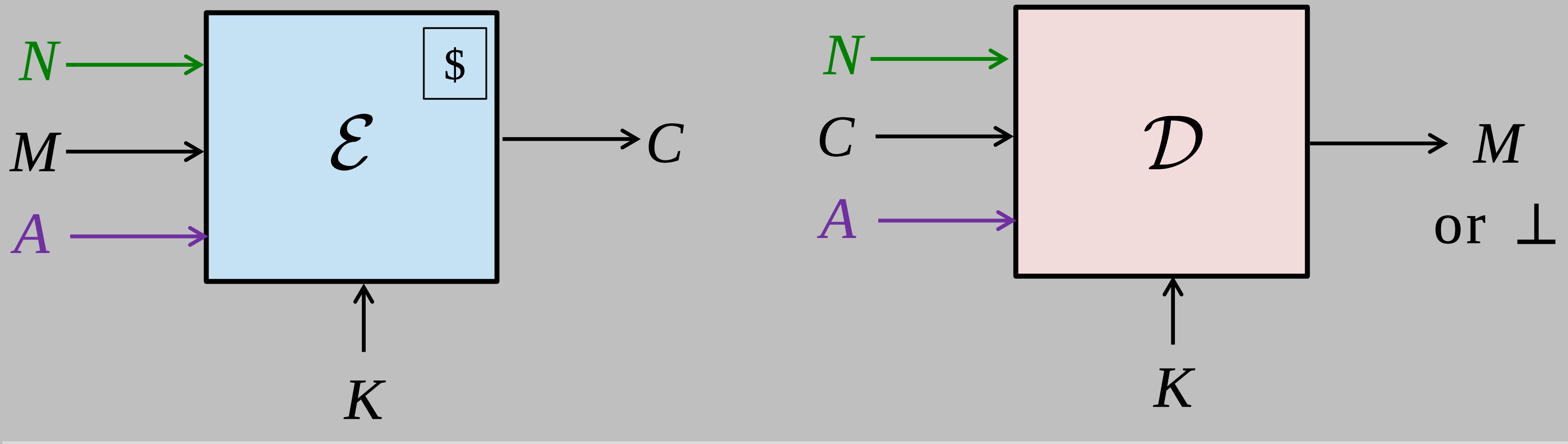


1) Move the coins out of $\mathcal{E}$ — make it deterministic **[RBBK01]**

To improve resistance to random-number generation problems
To architect to existing abstraction boundaries

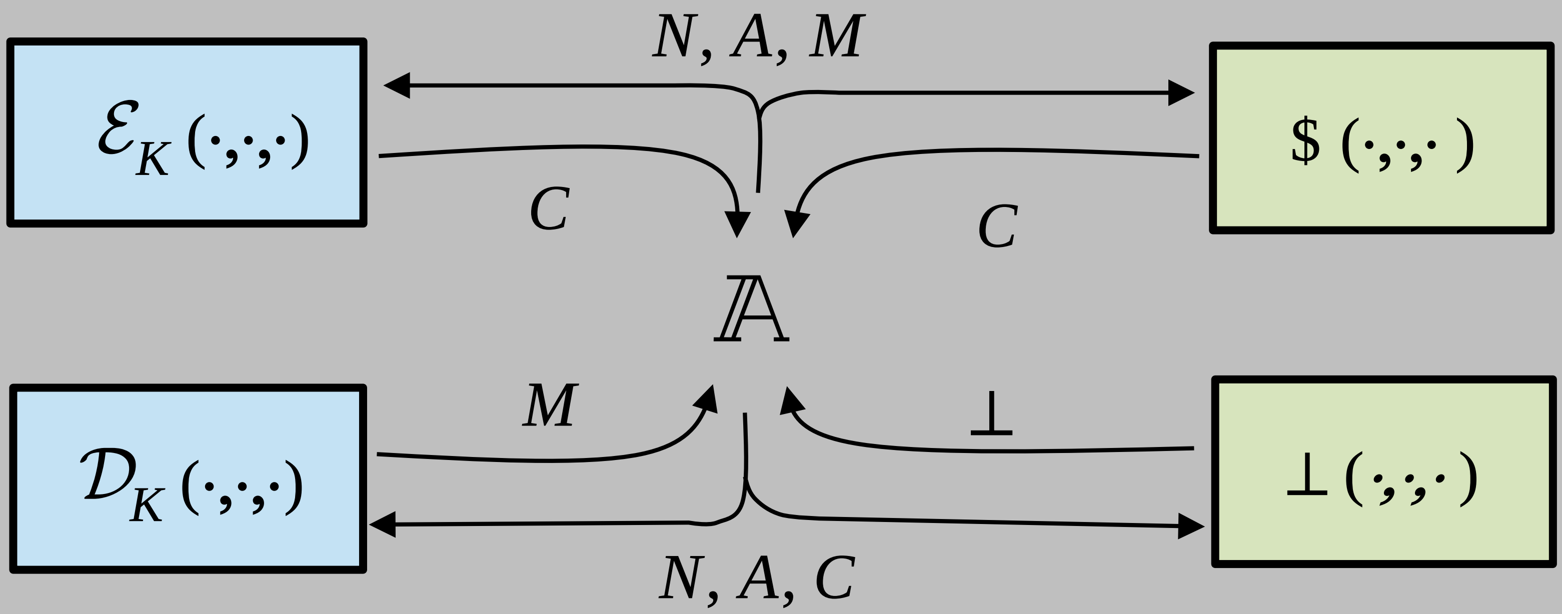
2) Add in "associated data" (AD) **[R02]**

To authenticate headers

Syntax: An AEAD scheme is a 3-tuple $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where

- $\mathcal{K}$ is a probabilistic algorithm that returns a string;
- $\mathcal{E}$ is a deterministic algorithm that maps a tuple (K, N, A, M) to a ciphertext $C = \mathcal{E}(K, N, A, M)$ of length $|M|+\tau$; and
- $\mathcal{D}$ is a deterministic algorithm that maps a tuple (K, N, A, C) to a plaintext M or the symbol $\perp$

