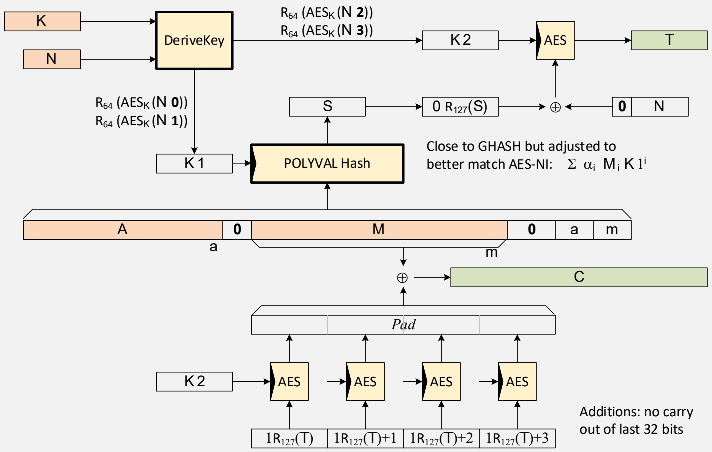
The Rise of Authenticated Encryption



Close to GHASH but adjusted to better match AES-NI: $\Sigma\ \alpha_i\ M_i\ K\ 1^i$

Additions: no carry out of last 32 bits

Phillip Rogaway
University of California, Davis, USA

With thanks to the organizers for their kind invitation to join.

CTCrypt 2018

May 28, 2018
Suzdal, Russia

Today: an **historical** and largely **personal** account of the development of **authenticated encryption** (AE)

Theme:

The importance of **definitions**

Traditional view of shared-key cryptography
(until ~2000)

K
Sender
K
Receiver

Privacy
(confidentiality)

Authenticity
(data-origin authentication)

Encryption scheme

Authenticated Encryption (AE)
Achieve both of these aims

Message Authentication Code (MAC)

IND-CPA
[Bellare, Desai, Jokipii, R 1997]
following [Goldwasser, Micali 1982]

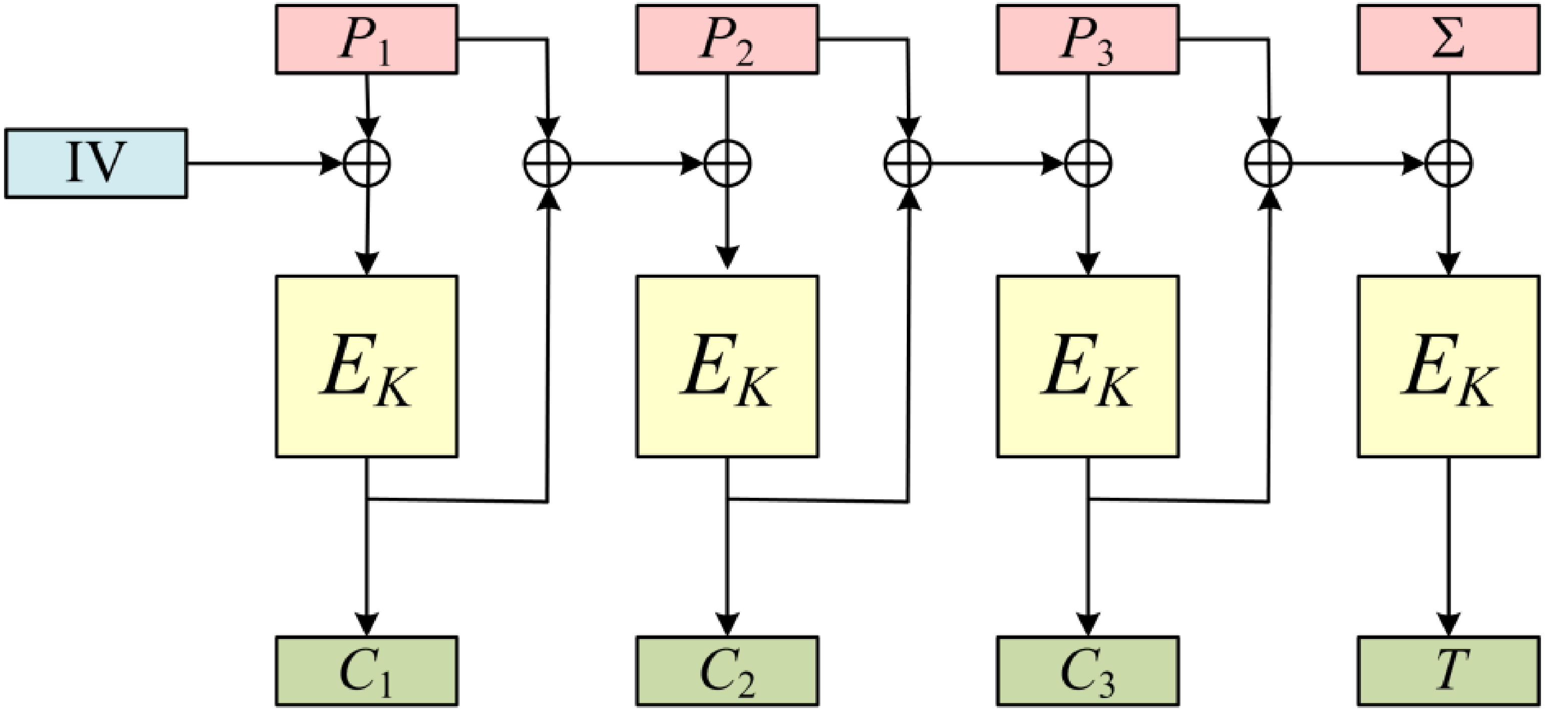
Existential-unforgeability under ACMA
[Bellare, Kilian, R 1994], [Bellare, Guerin, R 1995]
following [Goldwasser, Micali, Rivest 1984/1988]

AE is a folklore aim

Eg: Kerberos' attempt

PCBC

≤ 1982



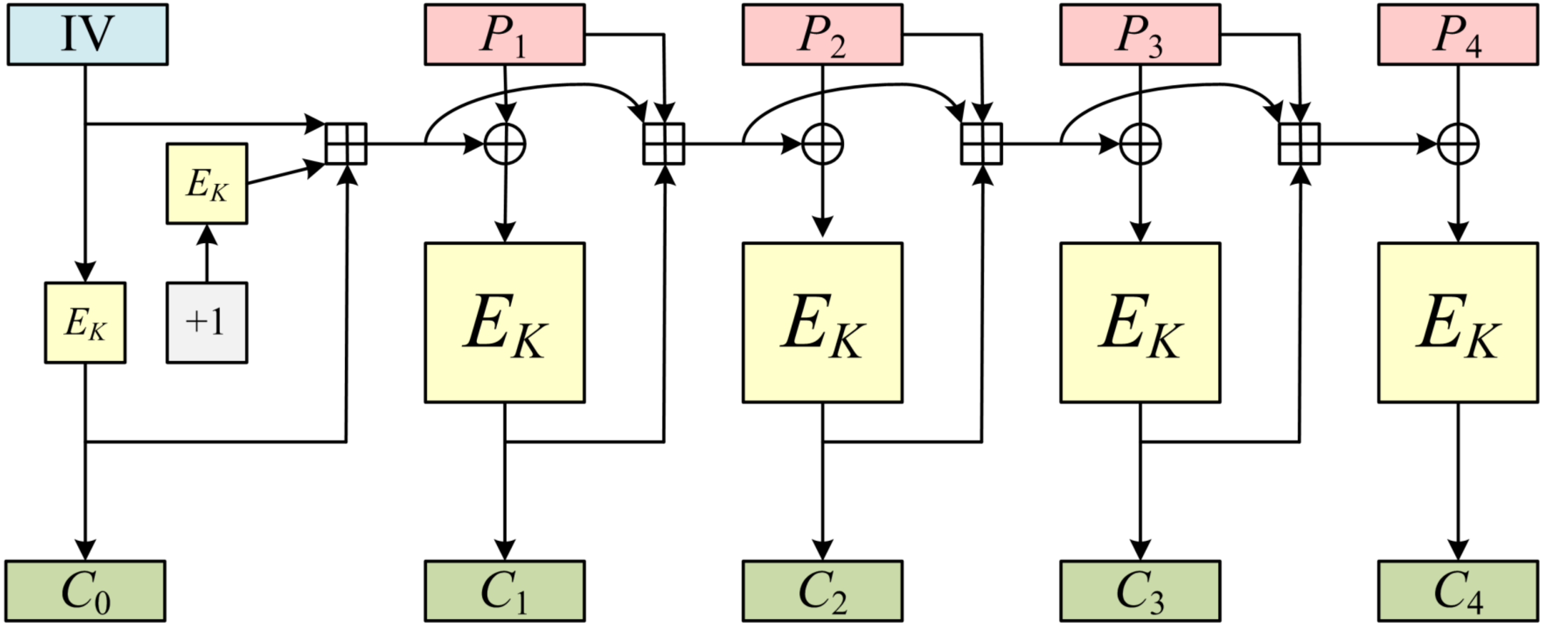
Doesn't work

See **[Yu, Hartman, Raeburn 2004]**
The Perils of Unauthenticated Encryption: Kerberos Version 4
for real-world attacks

Ad hoc mechanisms have routinely **failed**

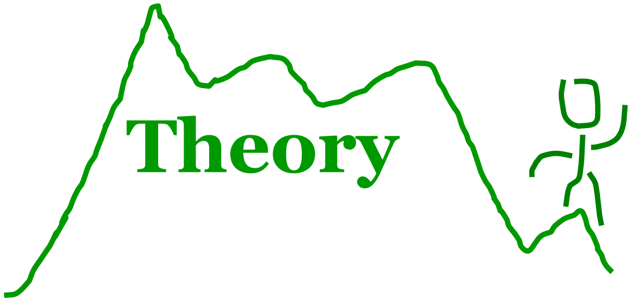
iaPCBC

[Gligor, Donescu 1999]



Doesn't work

Promptly broken by Jutla (1999)
& Ferguson, Whiting, Kelsey, Wagner (1999)



Theory

Practice

By 2000

There was a huge **gap** in how **theory people** and **practical people** viewed sym enc.

