$M \in \{0,1\}^*$



$|M| = |C|$

Cipher	vs	Encryption Scheme
Length-Preserving		Not Necessarily
Deterministic		Randomized, Stateful (nonce)
Indistinguishable from permutations		Indistinguishable from random bits

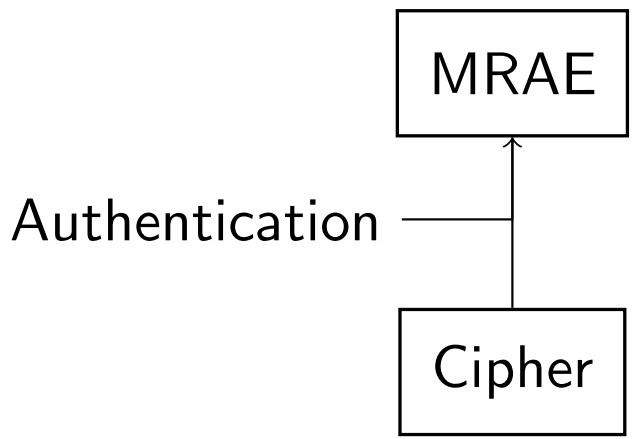
Background: Achieving AE via Ciphers

Background: Achieving AE via Ciphers

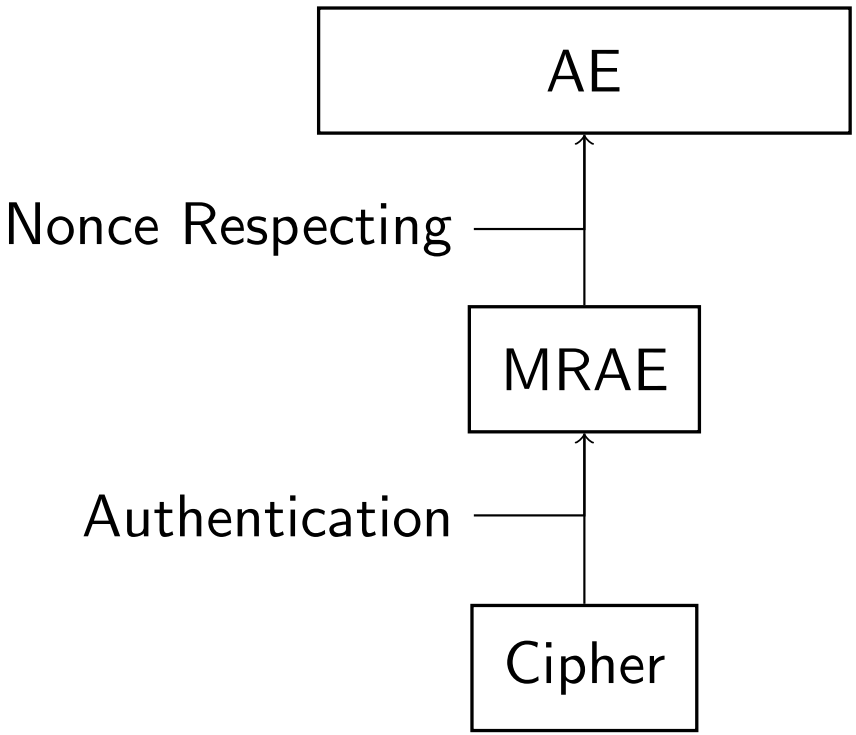
Authentication

Cipher

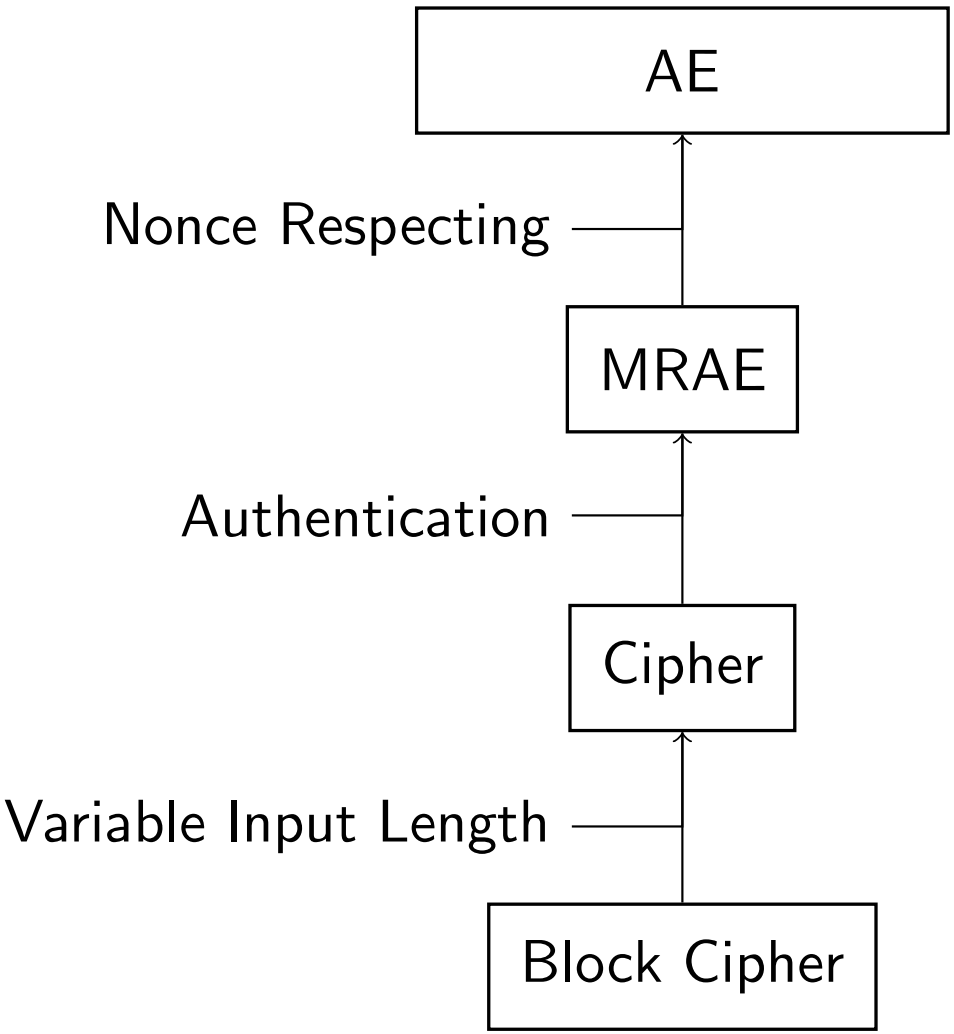
Background: Achieving AE via Ciphers



Background: Achieving AE via Ciphers



Background: Achieving AE via Ciphers

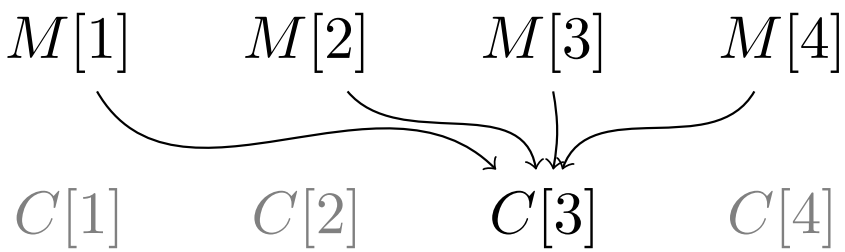


Background: *Online* Cipher Definition

1. Same interface as a cipher
2. More efficient and "on-the-fly" computing
3. Different (weaker) security requirement: up to prefix

Background: *Online* Cipher Definition

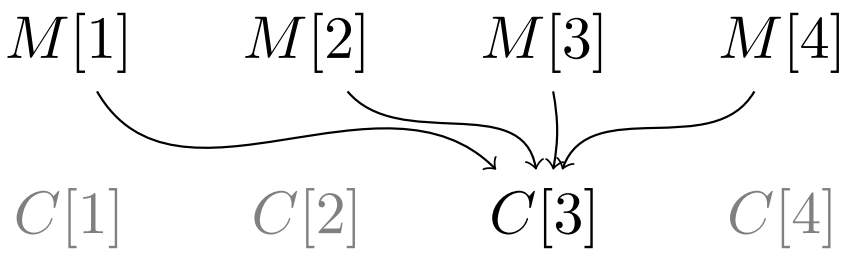
1. Same interface as a cipher
2. More efficient and "on-the-fly" computing
3. Different (weaker) security requirement: up to prefix



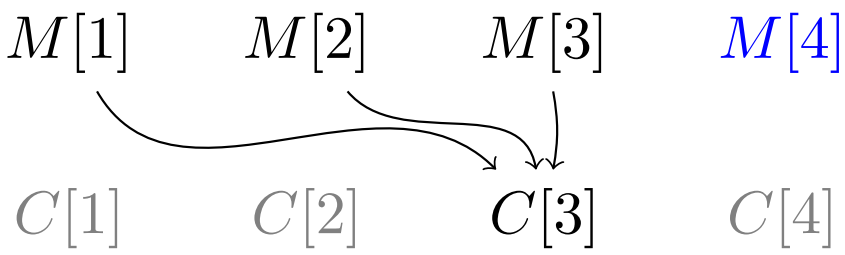
Dependency in a cipher.