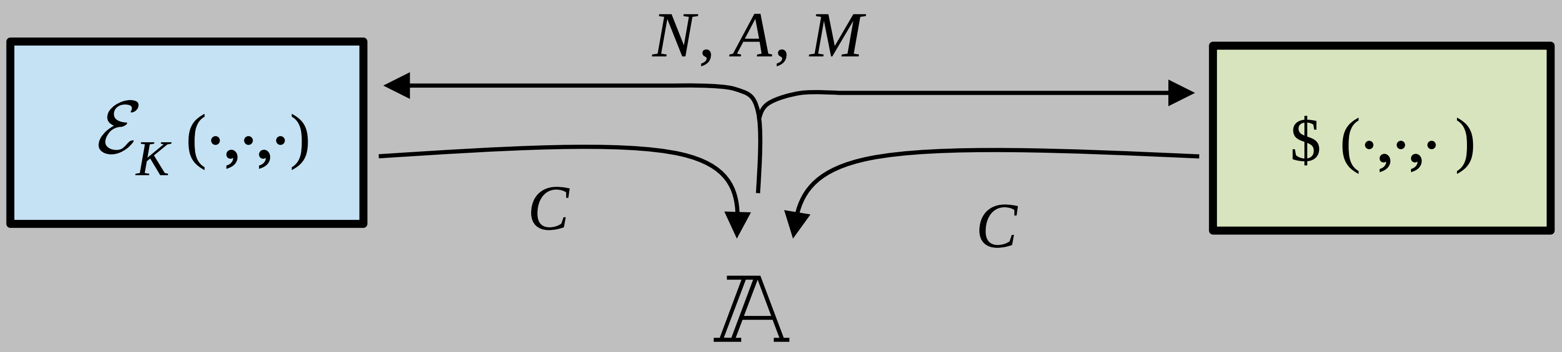
If $C = \mathcal{E}(K, N, A, M) \neq \perp$ then $\mathcal{D}(K, N, A, C) = M$


N, A, M
$\mathcal{E}_K(\cdot,\cdot,\cdot)$
$\$(\cdot,\cdot,\cdot)$
C
C
$\mathbb{A}$
M
$\perp$
$\mathcal{D}_K(\cdot,\cdot,\cdot)$
$\perp(\cdot,\cdot,\cdot)$
N, A, C

$$\mathbf{Adv}_{\mathcal{E}}^{\text{aead}}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K,\, \mathcal{D}_K} \rightarrow 1] \; - \; \Pr[\mathbb{A}^{\$,\, \perp} \rightarrow 1]$$

$\mathbb{A}$ may not:

- Repeat an N in an enc query
- Ask a dec query (N, A, C) after C is returned by an $(N, A, \cdot)$ enc query



$\mathcal{E}_K(\cdot,\cdot,\cdot)$

N, A, M

$\$(\cdot,\cdot,\cdot)$

C

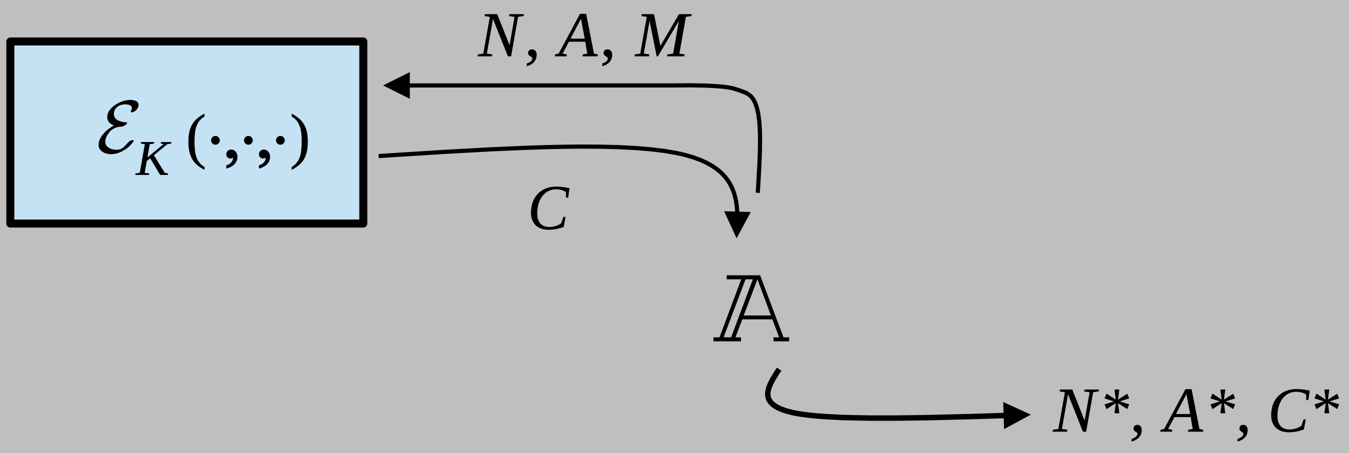
C

$\mathbb{A}$

$$\mathbf{Adv}^{\text{priv}}_{\mathcal{E}}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K} \rightarrow 1] - \Pr[\mathbb{A}^{\$} \rightarrow 1]$$

$\mathbb{A}$ may not:

- Ask a dec query (N, A, C) after C is returned by an $(N, A, \cdot)$ enc query



$\mathcal{E}_K(\cdot,\cdot,\cdot)$

N, A, M

C

$\mathbb{A}$

N^*, A^*, C^*

$$\mathbf{Adv}^{\text{auth}}_{\mathcal{E}}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathcal{E}_K} \text{ forges}]$$

It outputs an (N^*, A^*, C^*) where $\mathcal{D}(K, N^*, A^*, C^*) \neq \perp$ and no prior oracle query of (N^*, A^*, M) returned C^*

All-in-one definition

$$\mathbf{Adv}^{\mathrm{aead}}_{\Pi}(A) = \Pr[A^{\mathcal{E}(K,\,\cdots),\,\mathcal{D}(K,\,\cdots)} \Rightarrow 1] - \Pr[A^{\$(\cdots),\,\perp(\cdots)} \Rightarrow 1]$$

A may not repeat any *N* query to its Enc oracle.
It may not ask Dec(*N*, *A*, *C*) after an Enc(*N*, *A*, *M*) returned *C*.