Had mostly **ignored** symmetric crypto

and had **no interest** in anything so pedestrian as sym enc or MACs

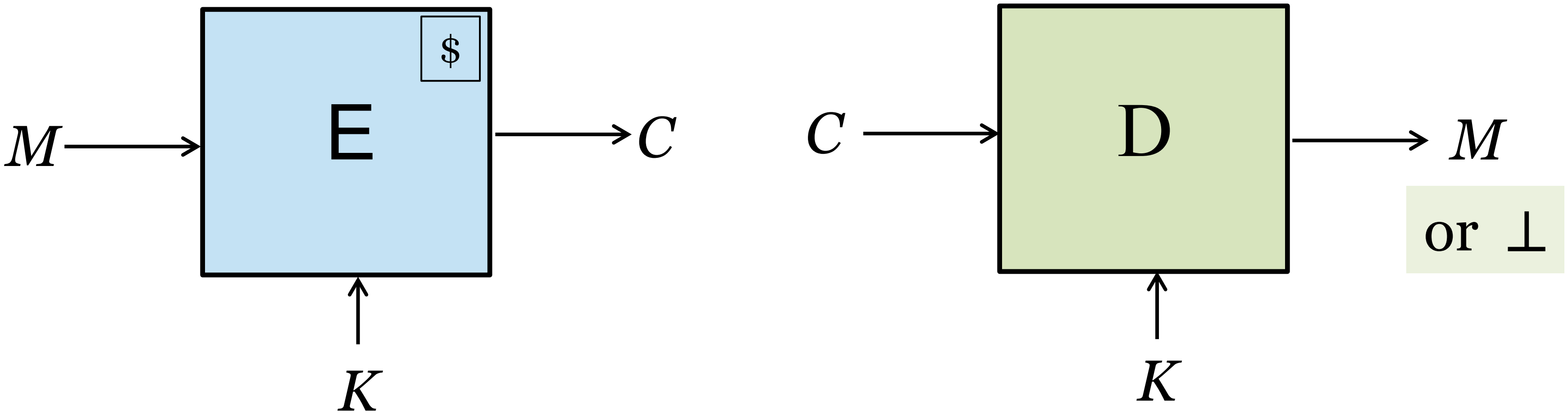
Had **assumed** they'd get authenticity **and** privacy from one tool: encryption

and were now coming to realize that methods in use, and proposed, **didn't do this**

Notion Emerged in 2000

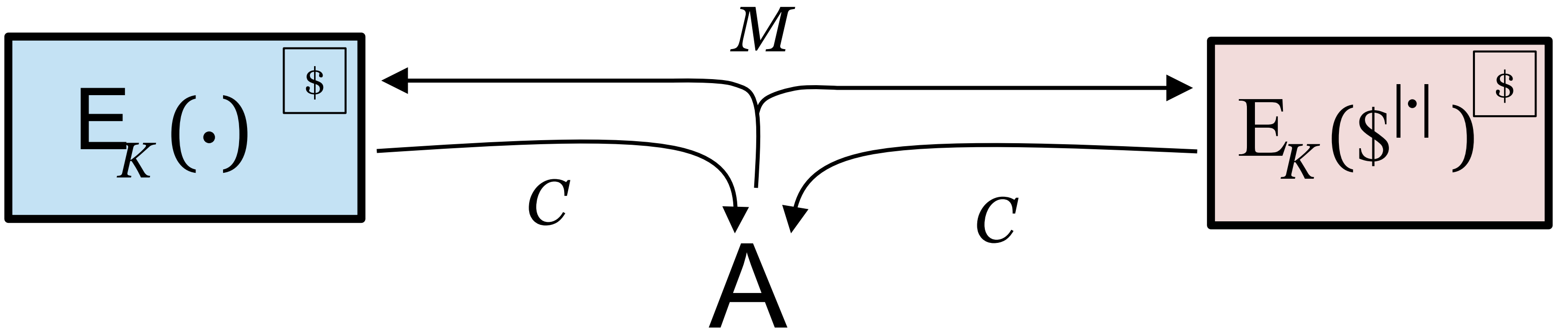
pAE – Probabilistic AE

[Bellare, Rogaway 2000]
[Katz, Yung 2000]
Following
[Bellare, Desai, Jokipii, Rogaway 1997]



pAE – Probabilistic AE

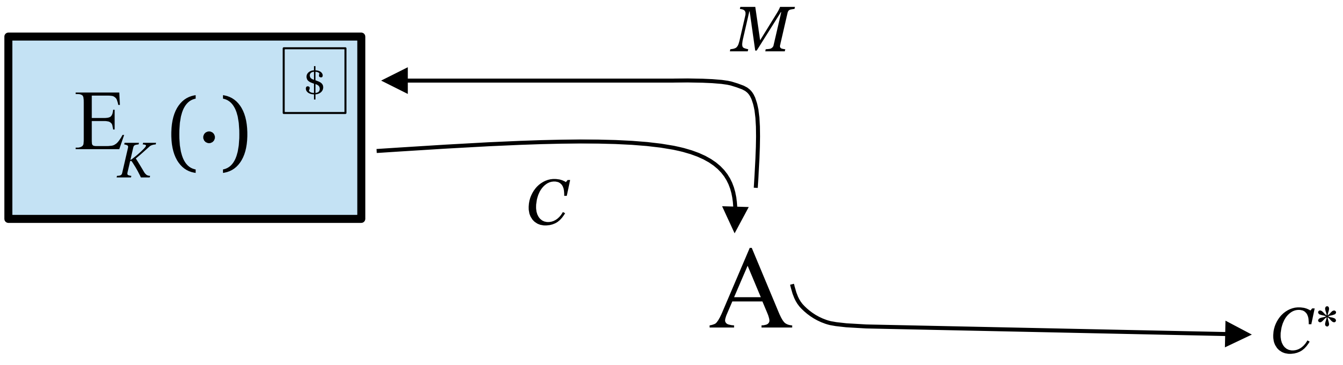
[Bellare, Rogaway 2000]
[Katz, Yung 2000]



$$\mathbf{Adv}_{E}^{\text{priv}}(A) = \Pr[A^{E_K(\cdot)} \rightarrow 1] - \Pr[A^{E_K(\$^{|\cdot|})} \rightarrow 1]$$

pAE – Probabilistic AE

[Bellare, Rogaway 2000]
[Katz, Yung 2000]



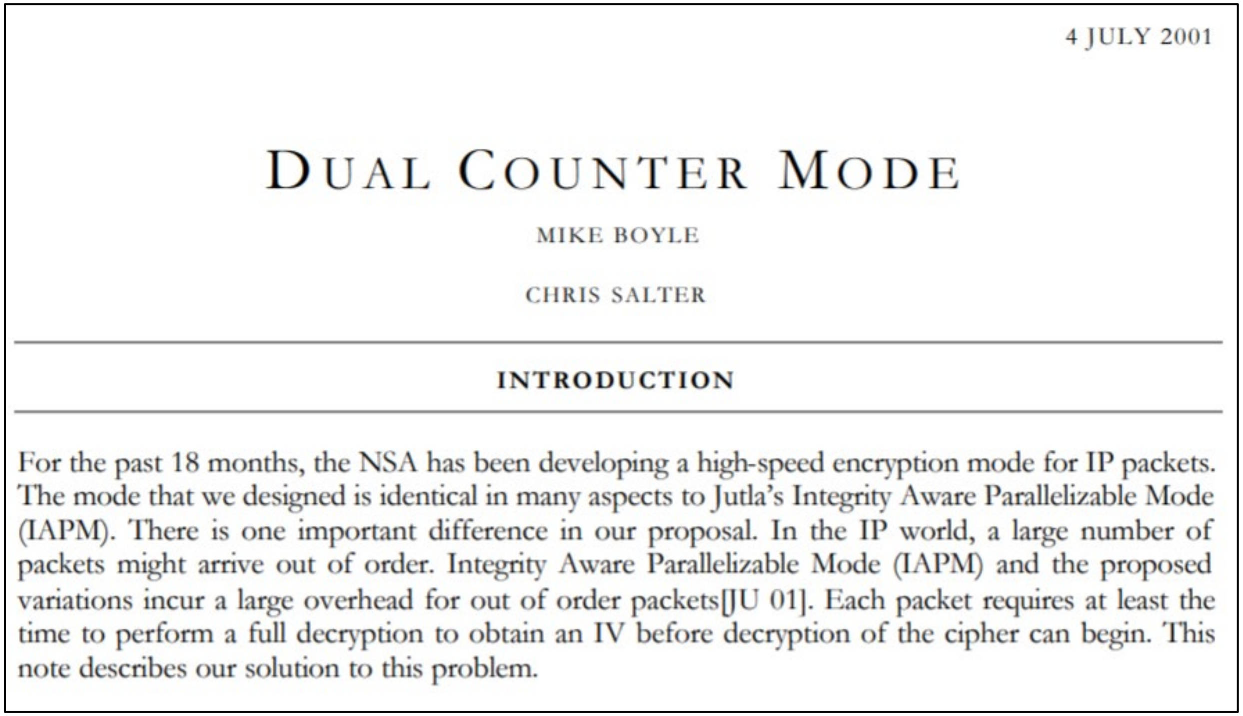
$$\mathbf{Adv}_{\mathrm{E}}^{\mathrm{priv}}(\mathrm{A}) = \Pr[\mathrm{A}^{\mathrm{E}_K(\cdot)} \rightarrow 1] \; - \; \Pr[A^{\mathrm{E}_K(\$^{|\cdot|})} \rightarrow 1]$$