Background: *Online* Cipher Definition

1. Same interface as a cipher
2. More efficient and "on-the-fly" computing
3. Different (weaker) security requirement: up to prefix

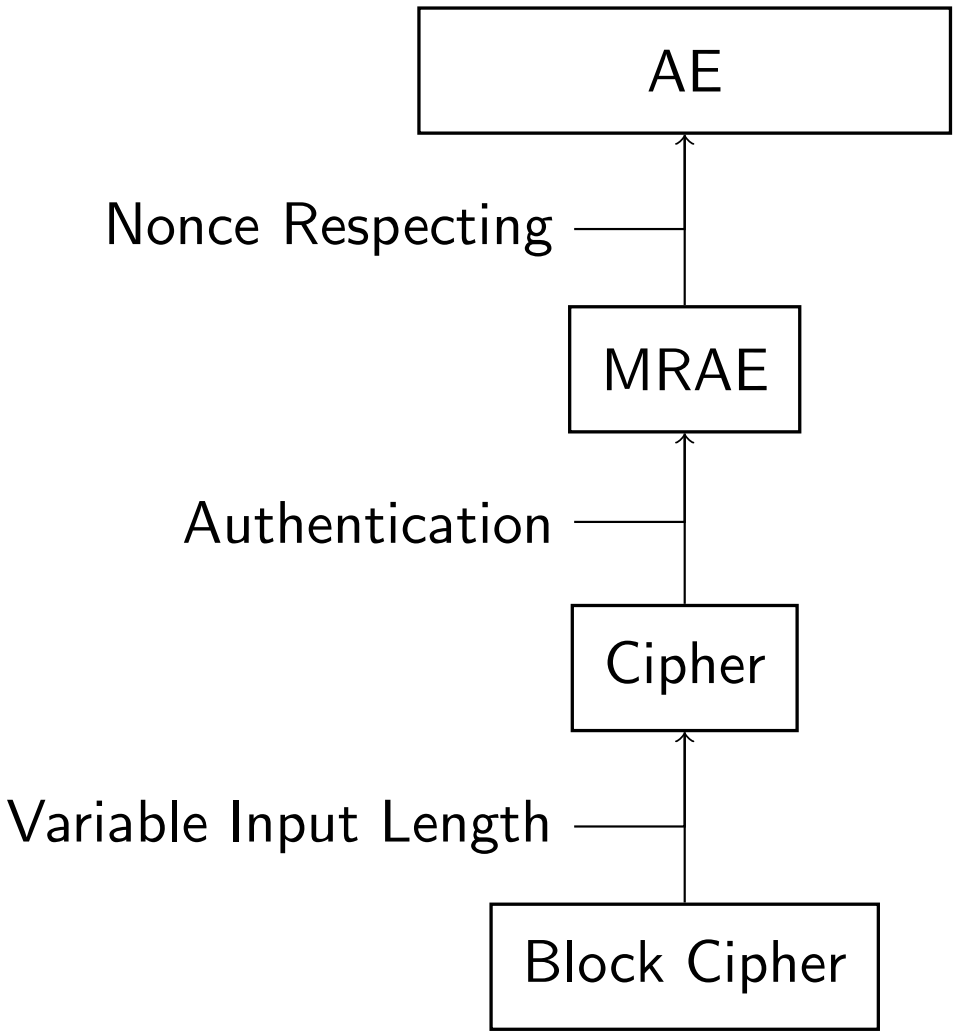


Dependency in a cipher.

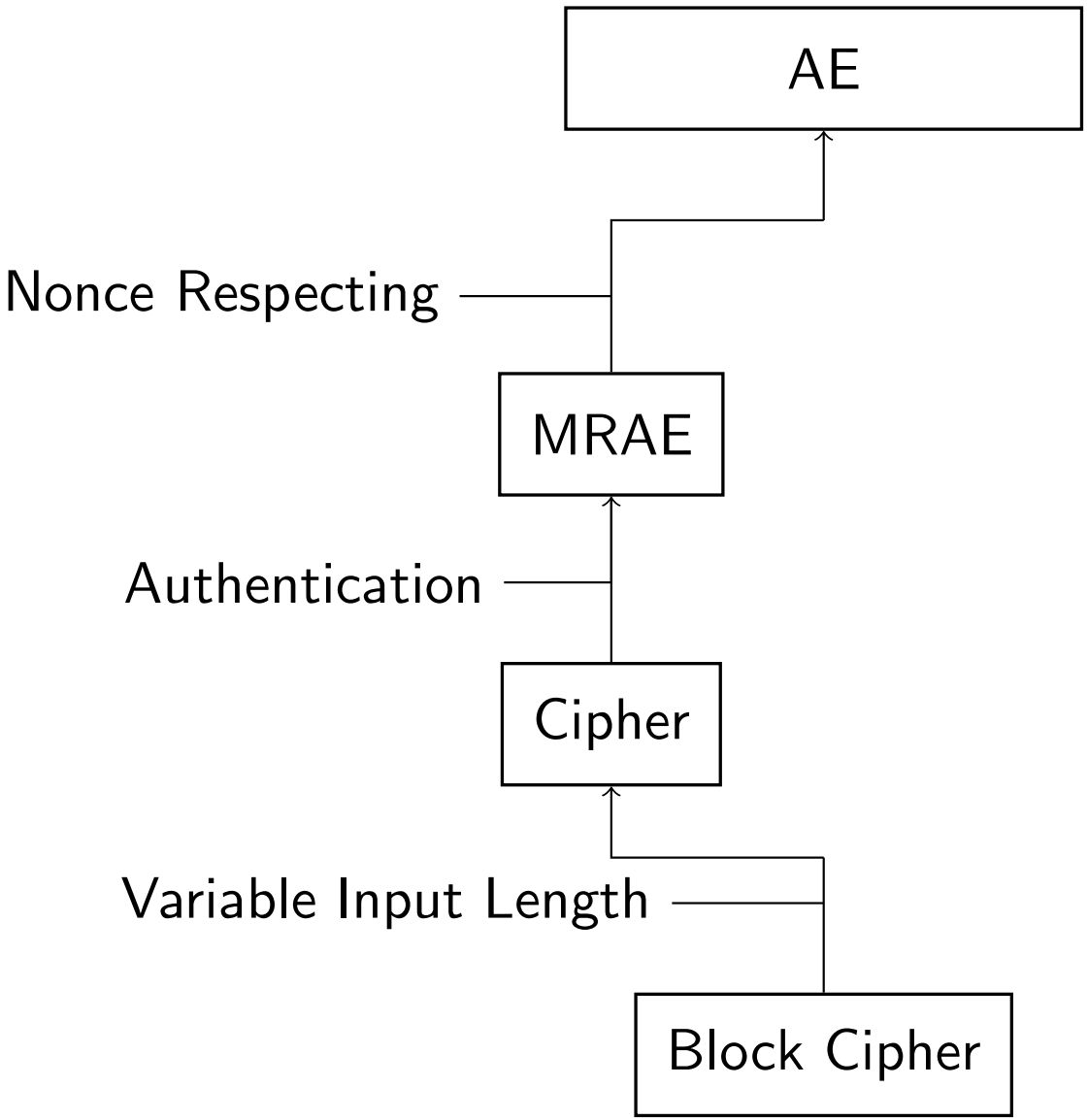


Dependency in an online cipher.

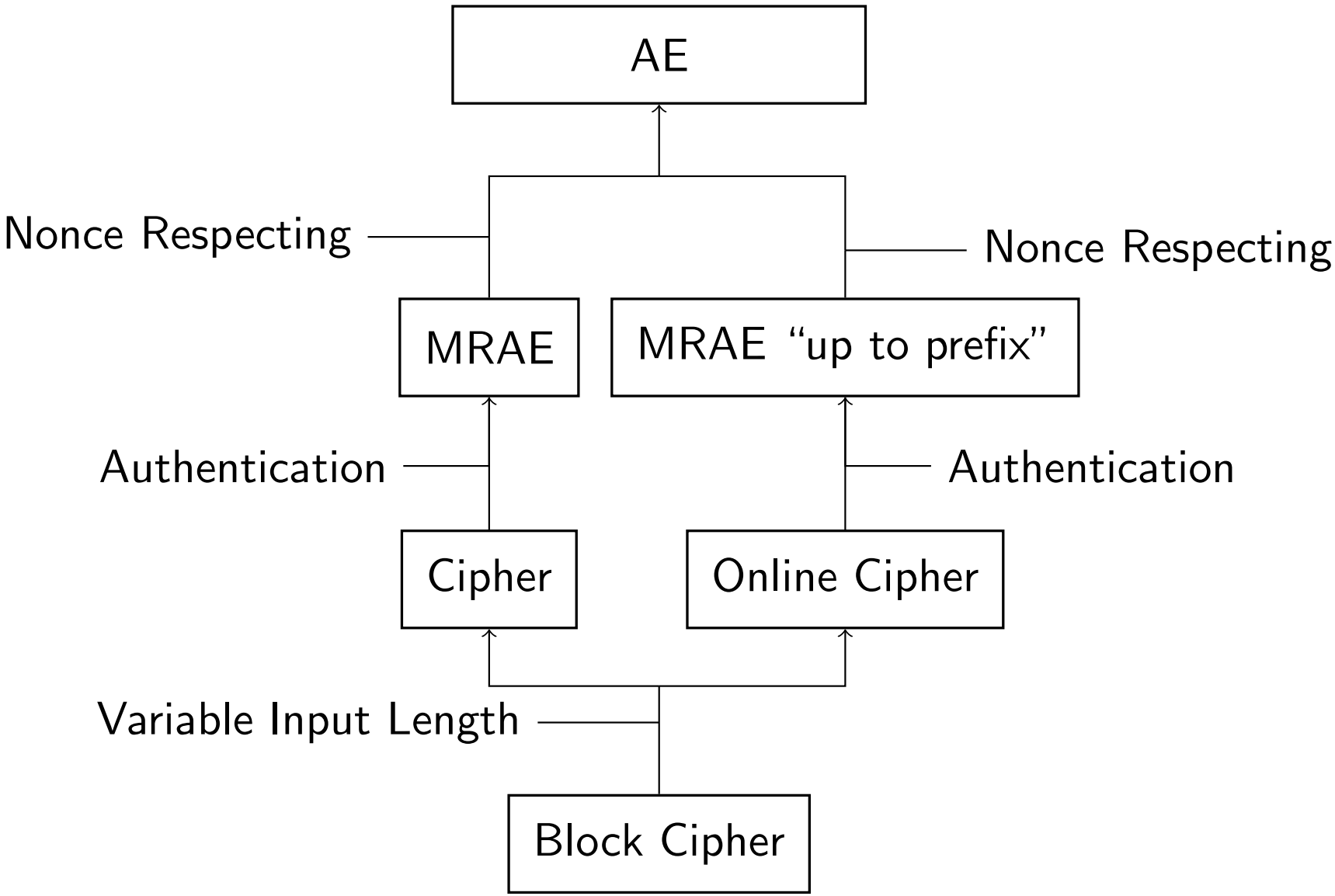
Background: Achieving AE Via Online Ciphers



Background: Achieving AE Via Online Ciphers



Background: Achieving AE Via Online Ciphers



Existing Work

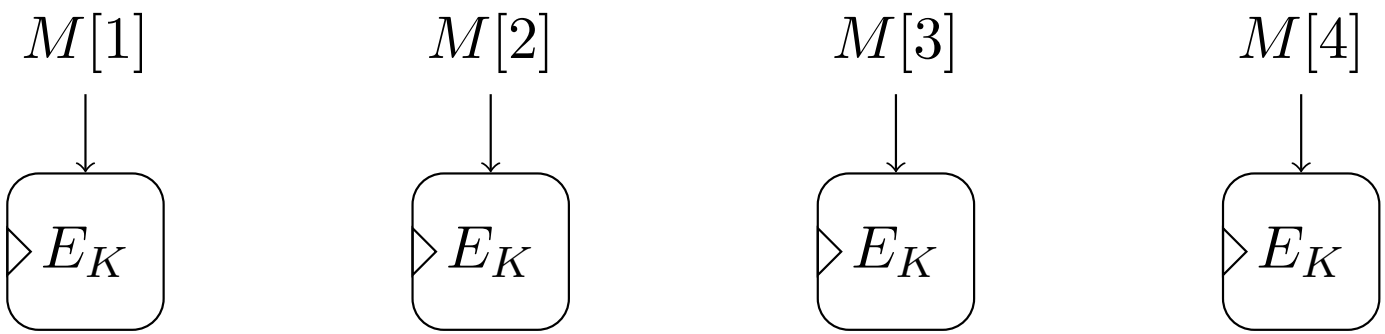
1. HCBC1, HCBC2 (BBKN, Crypto '01)
2. MHCBC, MCBC (Nandi, Indocrypt '08)
3. Rewritten with *tweakable block ciphers*: TC1, TC2, TC3 (Rogaway and Zhang, CT-RSA '11)
4. McOE family (FFL, FSE '12): TC3 with authentication

All schemes are inherently sequential.