Two-part definition

$$\mathbf{Adv}^{\mathrm{priv}}_{\Pi}(A) = \Pr[A^{\mathcal{E}(K,\,\cdots)} \Rightarrow 1] - \Pr[A^{\$(\cdots)} \Rightarrow 1]$$

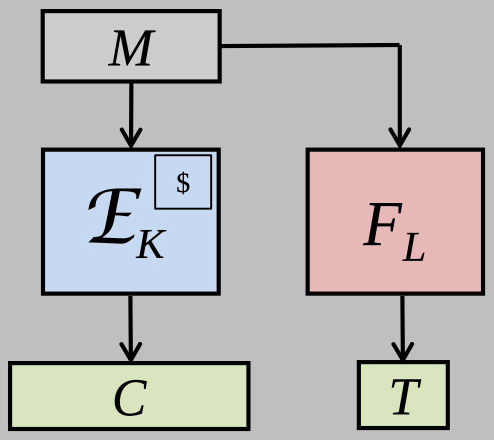
A may not repeat any *N* query.

$$\mathbf{Adv}^{\mathrm{auth}}_{\Pi}(A) = \Pr[A^{\mathcal{E}(K,\,\cdots)} \text{ forges}]$$

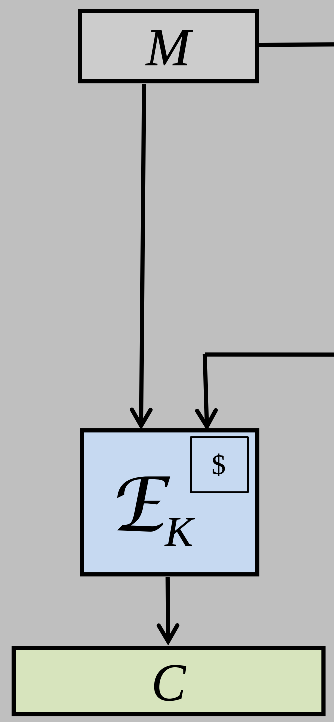
It outputs an (N, A, C) where $\mathcal{D}(K, N, A, C) \neq \perp$ and
no prior oracle query of (N, A, M) returned C

Generic composition

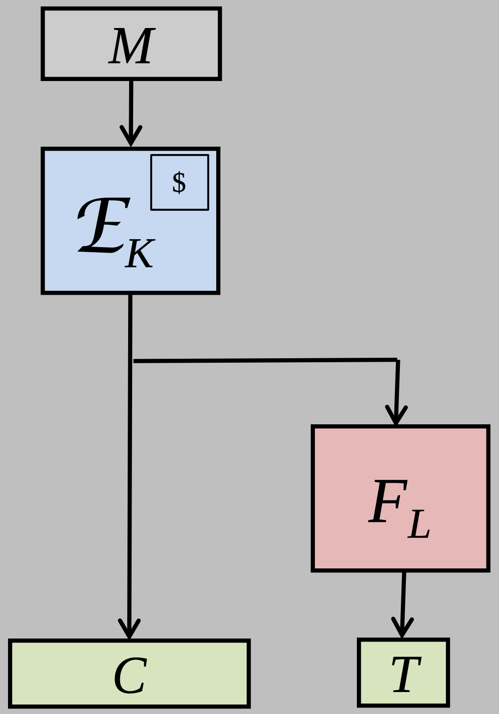
[Bellare, Namprempre 2000]