$$\mathbf{Adv}_{\mathrm{E}}^{\mathrm{auth}}(\mathrm{A}) = \Pr[\mathrm{A}^{\mathrm{E}_K(\cdot)} \underbrace{\rightarrow C^*\text{: no query returned } C^* \text{ and } \mathrm{D}_K(C^*) \neq \perp}_{\text{“A forges”}}]$$

Practice-oriented provable-security
(Bellare, Rogaway ~1993-2000)
One part of this: *A security definition* ***is*** *an association of a real number* $\mathbf{Adv}_{\Pi}(\mathrm{A})$ *to any adversary* A *and scheme* $\Pi \in C$

In praise of definitions

1. Enables **proofs**
2. Enables precise **thinking** and **discourse**
3. Let's you see **attacks** (eg: NSA's Dual Counter Mode)
4. Can enhance **efficiency**



4 JULY 2001

DUAL COUNTER MODE

MIKE BOYLE

CHRIS SALTER

INTRODUCTION

For the past 18 months, the NSA has been developing a high-speed encryption mode for IP packets. The mode that we designed is identical in many aspects to Jutla's Integrity Aware Parallelizable Mode (IAPM). There is one important difference in our proposal. In the IP world, a large number of packets might arrive out of order. Integrity Aware Parallelizable Mode (IAPM) and the proposed variations incur a large overhead for out of order packets[JU 01]. Each packet requires at least the time to perform a full decryption to obtain an IV before decryption of the cipher can begin. This note describes our solution to this problem.

AE quickly became real

Urgent need

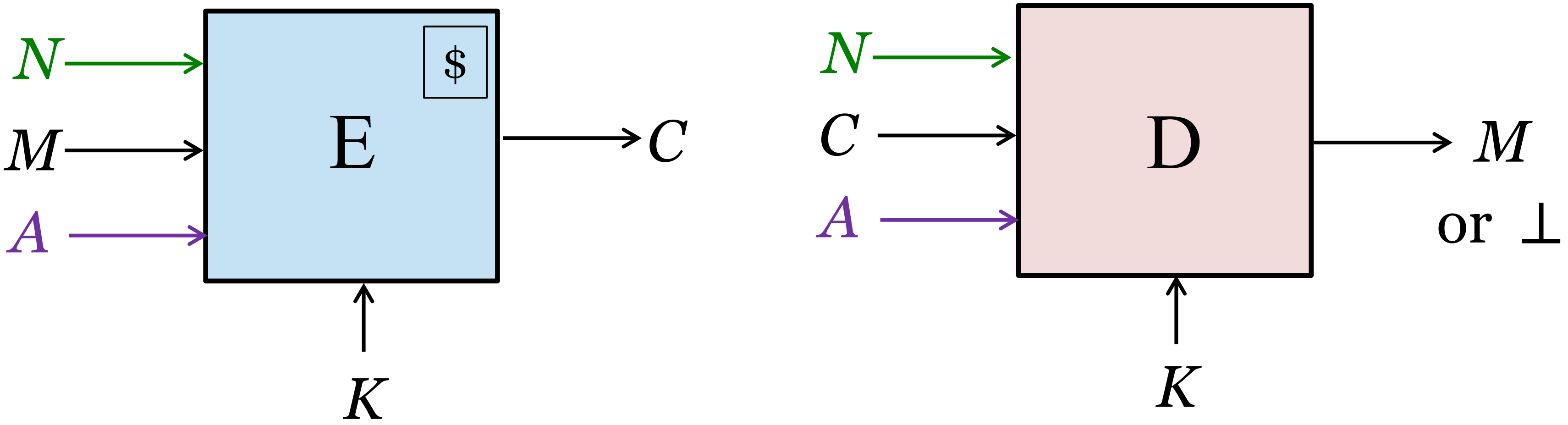
- **802.11** standard ratified in 1999
  Uses **WEP** security – RC4 with a CRC-32 checksum for integrity

- **Fatal attacks** soon emerge:
  - [Fluhrer, Mantin, Shamir 2001]
    Weaknesses in the key scheduling algorithm of RC4
  - [Stubblefield, Ioannidis, Rubin 2001]
    Using the Fluhrer, Mantin, Shamir attack to break WEP
  - [Borisov, Goldberg, Wagner 2001]
    Intercepting mobile communications: the insecurity of 802.11
  - [Cam-Winget, Housley, Wagner, Walker 2003]
    Security flaws in 802.11 data links protocols

- **WEP → WPA** (uses **TKIP**) → **WPA2** (uses **CCM**)
  - Draft solutions based on **OCB**
  - Politics +patent-avoidance:
    CCM developed **[Whiting, Housley, Ferguson 2002]**
  - Standardized in **IEEE 802.11** [2004] , **NIST 800-38C** [2004]

To make it real
the definitions needed work

[Rogaway 2002]



1) Move the coins out of E — make it deterministic **[RBBK01]**

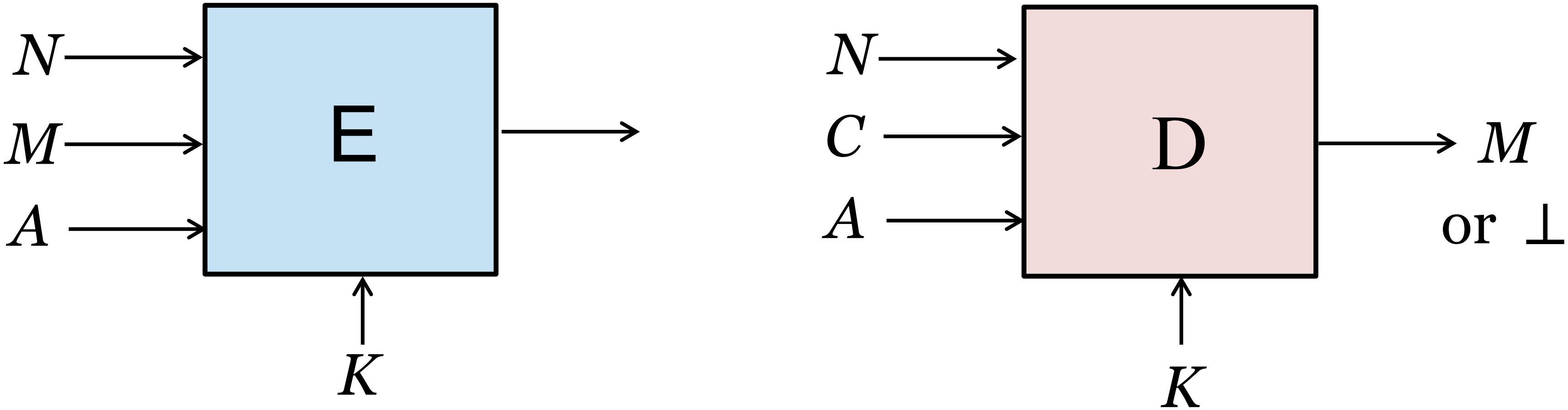
To improve resistance to random-number generation problems
To architect to existing abstraction boundaries

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

To authenticate headers
Jesse Walker, Nancy Cam-Winget, Burt Kaliski
all "requested" this functionality for their
standardization-related work

Formalizing the Syntax

For AEAD



One approach: An AEAD scheme is a function

E: K × N × A × M → {0,1}* where

- K is a finite set.