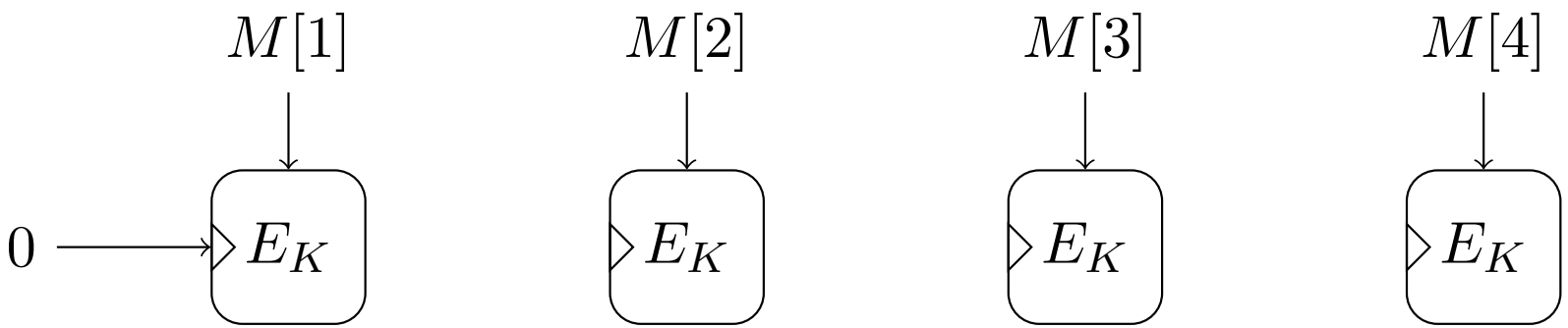
Existing Work: TC3

$M[1]$ $M[2]$ $M[3]$ $M[4]$

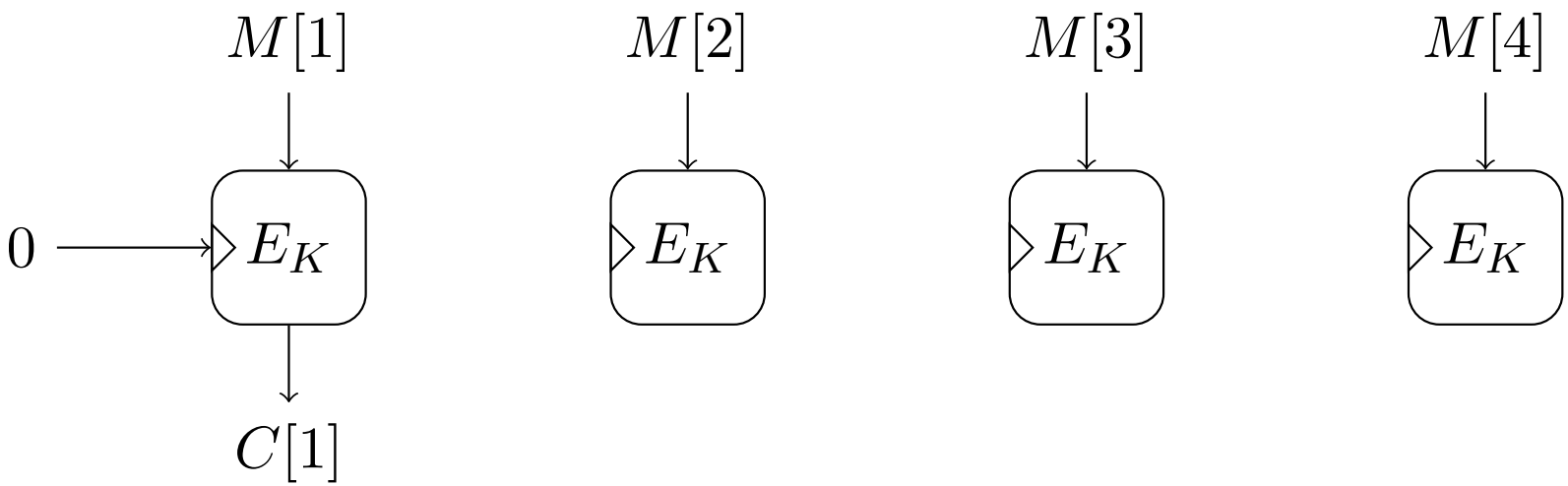
Existing Work: TC3



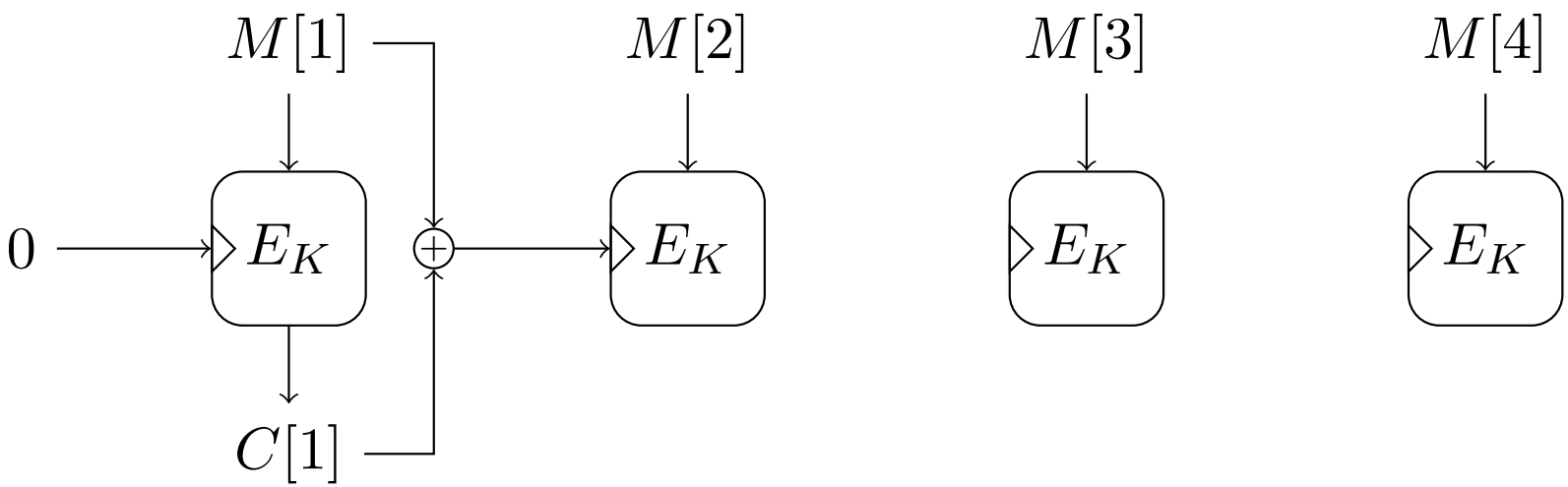
Existing Work: TC3



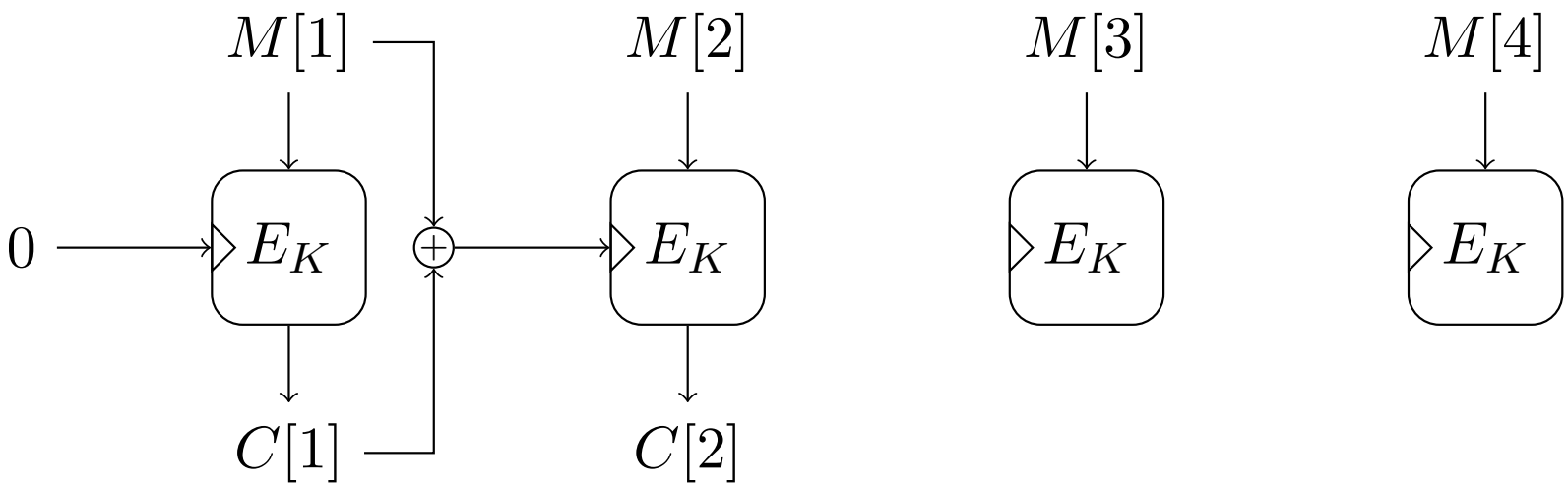
Existing Work: TC3



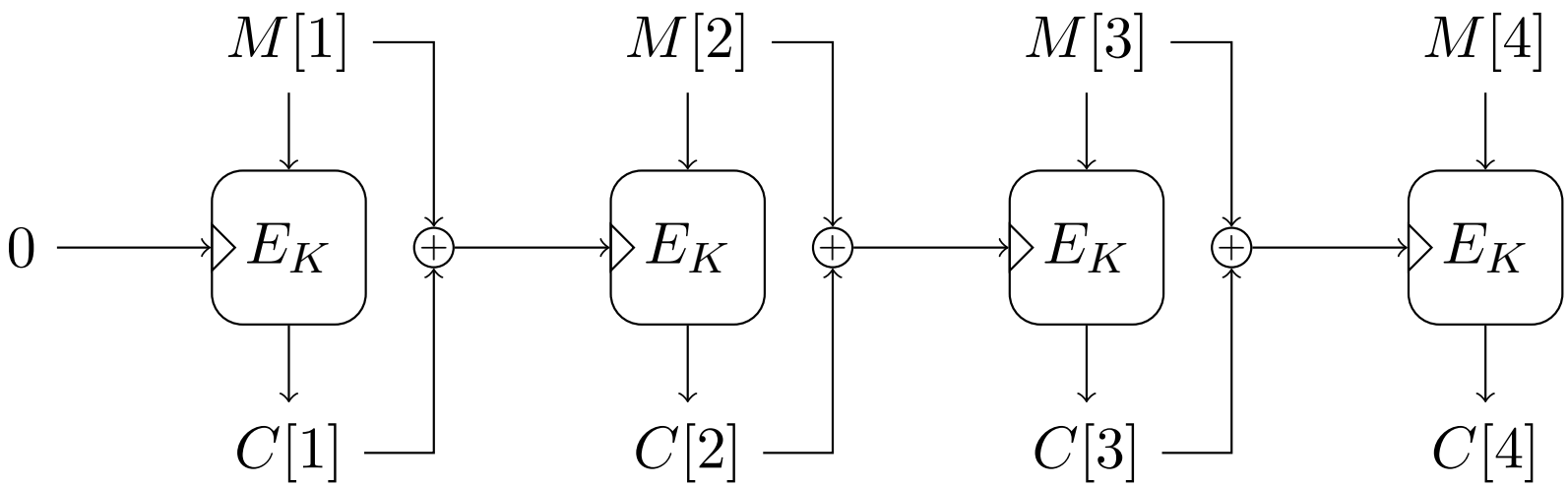