✗ **Encrypt-and-MAC**



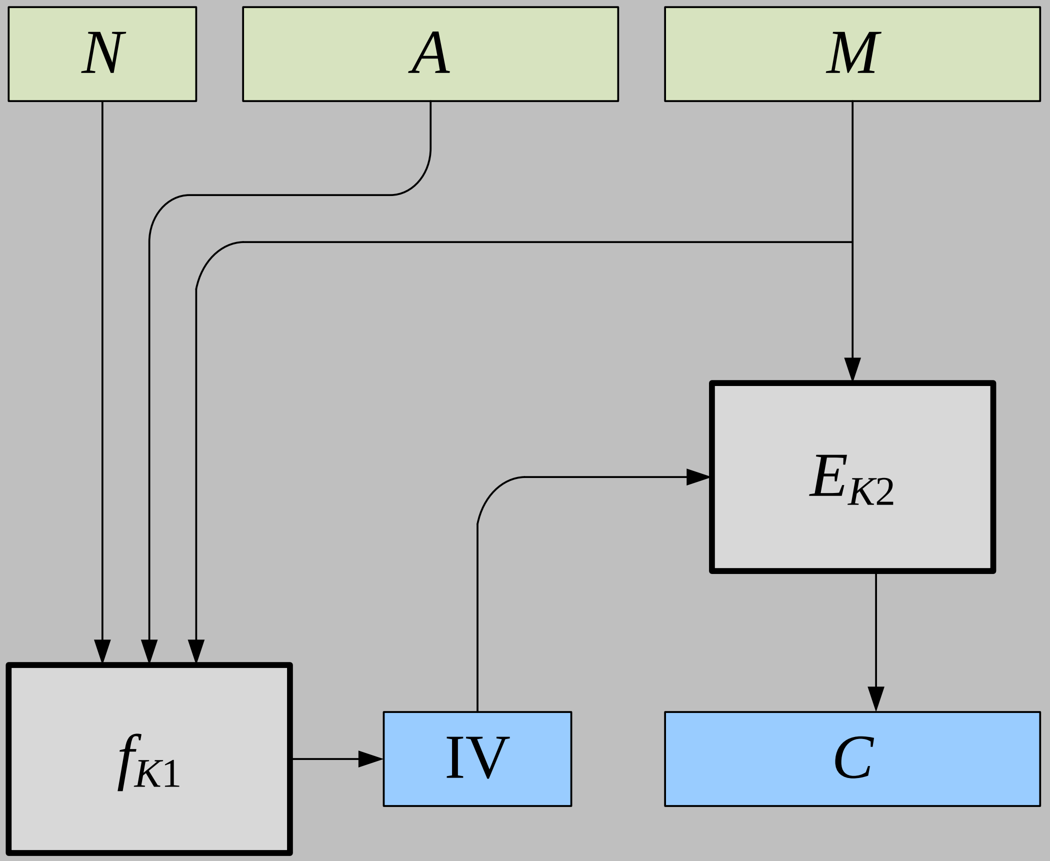
✗ **MAC-then-Encrypt**



✓ **Encrypt-then-MAC**

SIV mode

[Rogaway, Shrimpton 2006]