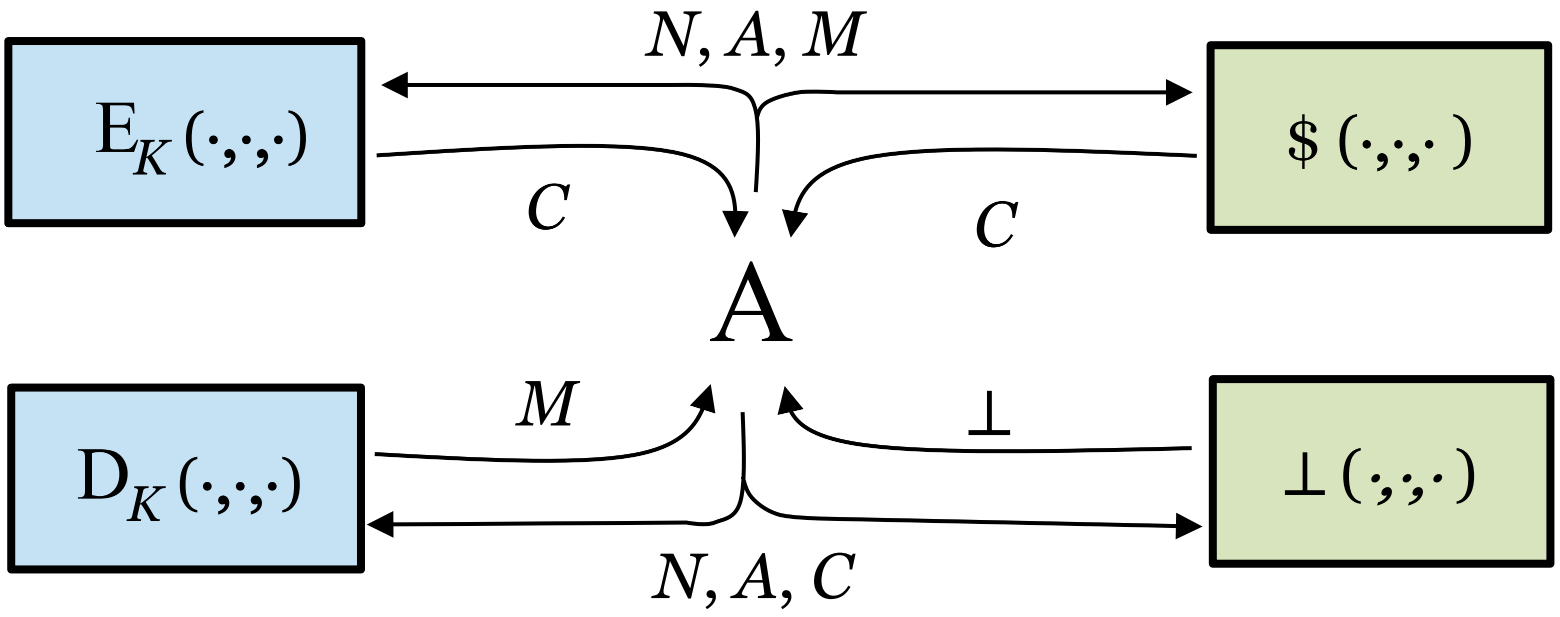
  N, A, M are nonempty sets of strings

  M contains a string x iff it contains all strings of length $|x|$
- Each **E**$(K, N, A, \cdot)$ is an injection
- For some λ, |**E**(K, N, A, M) | = $|M| + \lambda$

Under this approach, the desired functionality of D is determined by E:
D$(K, N, A, C)=M$ if E$(K, N, A, M)=C$ for some M; else D$(K, N, A, C) = \perp$

AEAD (or simply AE)

[Rogaway, Shrimpton 2006]
[Rogaway 2002], [RBBK00]



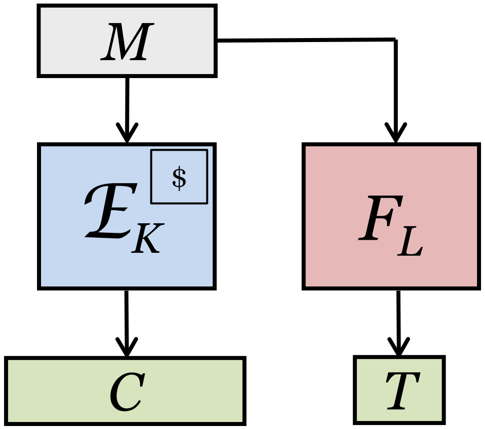
$$\mathbf{Adv}^{\text{aead}}_{\text{E}}(\text{A}) = \Pr[\text{A}^{E_K,\, D_K} \to 1] \;-\; \Pr[\text{A}^{\$,\, \perp} \to 1]$$

A may not:

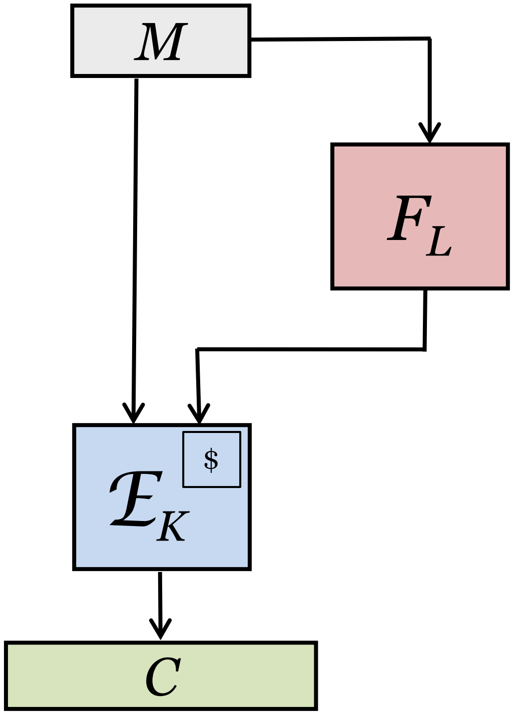
- Repeat an *N* in an enc query
- Ask a dec query (*N*, *A*, *C*) after *C* is returned by an (*N*, *A*, ·) enc query

Generic composition

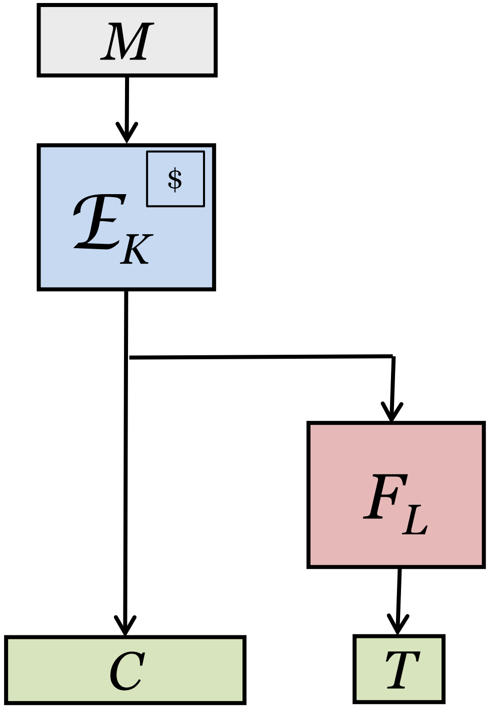
[Bellare, Namprempre 2000]