Existing Work: TC3



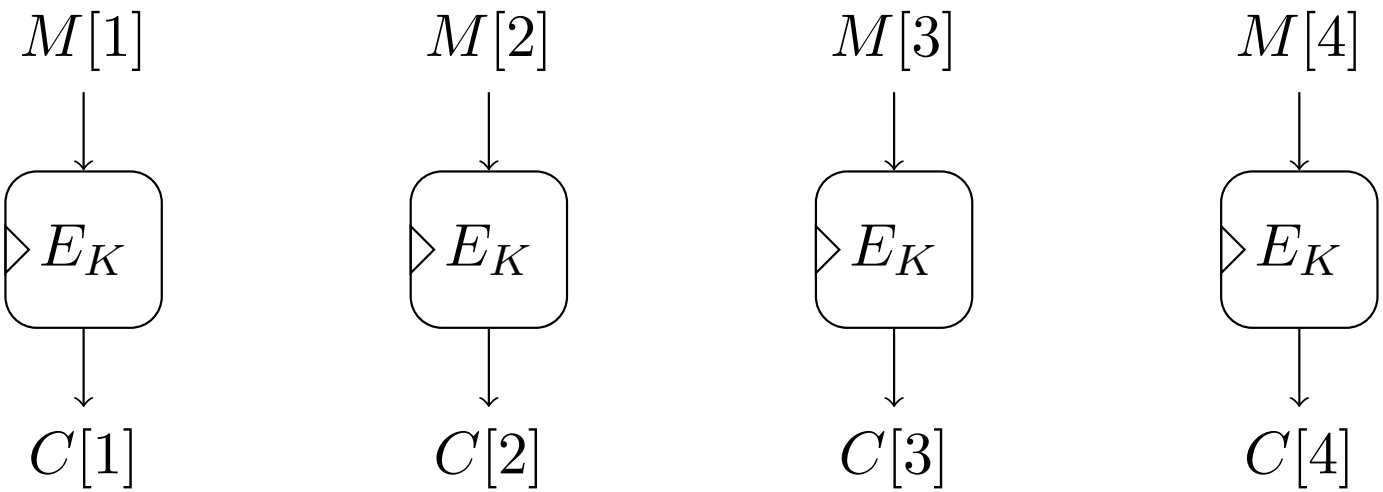
Existing Work: TC3



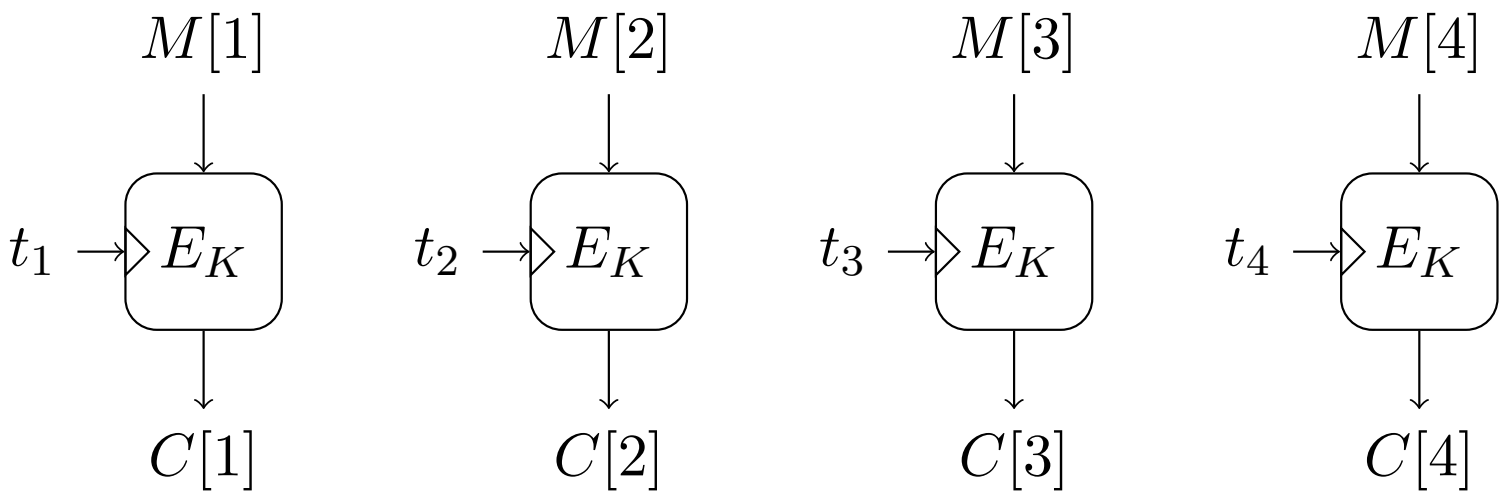
Existing Work: TC3



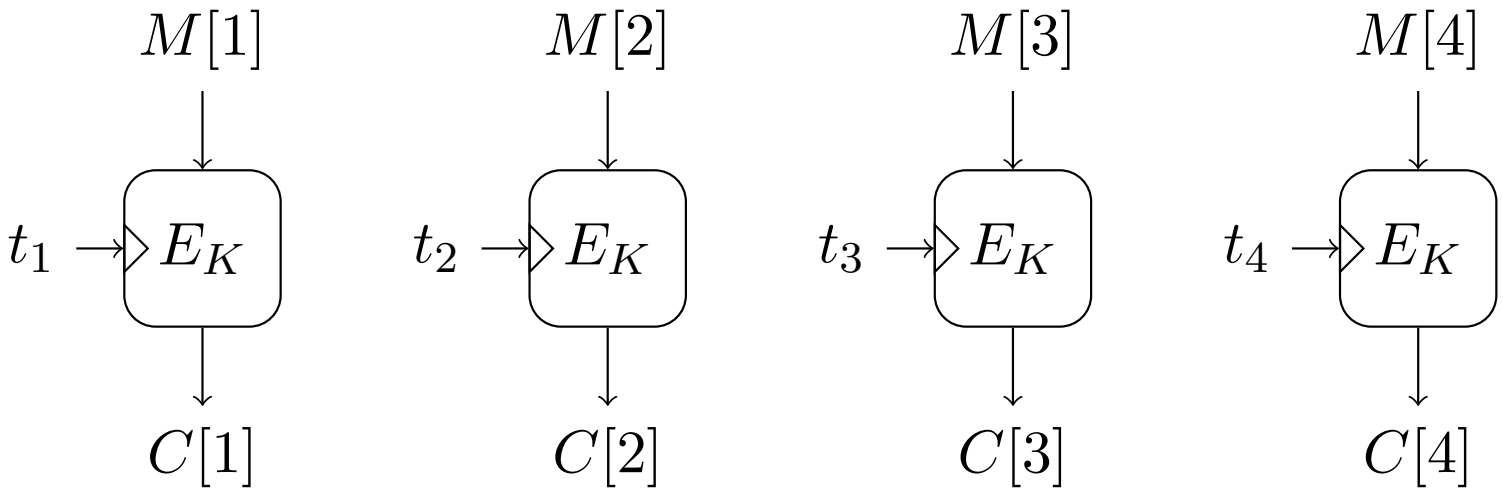
Achieving Parallelizability



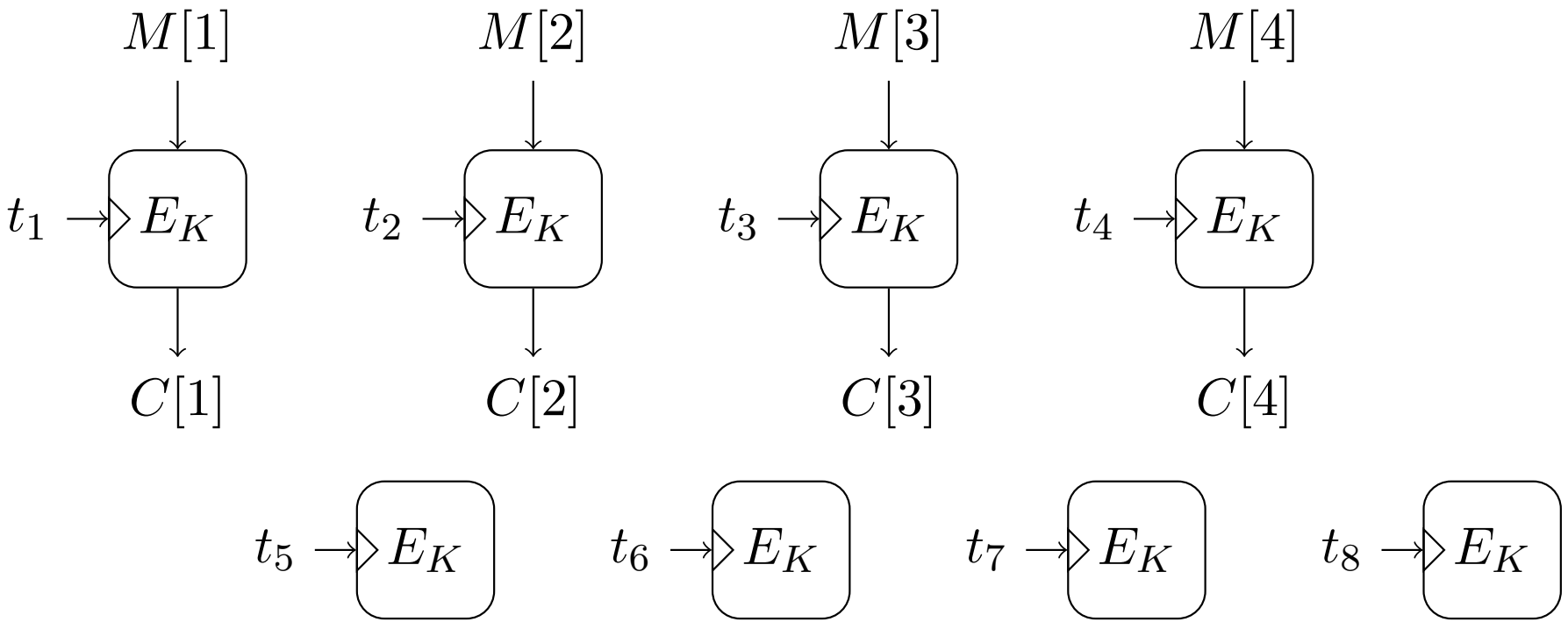
Achieving Parallelizability



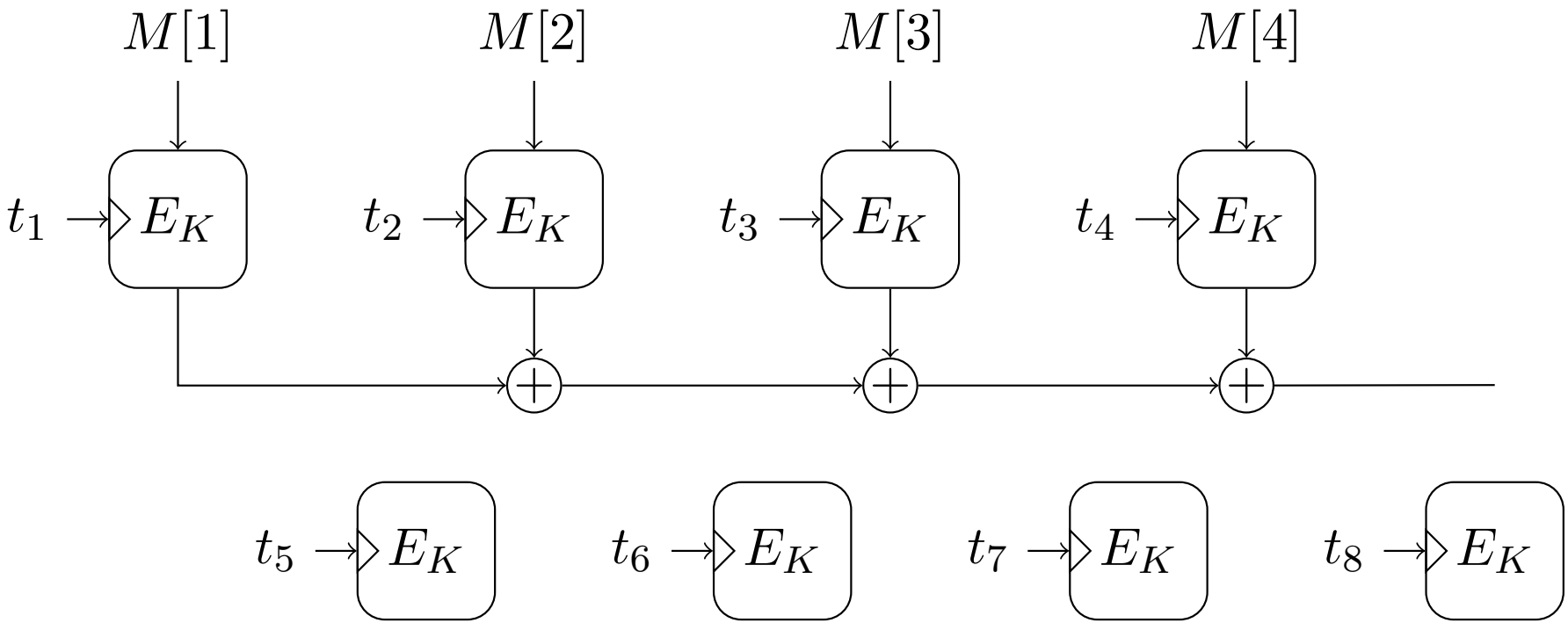