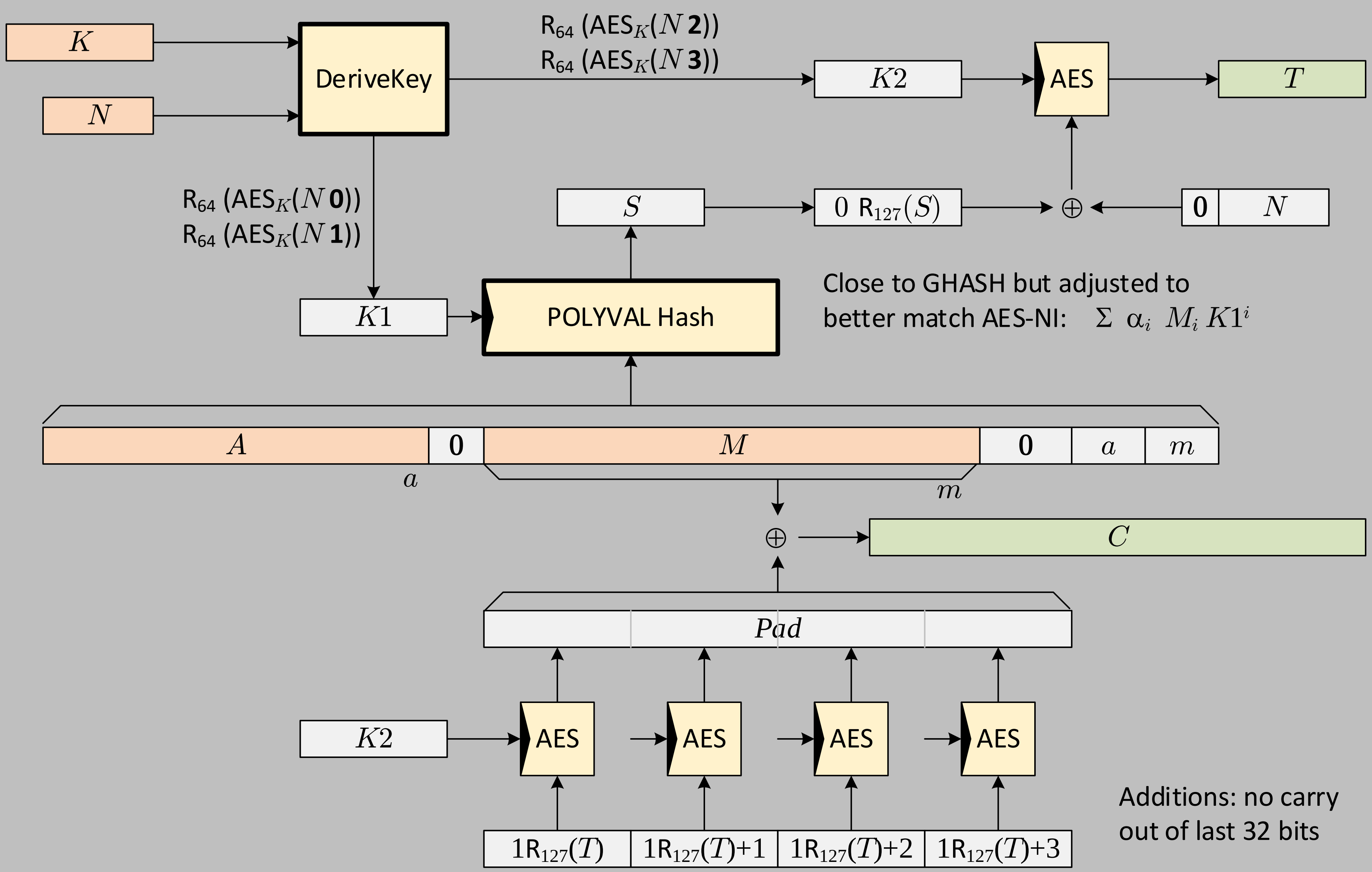


ivE encryption scheme (eg, CTR), secure

PRF operating on a **vector** of strings

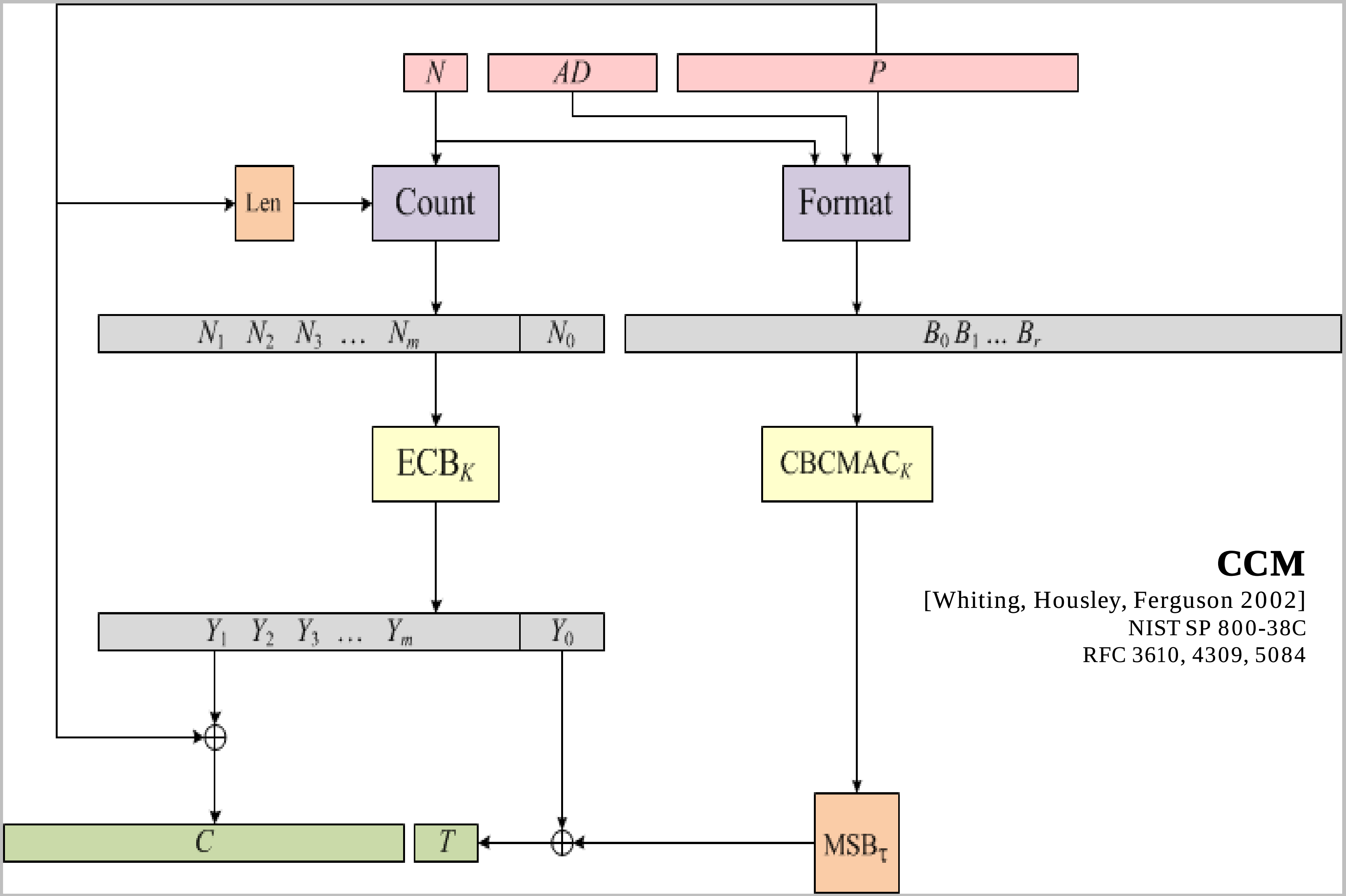
AES-GCM-SIV

[Gueron, Langley, Lindell 2017]
[Bose, Hoang, Tessaro 2018]



Close to GHASH but adjusted to better match AES-NI: $\Sigma\ \alpha_i\ M_i\ K1^i$