Encrypt-and-MAC ✗



MAC-then-Encrypt ✗



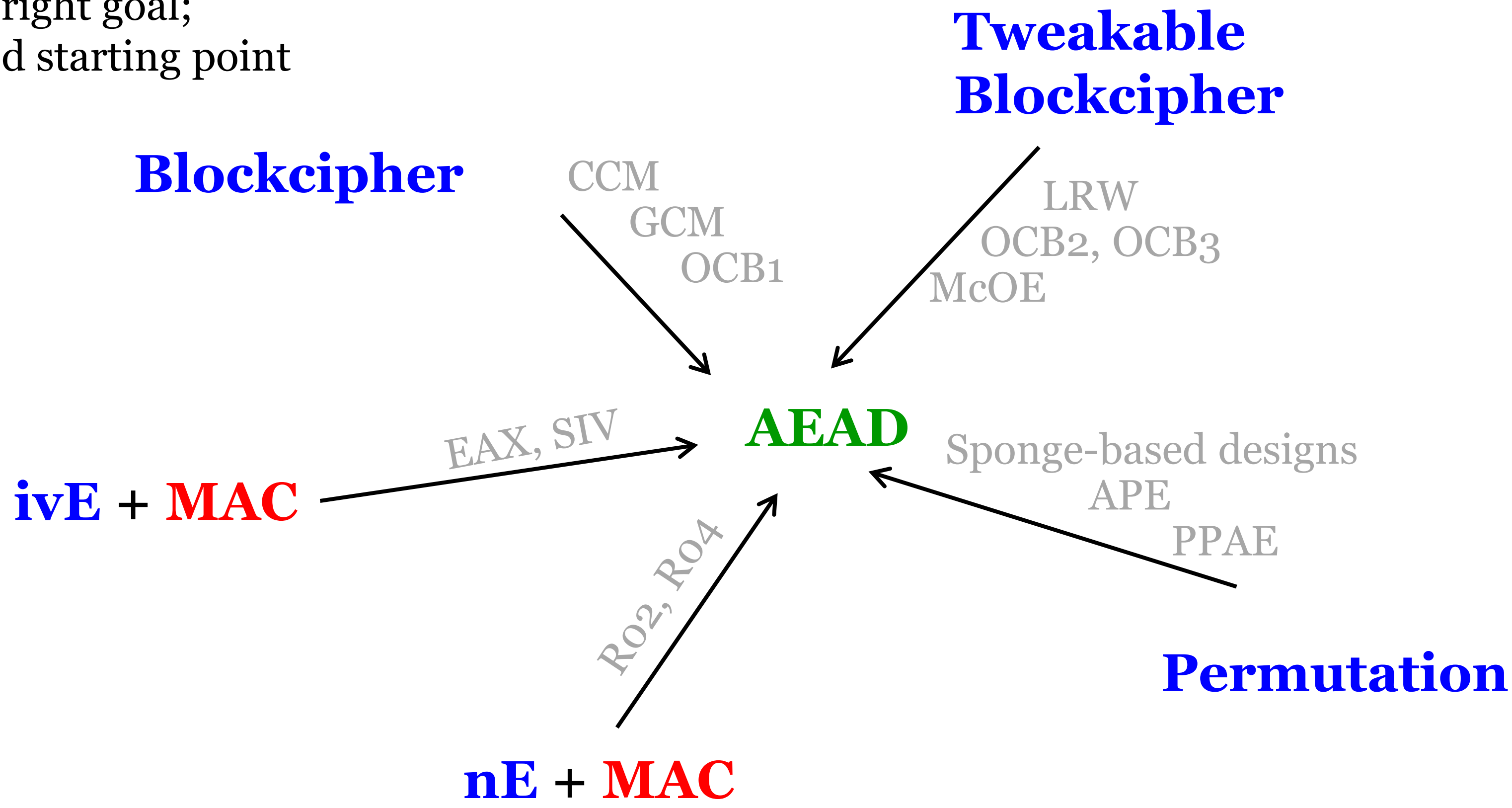
✓ **Encrypt-then-MAC**

BN studied: pE + MAC → pAE

Not understanding this made Mechanism 5 of ISO/IEC 19772: 2009 wrong

Modern perspective:

pAE isn’t the right goal;
pE isn’t a good starting point



Tweakable Blockcipher

Blockcipher

CCM
GCM
OCB1

LRW
OCB2, OCB3
McOE

AEAD

EAX, SIV

ivE + MAC

Sponge-based designs
APE
PPAE

RO2, RO4

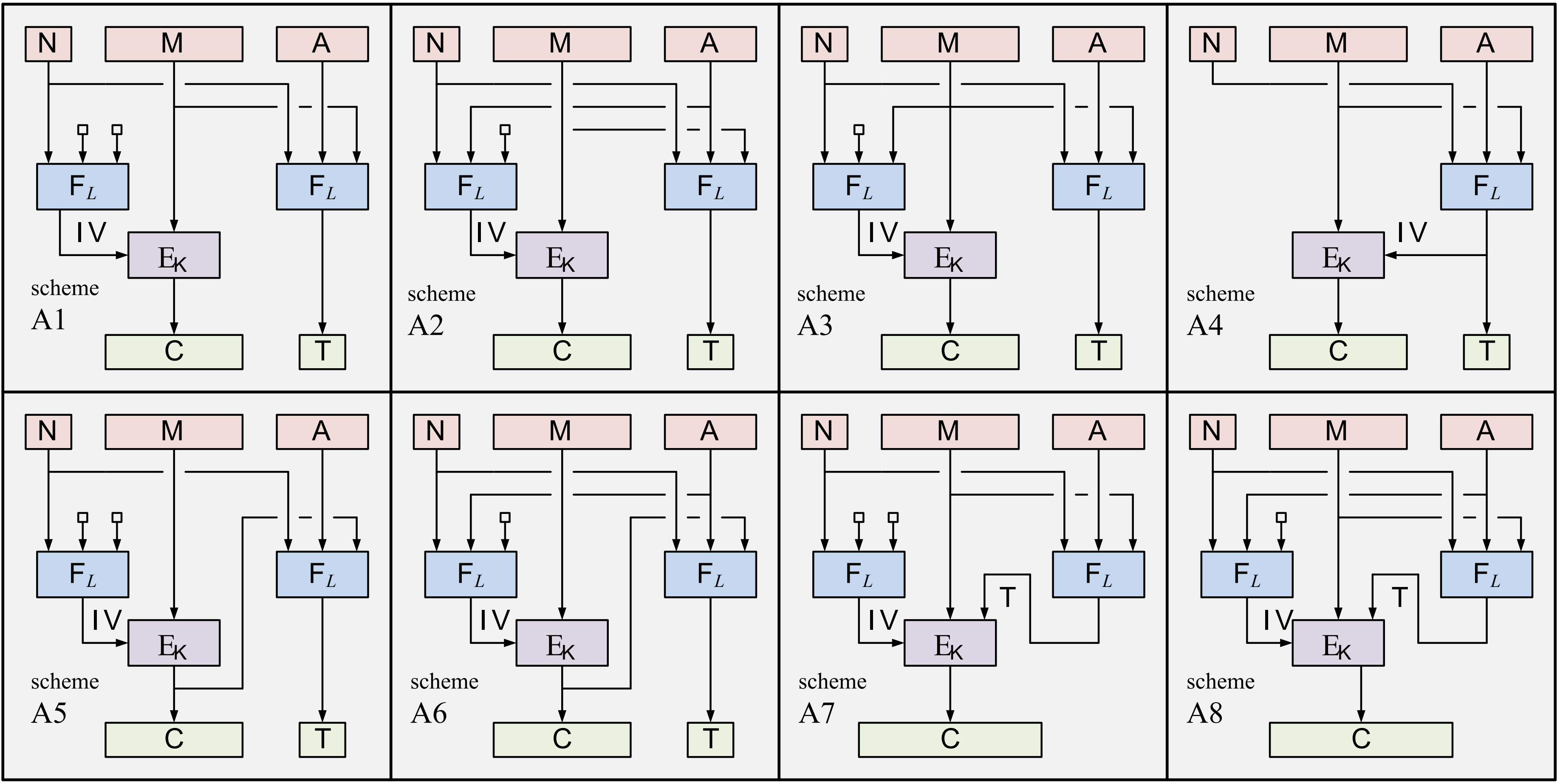
Permutation

nE + MAC

Eight "favored" schemes (of 160)

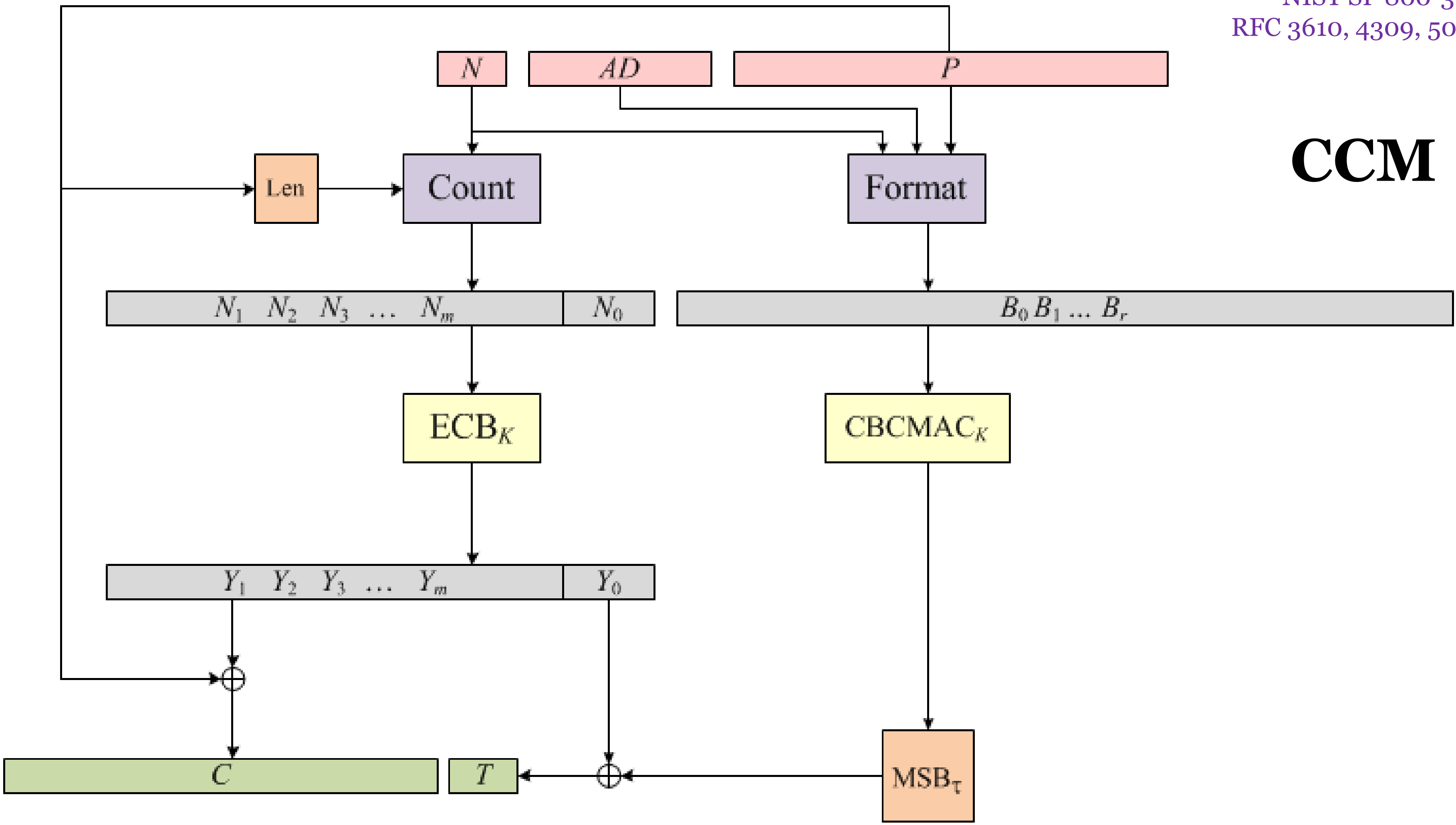
for ivE + MAC → nAE

[Namprempre, Rogaway, Shrimpton 2014]