Achieving Parallelizability



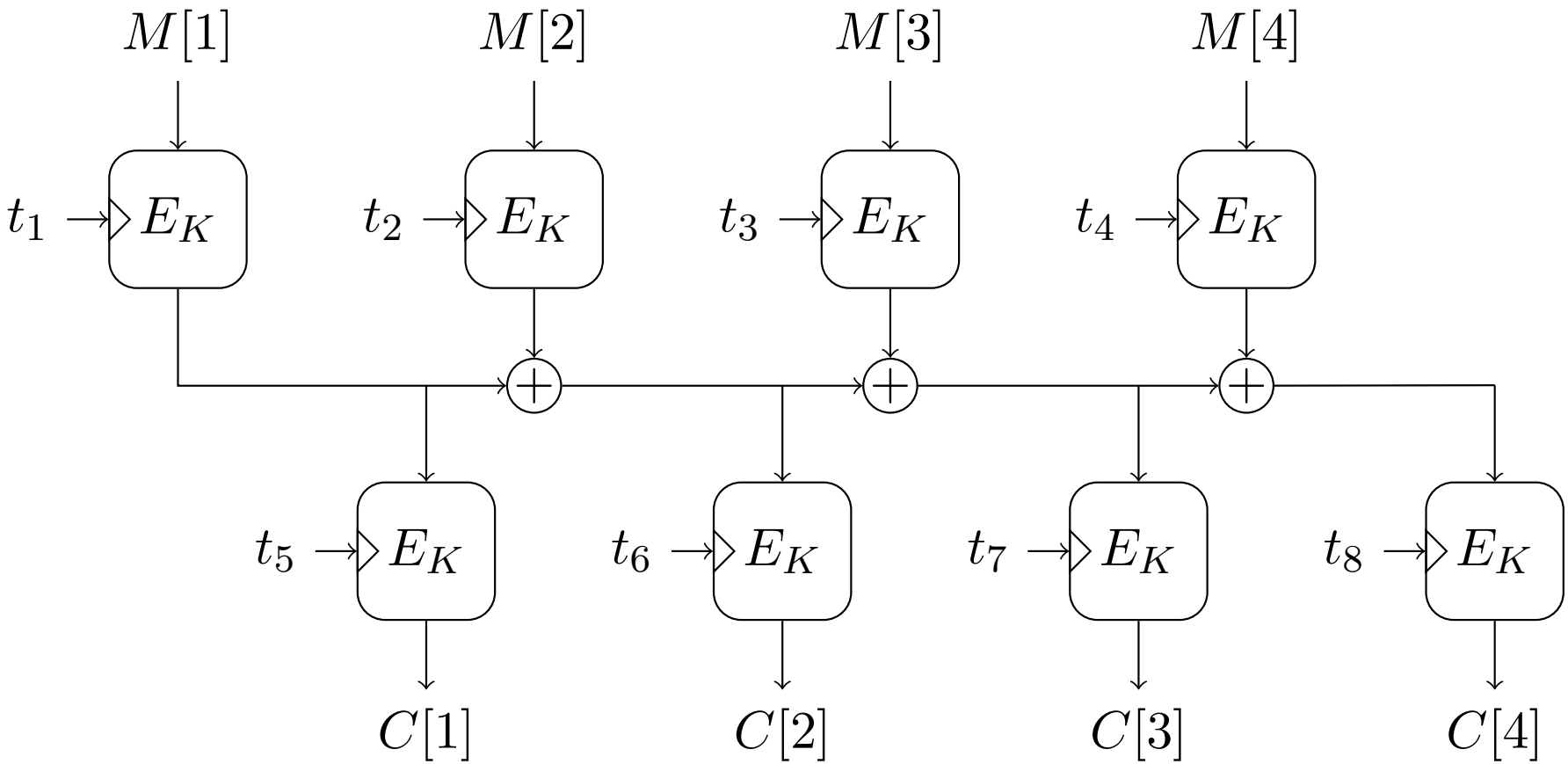
Achieving Parallelizability



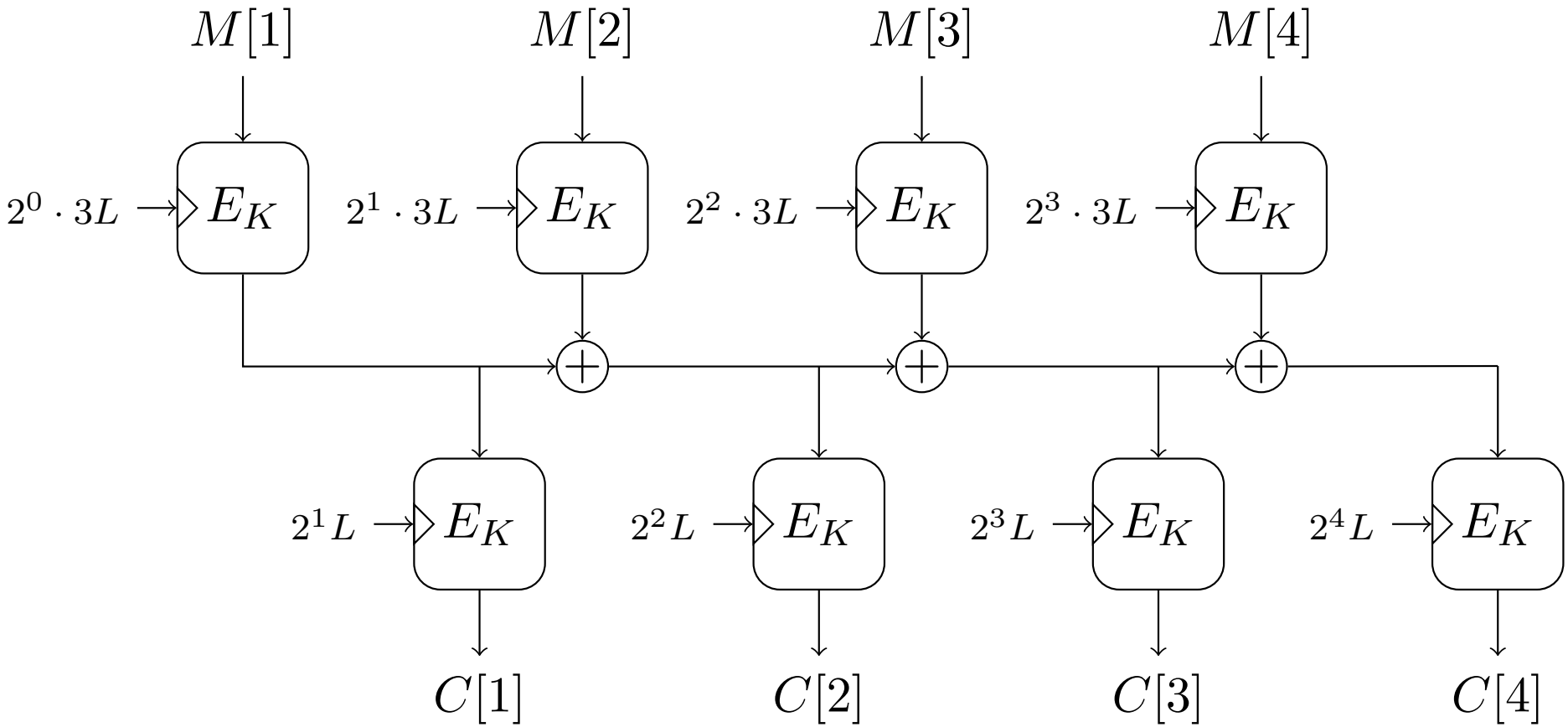
Achieving Parallelizability



Achieving Parallelizability

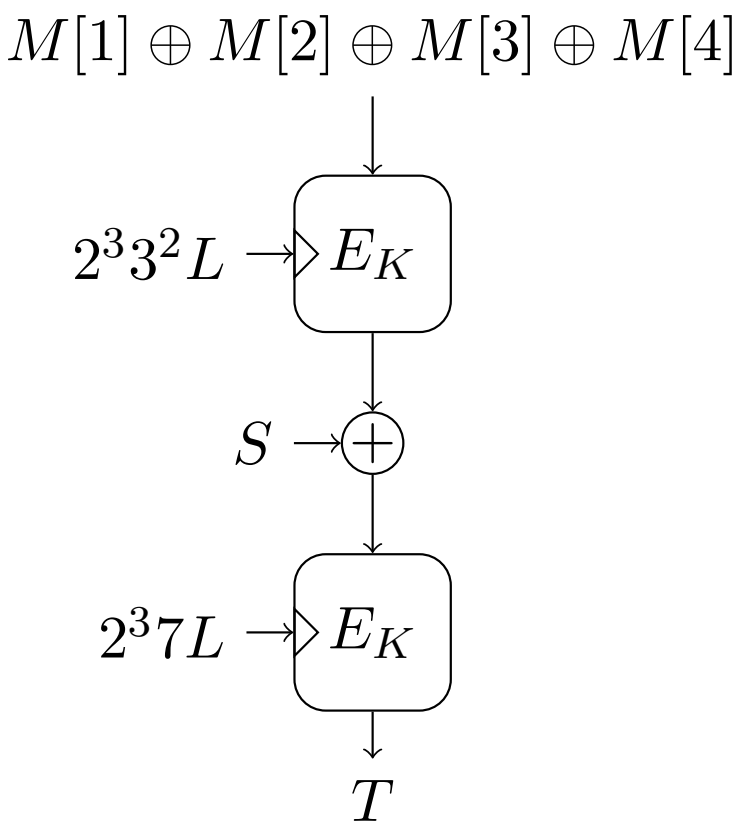


Our Online Cipher: COPE

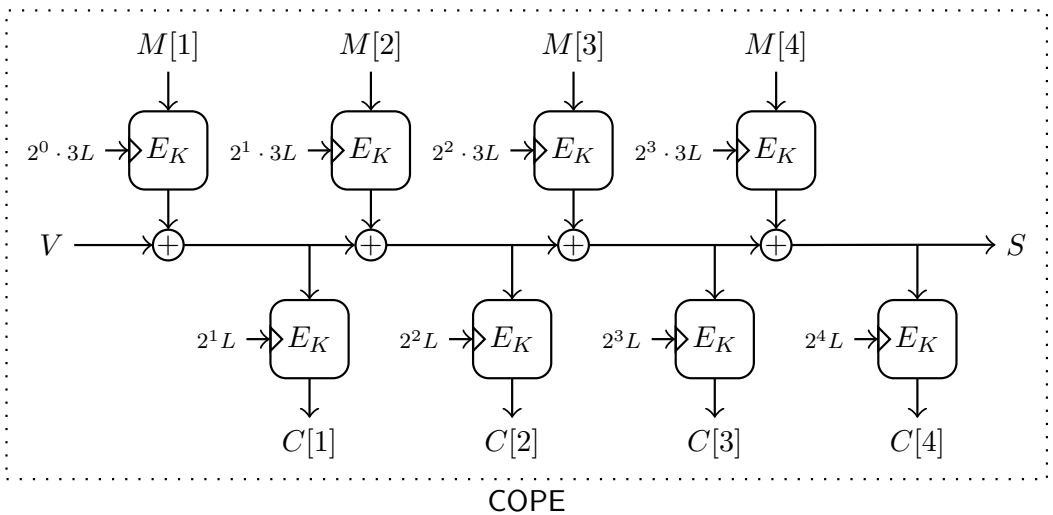


$$L := E_K(0)$$