Additions: no carry out of last 32 bits



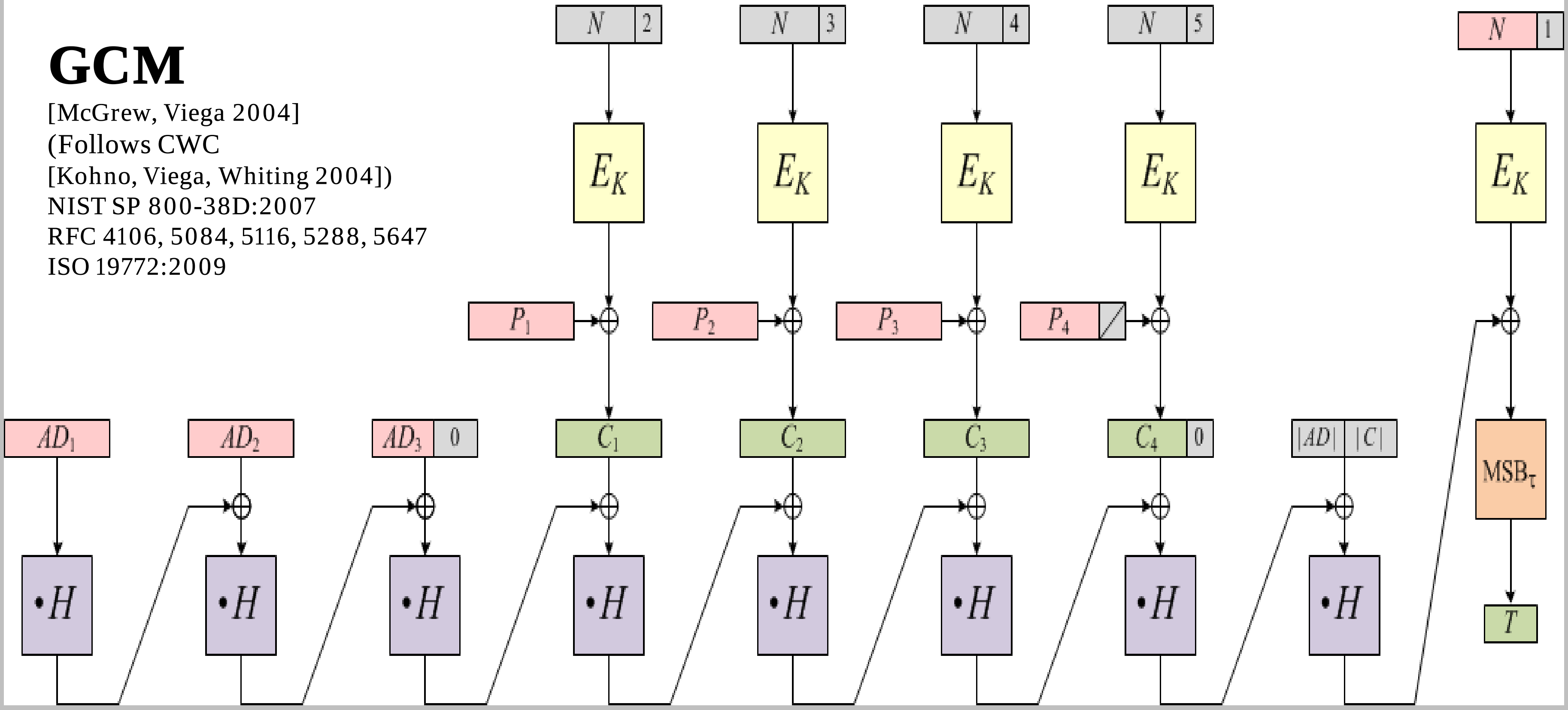
CCM

[Whiting, Housley, Ferguson 2002]
NIST SP 800-38C
RFC 3610, 4309, 5084

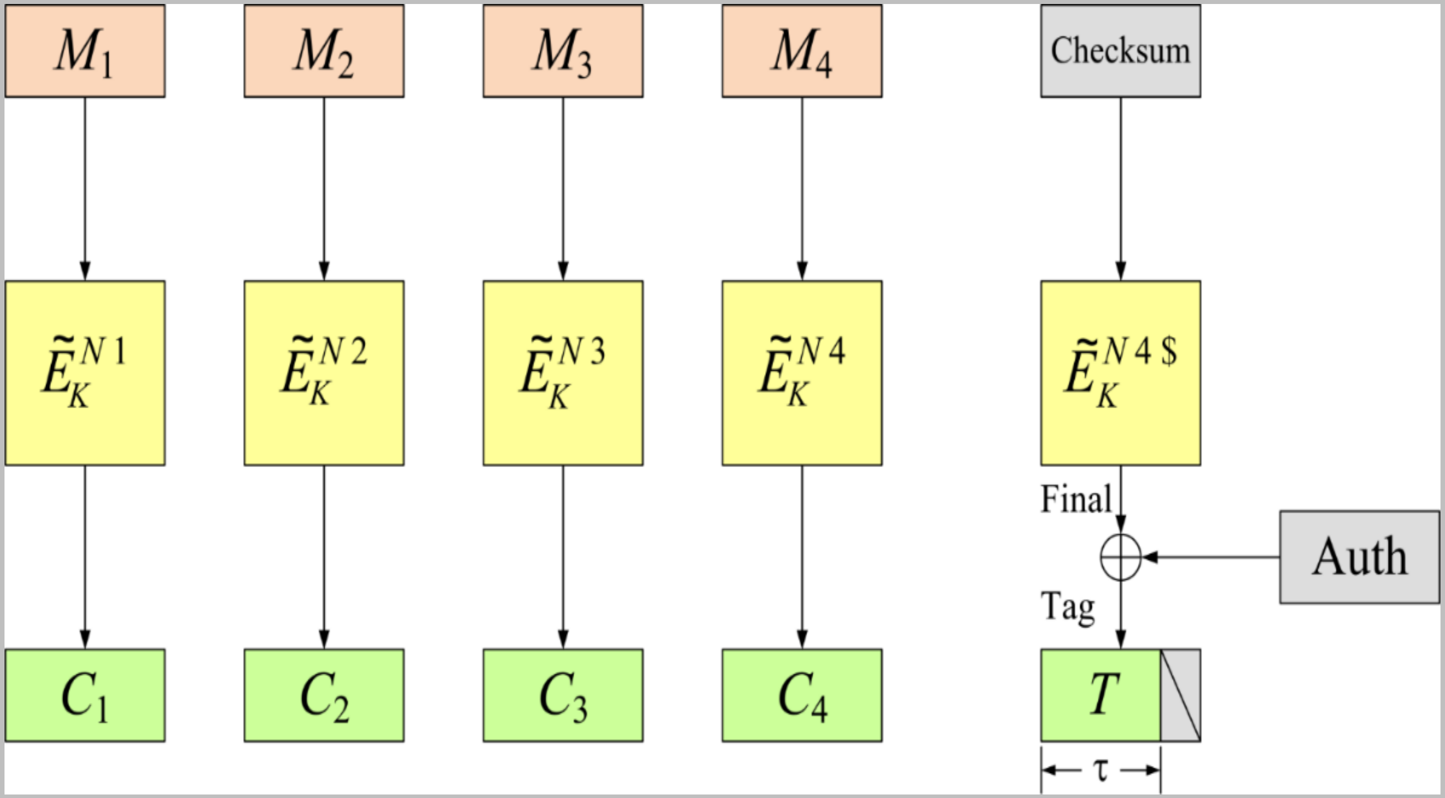
Thm [Jonsson 2002] CCM is provably secure if *E* is a good PRP.

GCM

[McGrew, Viega 2004]
(Follows CWC
[Kohno, Viega, Whiting 2004])
NIST SP 800-38D:2007
RFC 4106, 5084, 5116, 5288, 5647
ISO 19772:2009



Thm [Iwata , Ohashi , and Minematsu 2012] (correcting [McGrew, Viega 2004])
GCM is provably secure (not great bounds) if E is a good PRP.



OCB (v3)

[Krovetz Rogaway 2011] , following
[RBBK01,LRW02,R04]
RFC 7253

Thm [Krovetz, Rogaway 2011]
OCB is provably secure (OK bounds) if *E* is a strong PRP.