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

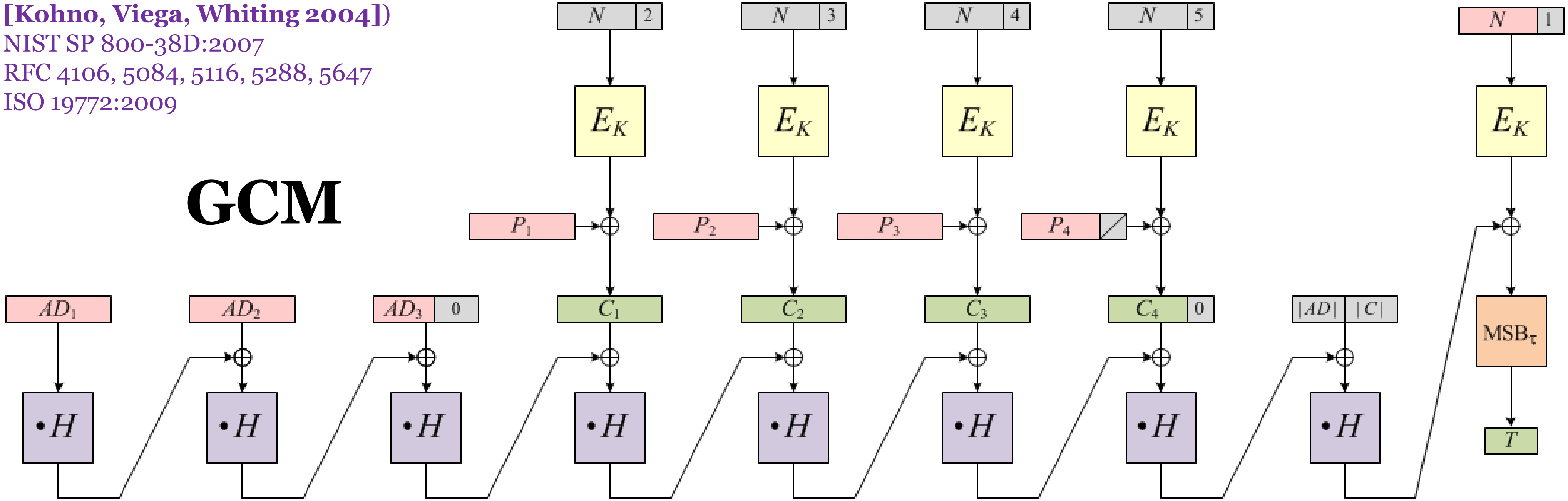
CCM



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

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

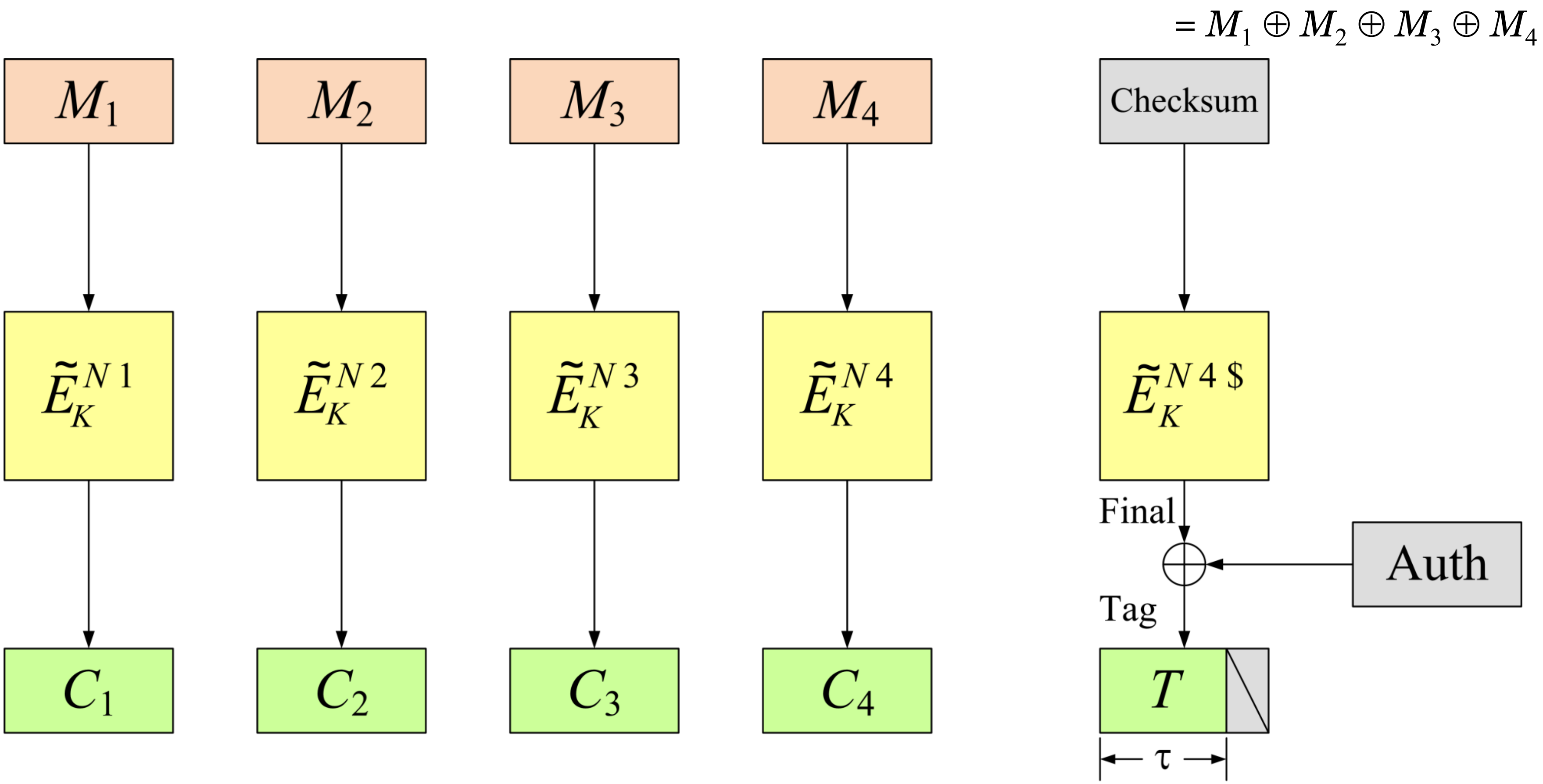
GCM



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

[Krovetz Rogaway 2011] , following
[RBBK01,LRW02,R04]
RFC 7253 ISO 19772

OCB



Thm: OCB is provably secure (up to the birthday bound) if E is a strong-PRP.

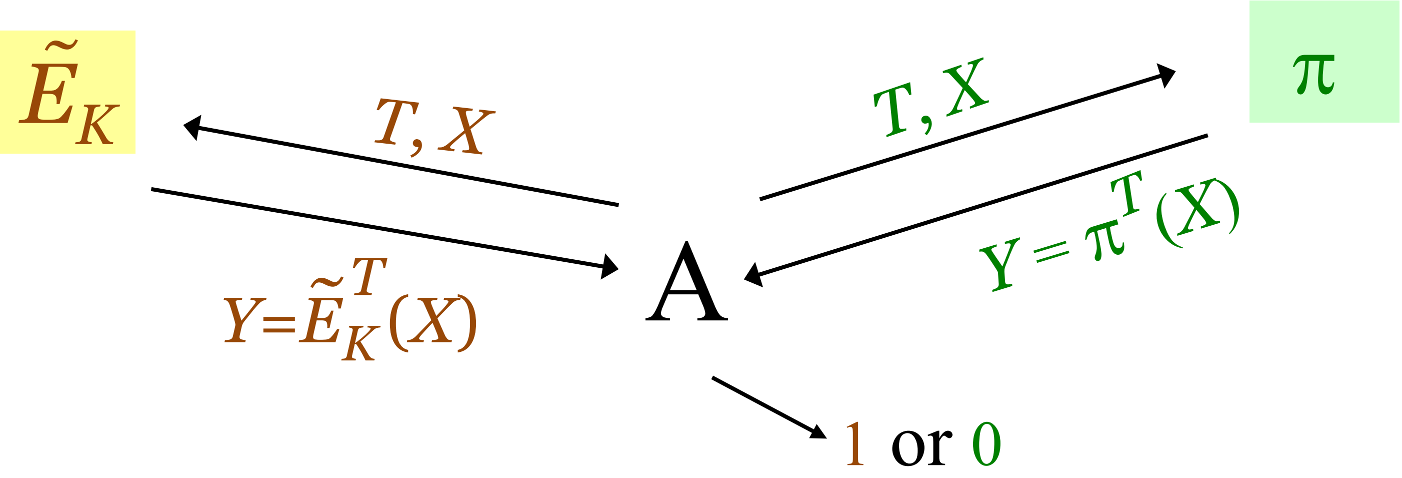
[Liskov, Rivest, Wagner 2002]