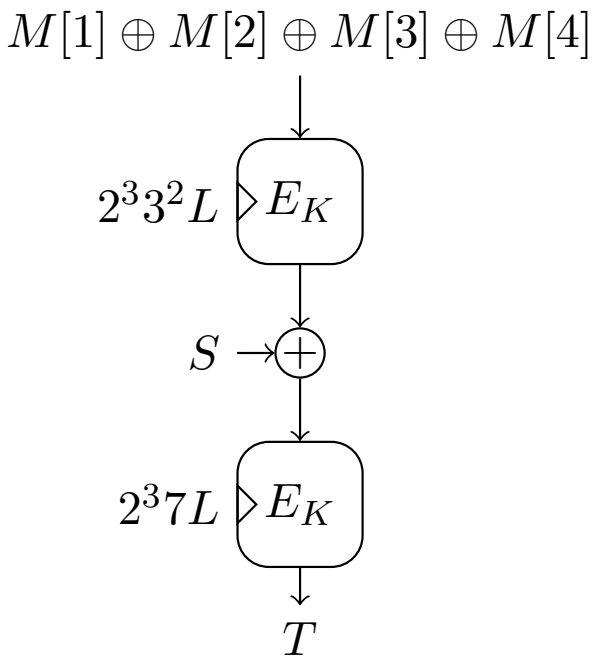
Adding Authenticity to COPE



Our Authenticated Online Cipher: COPA



COPE



Note: COPA also accepts associated data (while maintaining parallelizability)

Security

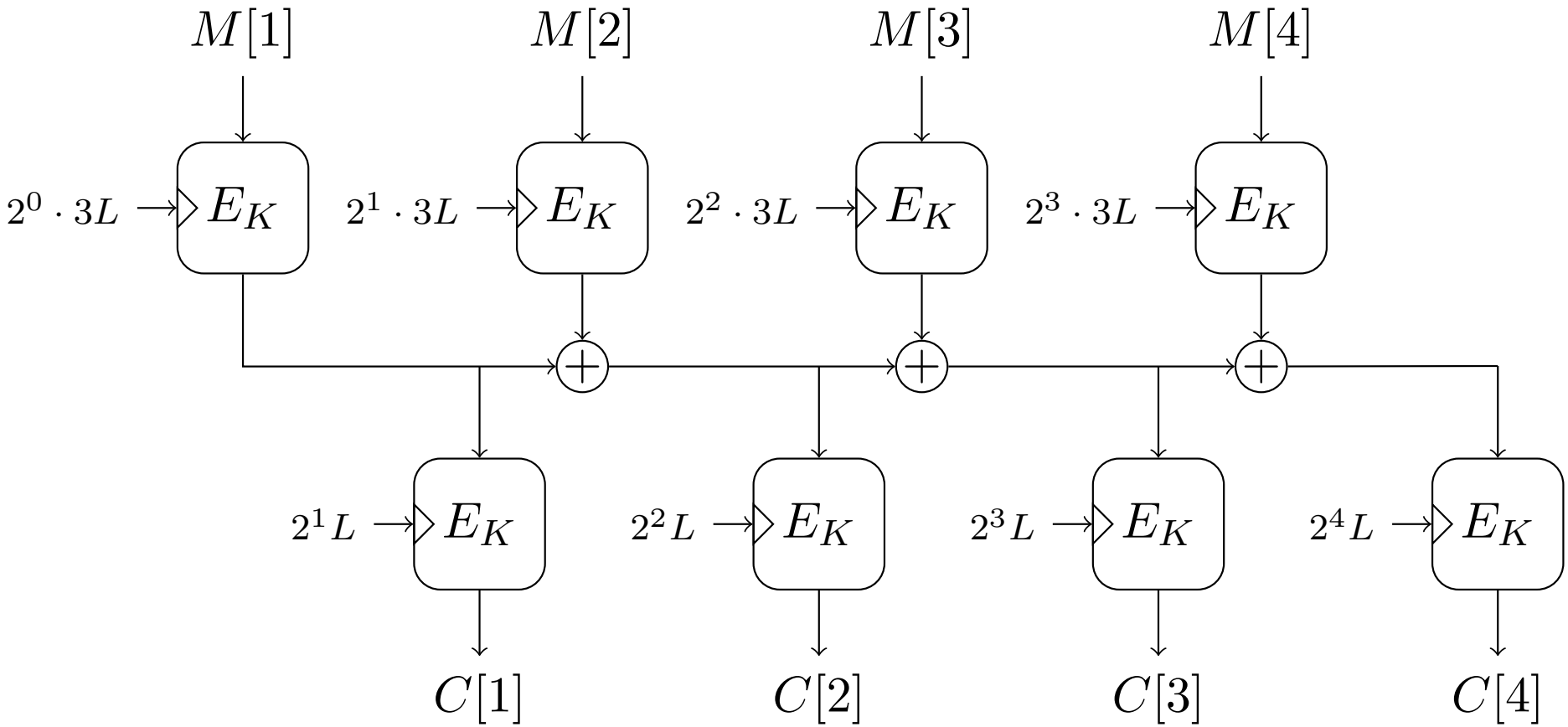
σ: total length of all queries in number of blocks
$a \approx 40, b \approx 4$