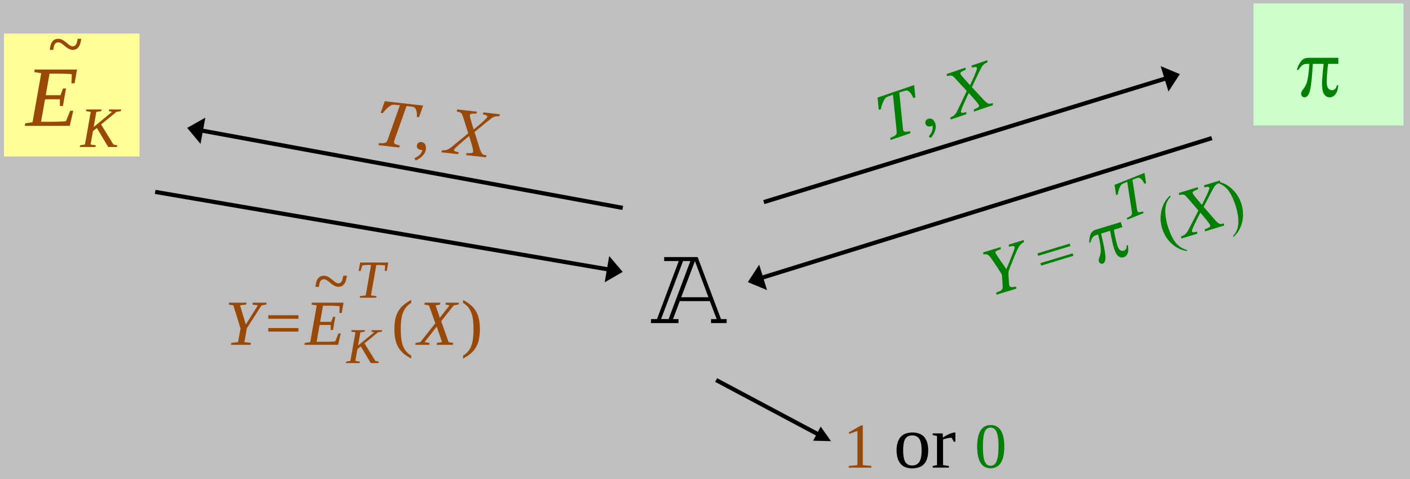
[Liskov, Rivest, Wagner 2002]

Tweakable Blockcipher (TBC)

$\tilde{E}\colon \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$

each $\tilde{E}_K^T(\cdot) = \tilde{E}(K, T, \cdot)$ a **permutation**

A $\mathcal{T}$-indexed family of random permutations on n bits



$$\boxed{\mathbf{Adv}^{\mathrm{prp}}_{\tilde{E}}(\mathbb{A}) = \Pr[\mathbb{A}^{\tilde{E}_K} \Rightarrow 1] - \Pr[\mathbb{A}^{\pi} \Rightarrow 1]}$$

This is the official public announcement of the portfolio, bringing the CAESAR competition to a close. ... [H]ere is the final portfolio:

Use case 1: **Ascon** first choice, **ACORN** second choice.
Use case 2: **AEGIS-128** and **OCB**, without a preference.
Use case 3: **Deoxys-II** first choice, **COLM** second choice.

57 round-1
(Mar 2014)

29 round-2
(Mar 2014)

16 round-3
(Aug 2016)

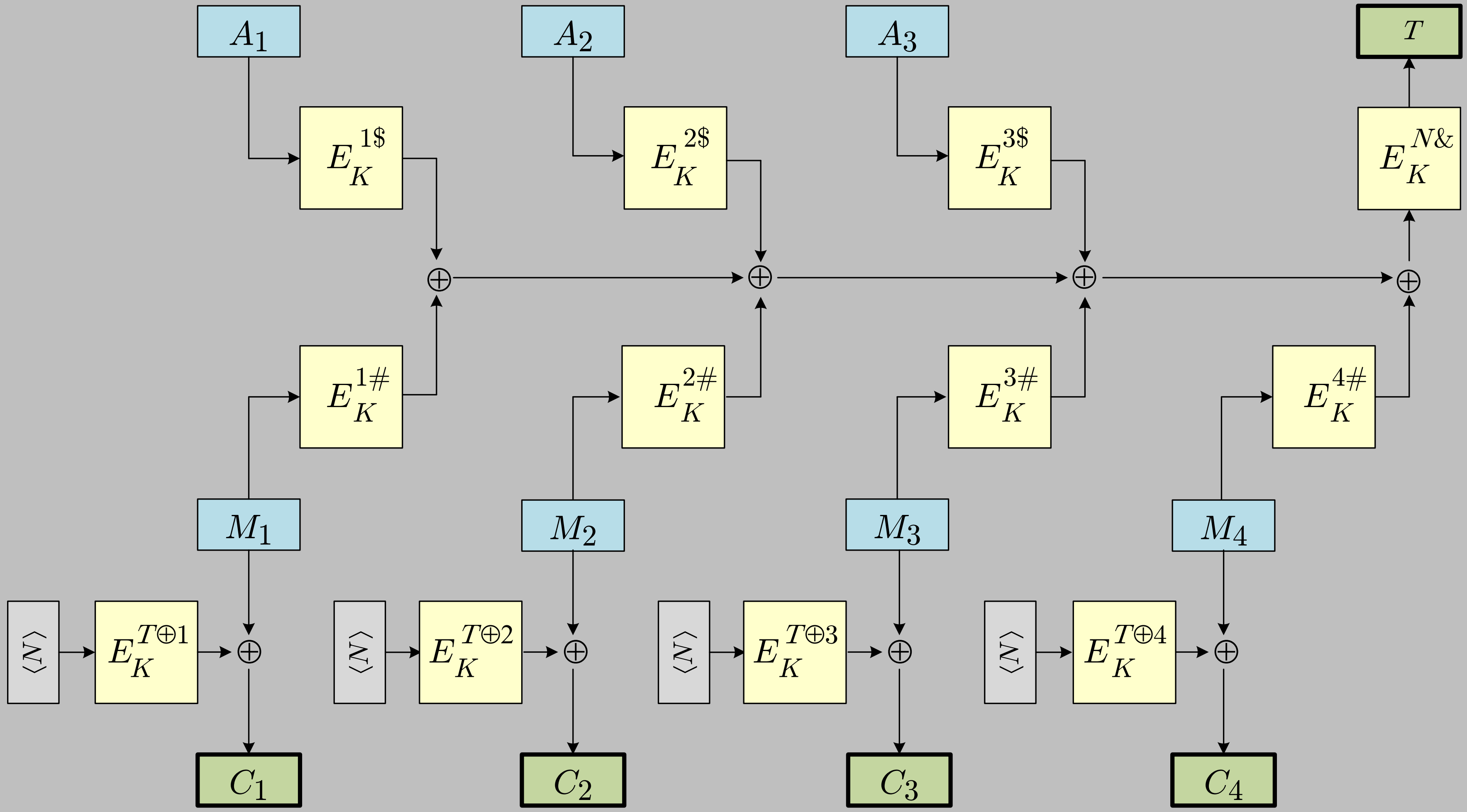
7 finalists
(Mar 2018)