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{COPE}}(t, \sigma) \leq \frac{a \cdot \sigma^2}{2^n} + \mathbf{Adv}^{\mathrm{prp}\pm 1}_{E}(t', b \cdot \sigma)$$

$$\mathbf{Adv}^{\mathrm{cpa}}_{\mathsf{COPA}}(t, \sigma) \leq \frac{a \cdot \sigma^2}{2^n} + \mathbf{Adv}^{\mathrm{prp}\pm 1}_{E}(t', b \cdot \sigma)$$

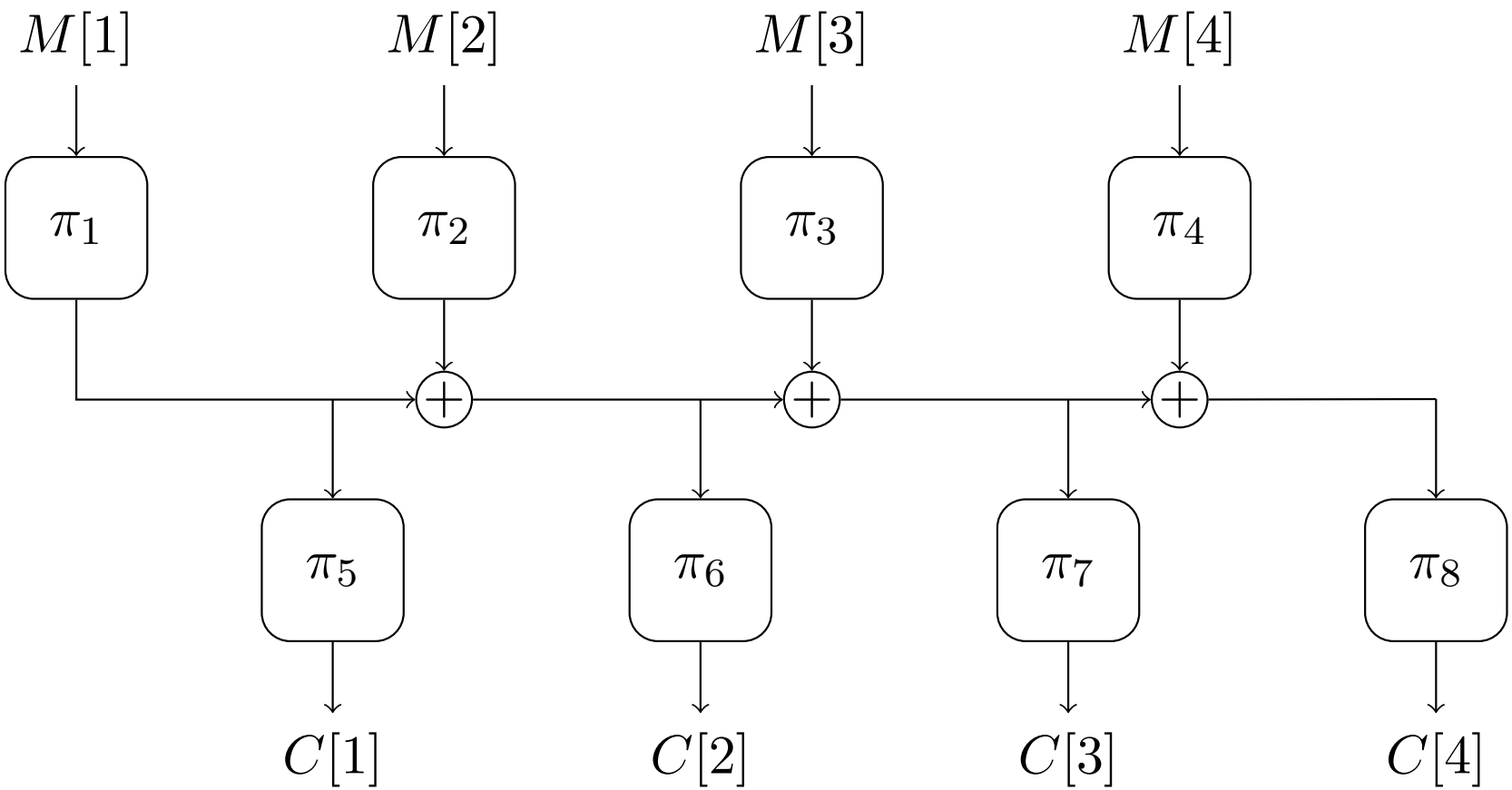
$$\mathbf{Adv}^{\mathrm{int}}_{\mathsf{COPA}}(t, \sigma) \leq \frac{a \cdot \sigma^2}{2^n} + \mathbf{Adv}^{\mathrm{prp}\pm 1}_{E}(t', b \cdot \sigma)$$

Security: Proof Idea

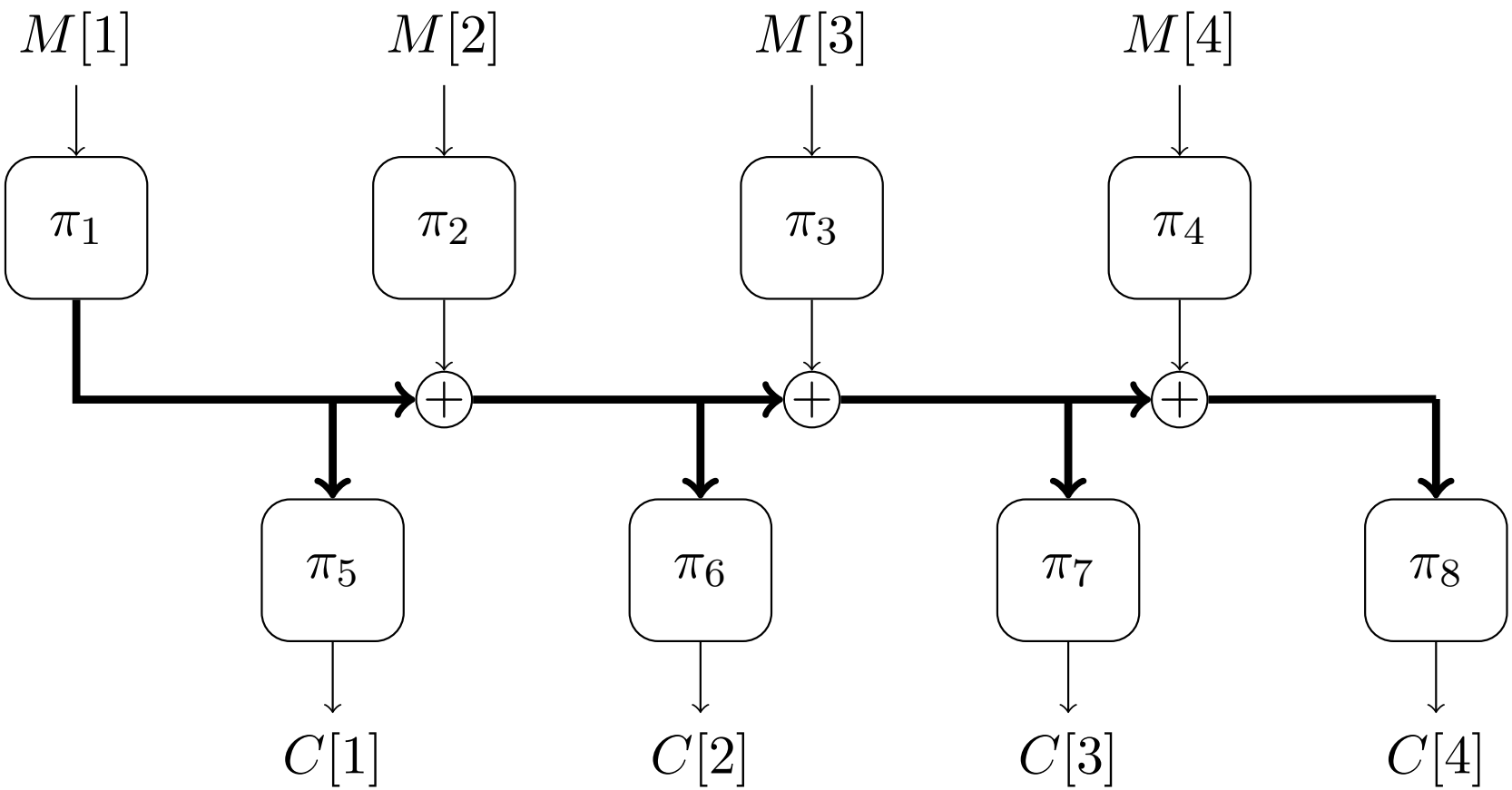


$$L := E_K(0)$$

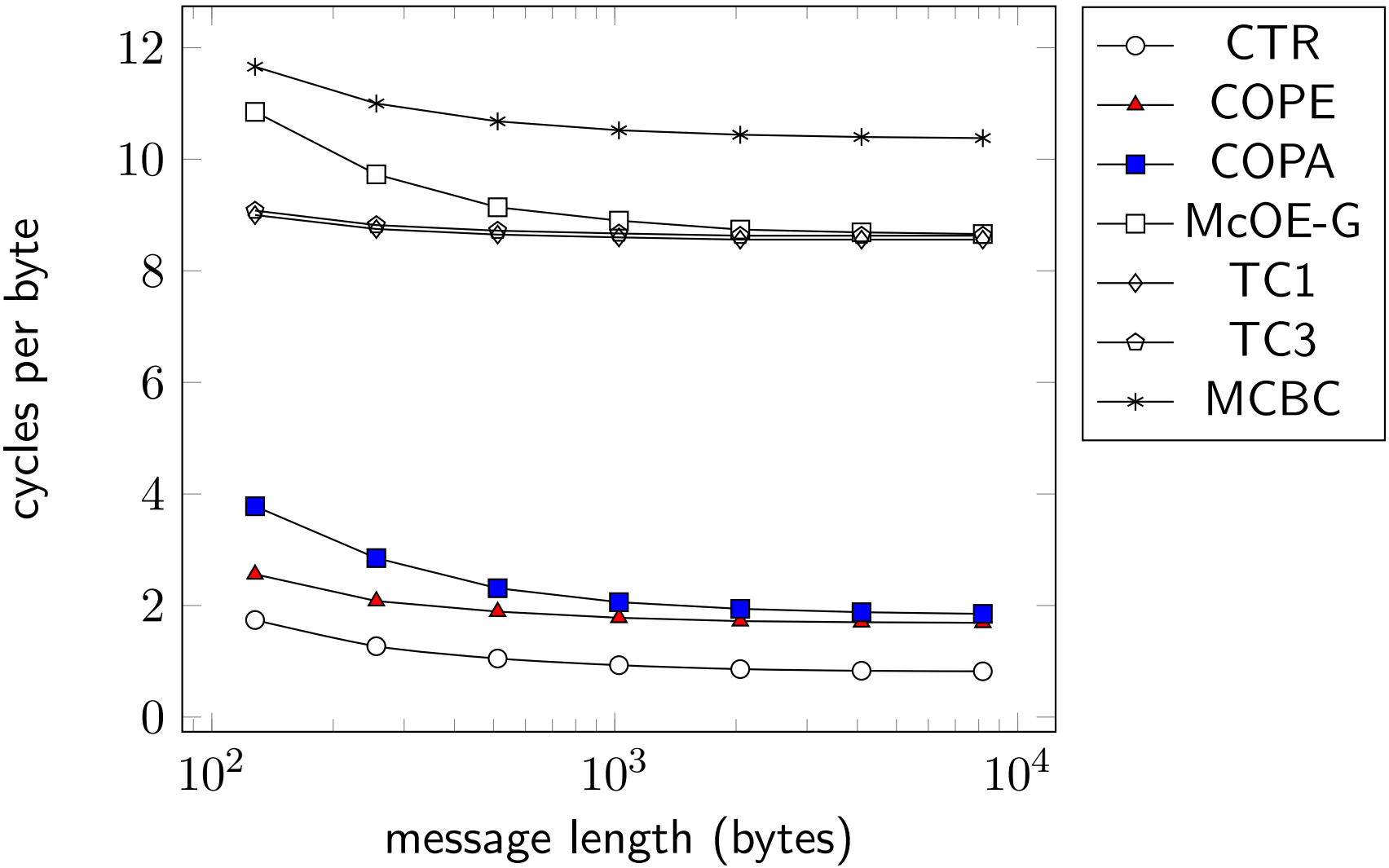
Security: Proof Idea



Security: Proof Idea



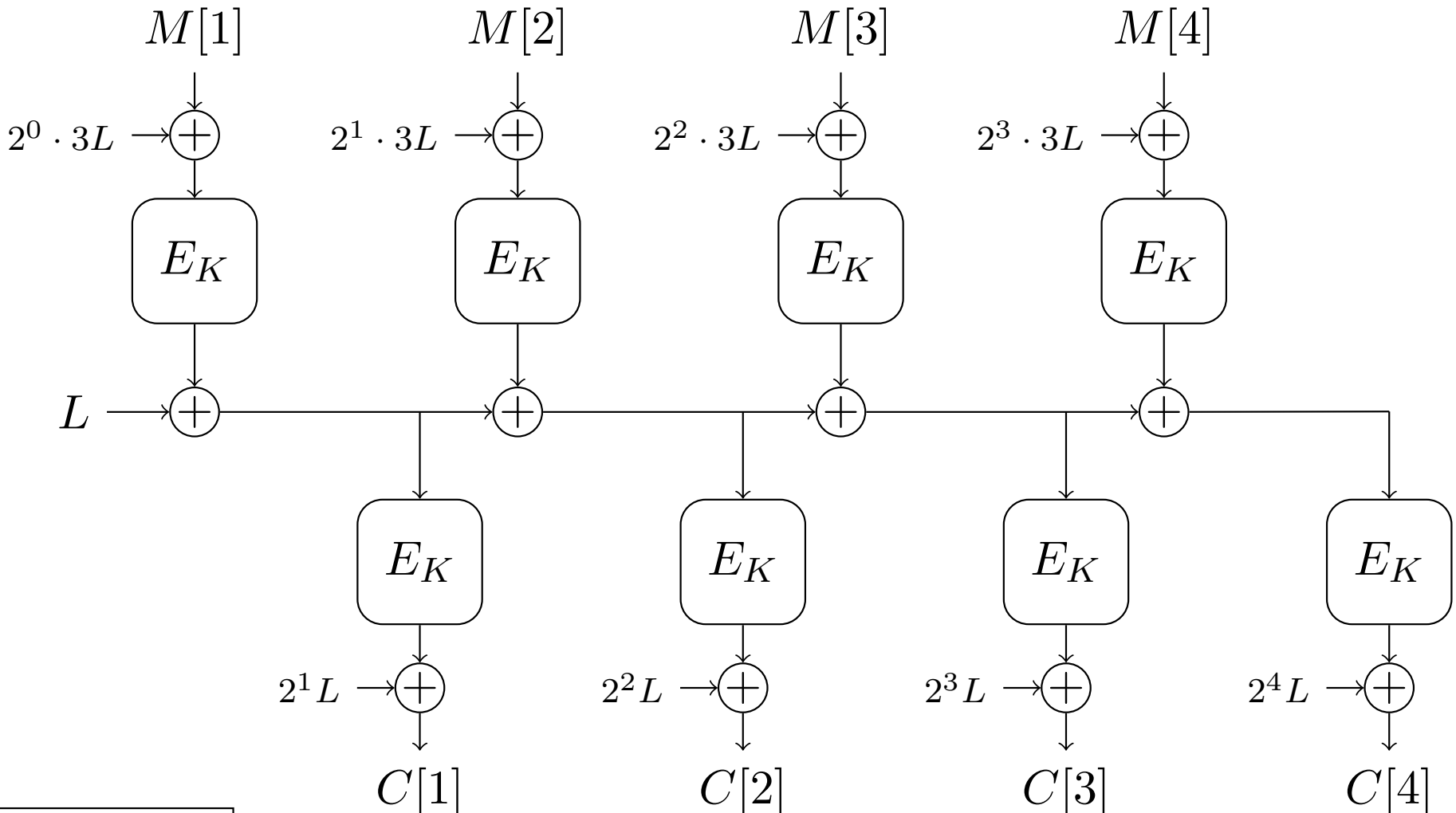
Results: Using AES-NI on Intel Sandy Bridge



Summary

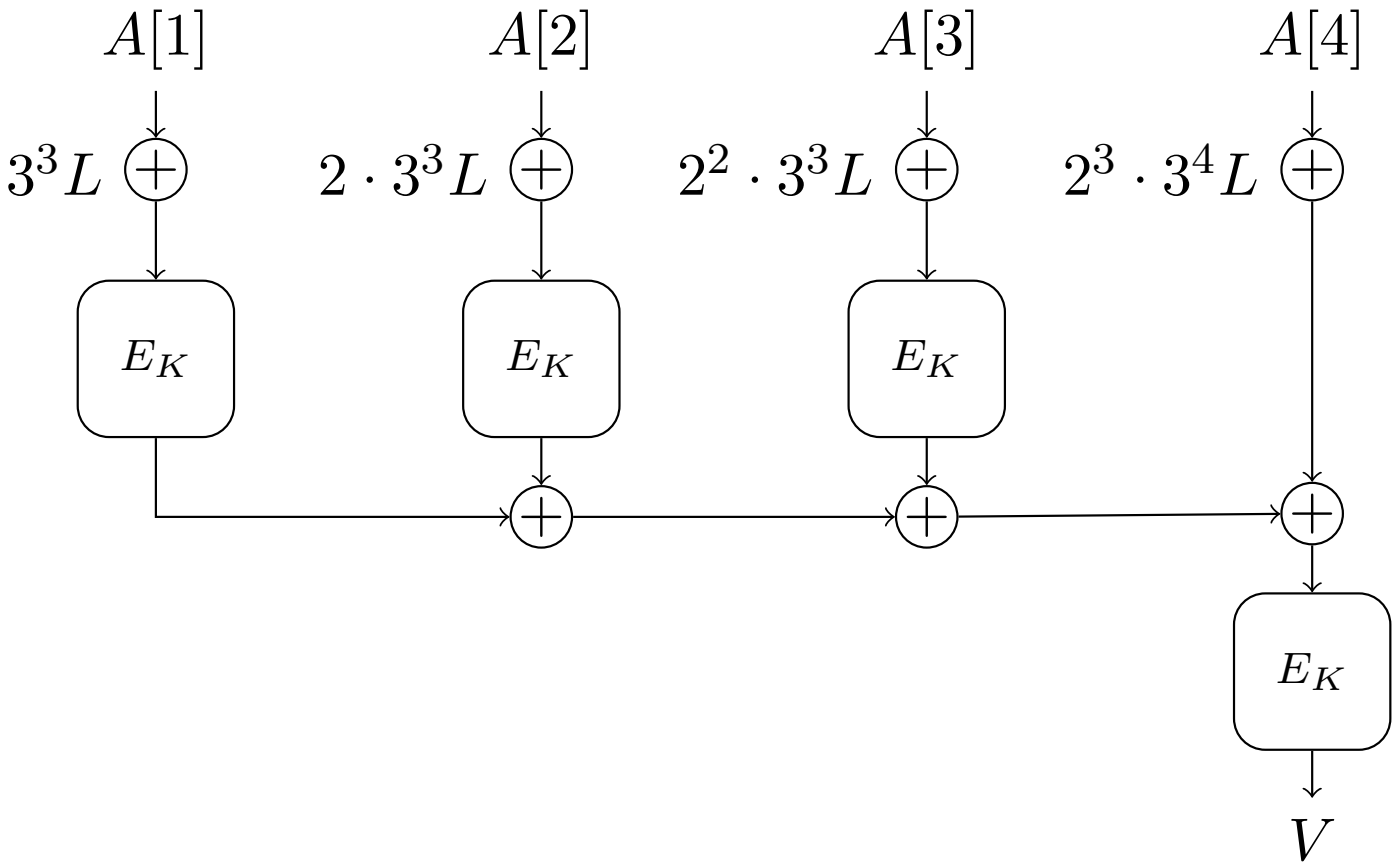
1. COPE: first parallelizable, online cipher
2. COPA: misuse resistant authenticated encryption (with associated data)
   - efficient
   - security reduction to block cipher
   - CAESAR submission

COPE


$M[1]$
$M[2]$
$M[3]$
$M[4]$
$2^0 \cdot 3L$
$2^1 \cdot 3L$
$2^2 \cdot 3L$
$2^3 \cdot 3L$
E_K
L
$2^1 L$
$2^2 L$
$2^3 L$
$2^4 L$
$C[1]$
$C[2]$
$C[3]$
$C[4]$

$L := E_K(0)$

Associated Data in COPA



Results

Table : Software performance of (authenticated) online ciphers based on the AES on the Intel Sandy Bridge platform (AES-NI). All numbers are given in cycles per byte (cpb).

	message length (bytes)						
Algorithm	128	256	512	1024	2048	4096	8192
CTR	1.74	1.27	1.05	0.93	0.86	0.83	0.82
TC1	9.00	8.75	8.65	8.60	8.56	8.56	8.56
TC3	9.08	8.82	8.72	8.67	8.63	8.63	8.62
MCBC	11.66	11.00	10.68	10.52	10.44	10.40	10.38
COPE	2.56	2.08	1.89	1.78	1.72	1.70	1.69
McOE-G	10.85	9.73	9.14	8.90	8.74	8.69	8.66
COPA	3.78	2.85	2.31	2.06	1.94	1.88	1.85