6 winners
(Feb 209)

Deoxys-II

Jean, Nikolić,
Peyrin, Seurin

Thm: Provably secure, with excellent bounds, if E is a TBC.



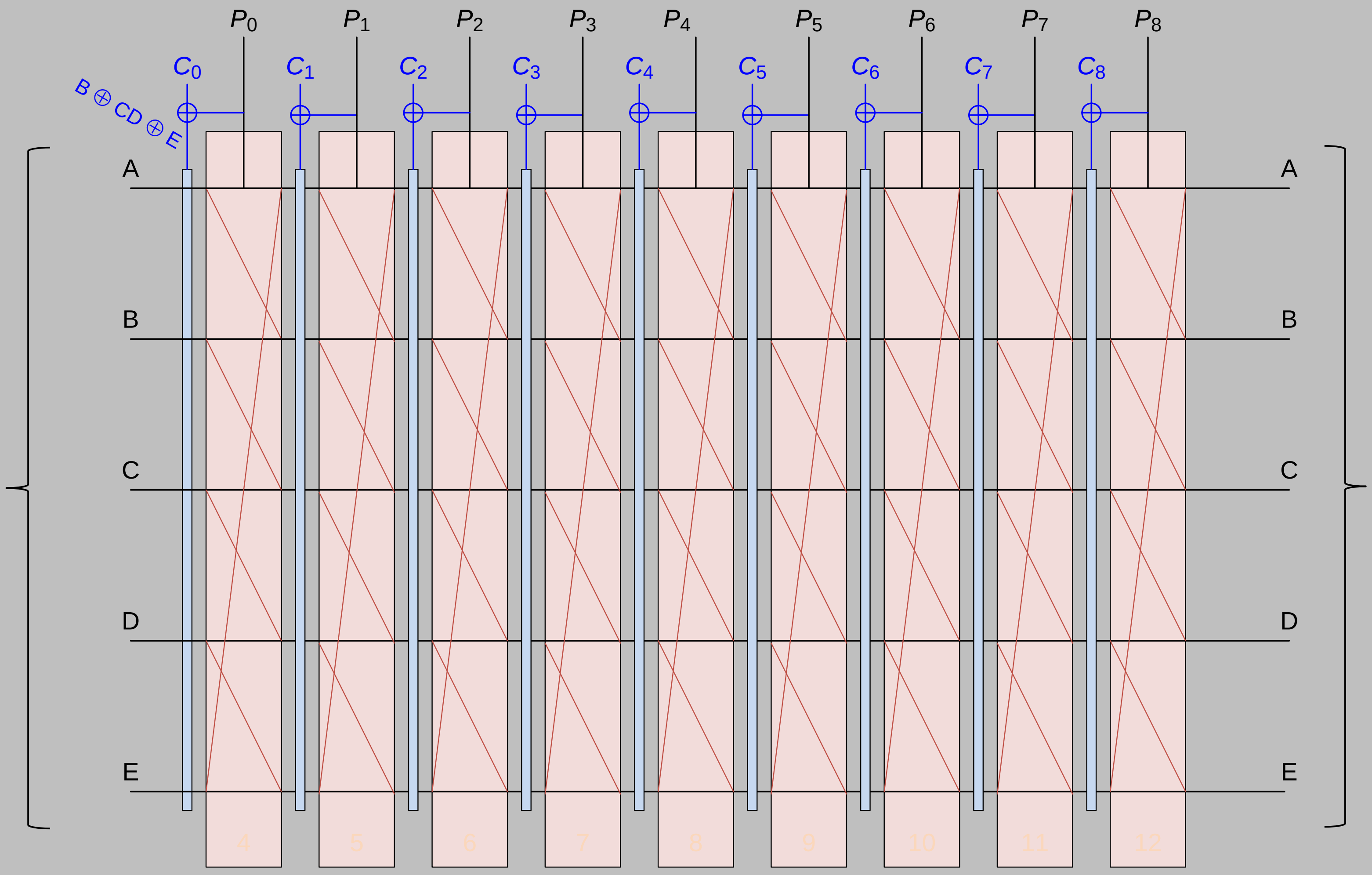
AEGIS

AEGIS-128
[Wu, Preneel 2013]

0.43 cpb (Skylake)
(**0.25 cpb** for **AEGIS-128L**
on 16K messages)

The fastest
CAESAR finalist
on recent Intel processors

K, N, A dependent initialization



$|A|$, $|P|$ dependent
tag computation