Tweakable Blockcipher (TBC)

$\tilde{E}$: K × T × $\{0,1\}^n \rightarrow \{0,1\}^n$

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

A T-indexed family of random permutations on n bits



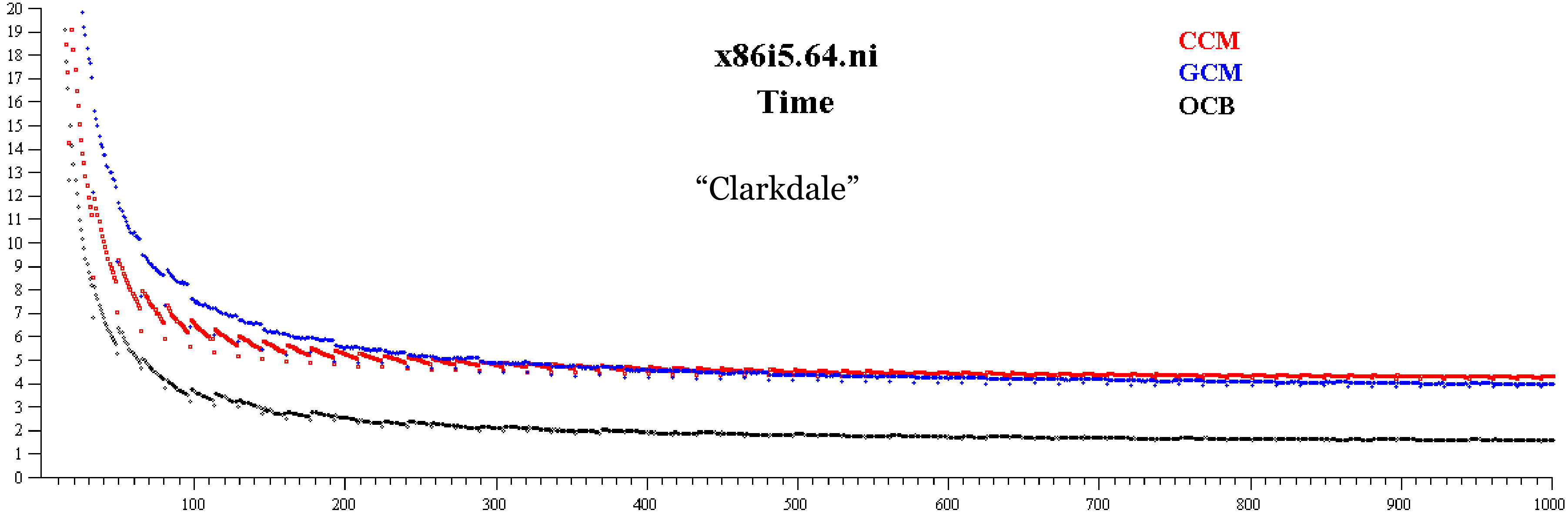
$$\mathbf{Adv}^{\mathrm{prp}}_{\tilde{E}}(\mathrm{A}) = \Pr[\mathrm{A}^{\tilde{E}_K} \Rightarrow 1] - \Pr[\mathrm{A}^{\pi} \Rightarrow 1]$$

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

[Krovetz Rogaway 2011] , following
[RBBK01,LRW02,R04]
RFC 7253   ISO 19772

OCB

On modern Intel processors, OCB runs at approximately the same rate as ECB: ~0.63 cpb



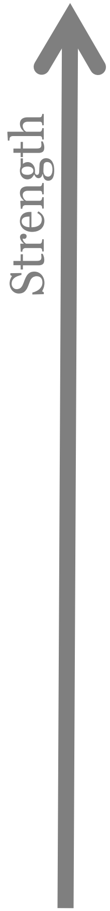
Robust AE (RAE)

Misuse-Resistant AE (MRAE)

Nonce-based AEAD (AE)

Probabilistic AE (pAE)

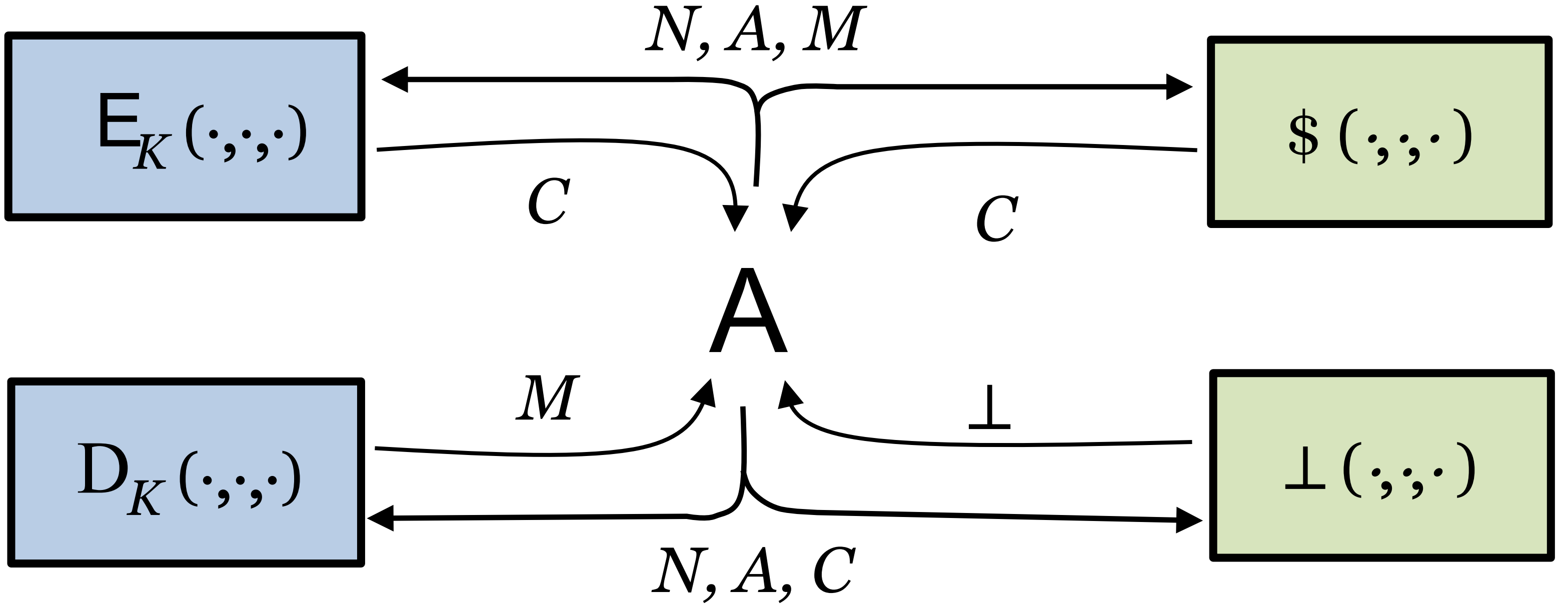
Probabilistic encryption (pENC)



MRAE

[Rogaway, Shrimpton 2006]

(nonce-reused) misuse-resistant AE



1. **Nonce-reuse security**: A repeated N **shouldn't** be cataclysmic
2. **Novelty exploitation**: Uniqueness of (N, A, M) **should** suffice

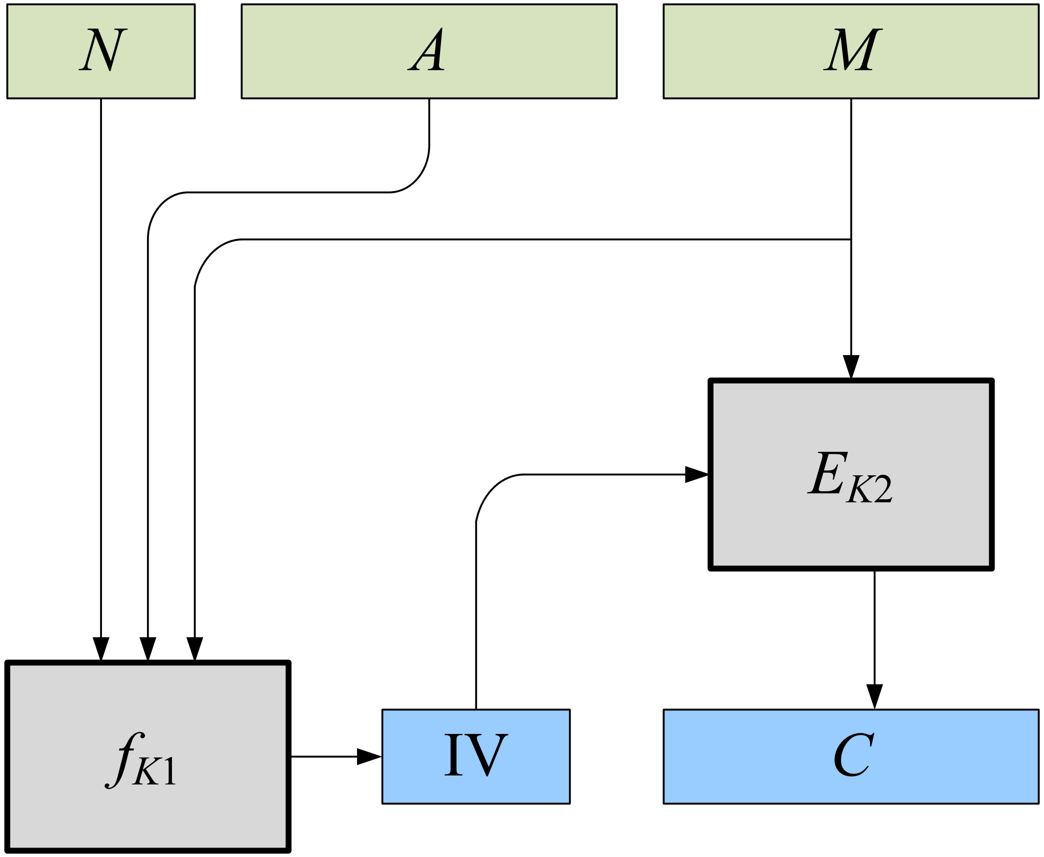
A may not ask queries that would trivially result in a win. It may not:

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

MRAE

[Rogaway, Shrimpton 2006]

SIV



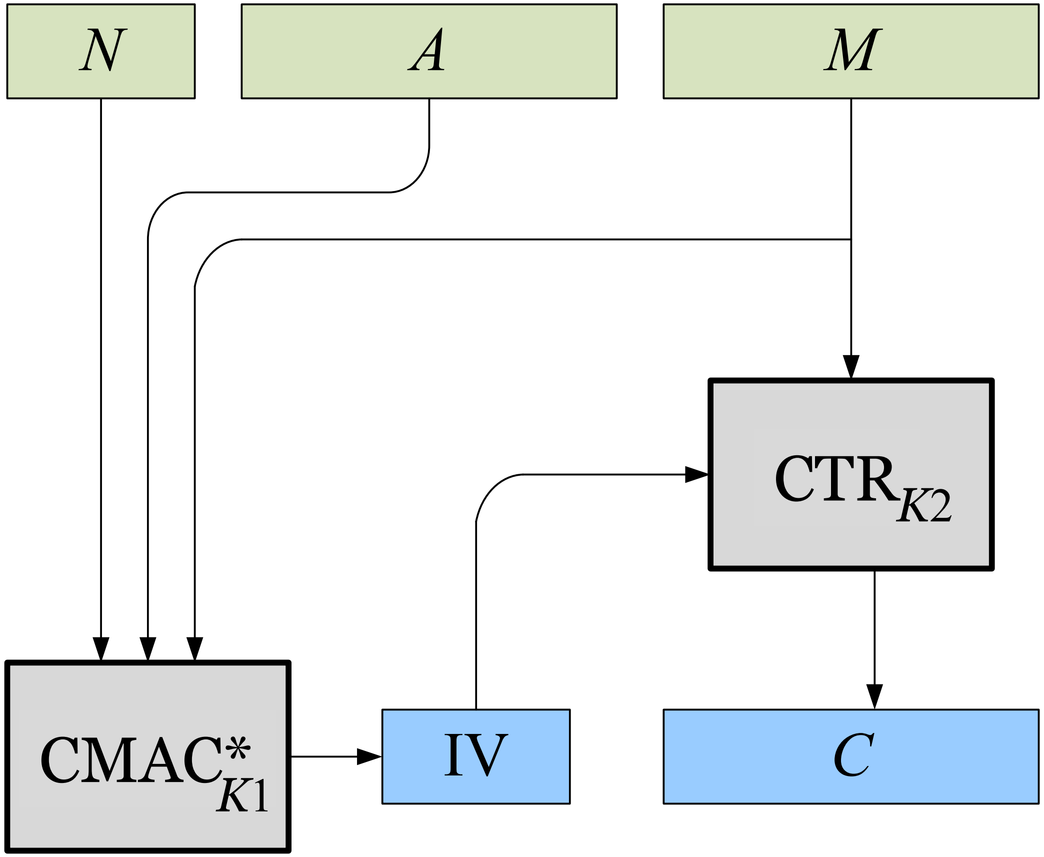
ivE encryption scheme (eg, CTR), secure

PRF operating on a **vector** of strings

MRAE

[Rogaway, Shrimpton 2006]

SIV

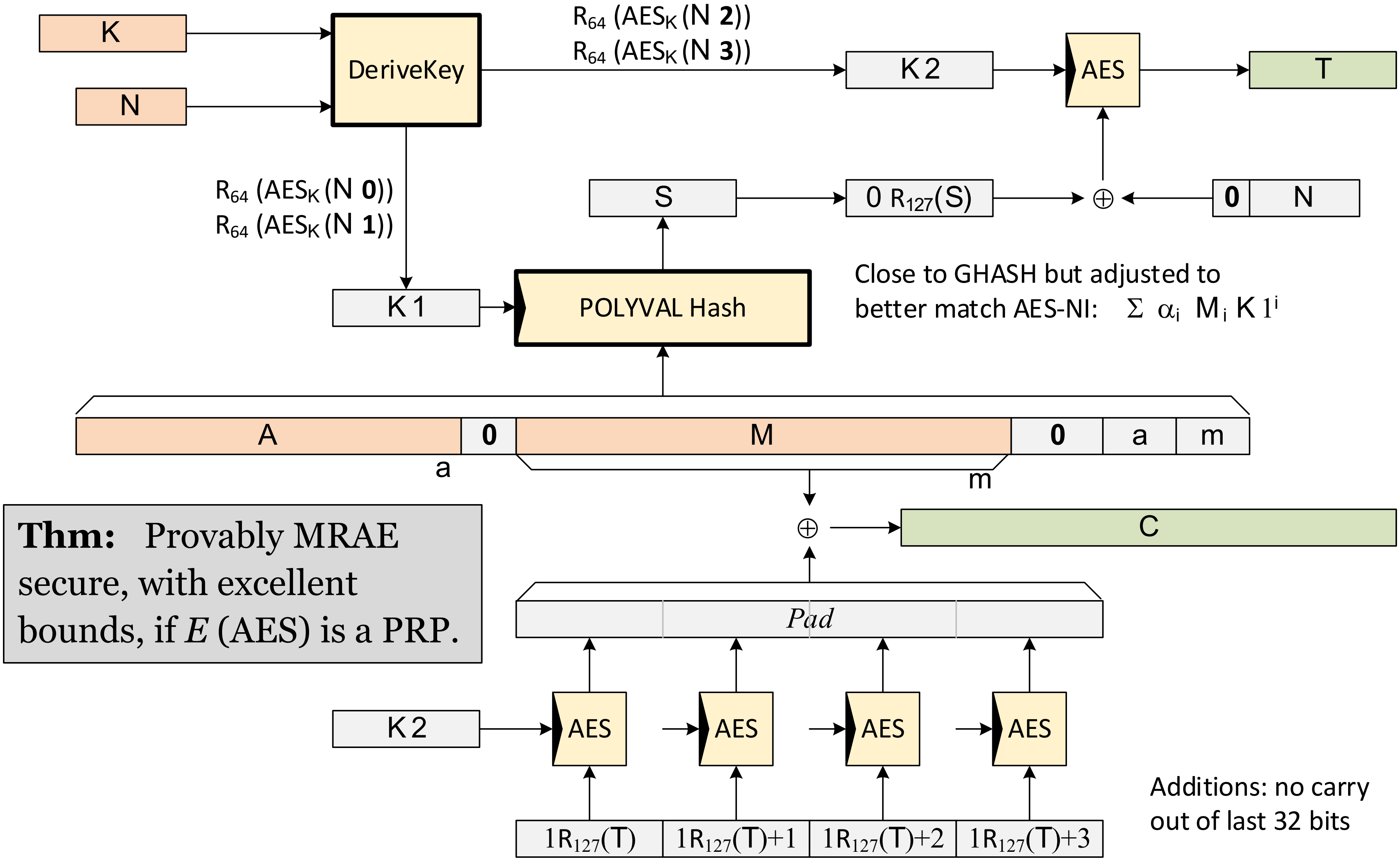


ivE encryption scheme (eg, CTR), secure

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

Thm: Provably MRAE secure, with excellent bounds, if *E* (AES) is a PRP.

CAESAR competition

ACORN for use case 1	Hongjun Wu
AEGIS for use case 2	Hongjun Wu, Bart Preneel
Ascon for use case 1	Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer
COLM for use case 3	Elena Andreeva, Andrey Bogdanov, Nilanjan Datta, Atul Luykx, Bart Mennink, Mridul Nandi, Elmar Tischhauser, Kan Yasuda
Deoxys-II for use case 3	Jérémy Jean, Ivica Nikolić, Thomas Peyrin, Yannick Seurin
MORUS for use case 2	Hongjun Wu, Tao Huang
OCB for use case 2	Ted Krovetz, Phillip Rogaway

57 round-1
(Mar 2014)

29 round-2
(Mar 2014)

16 round-3
(Aug 2016)

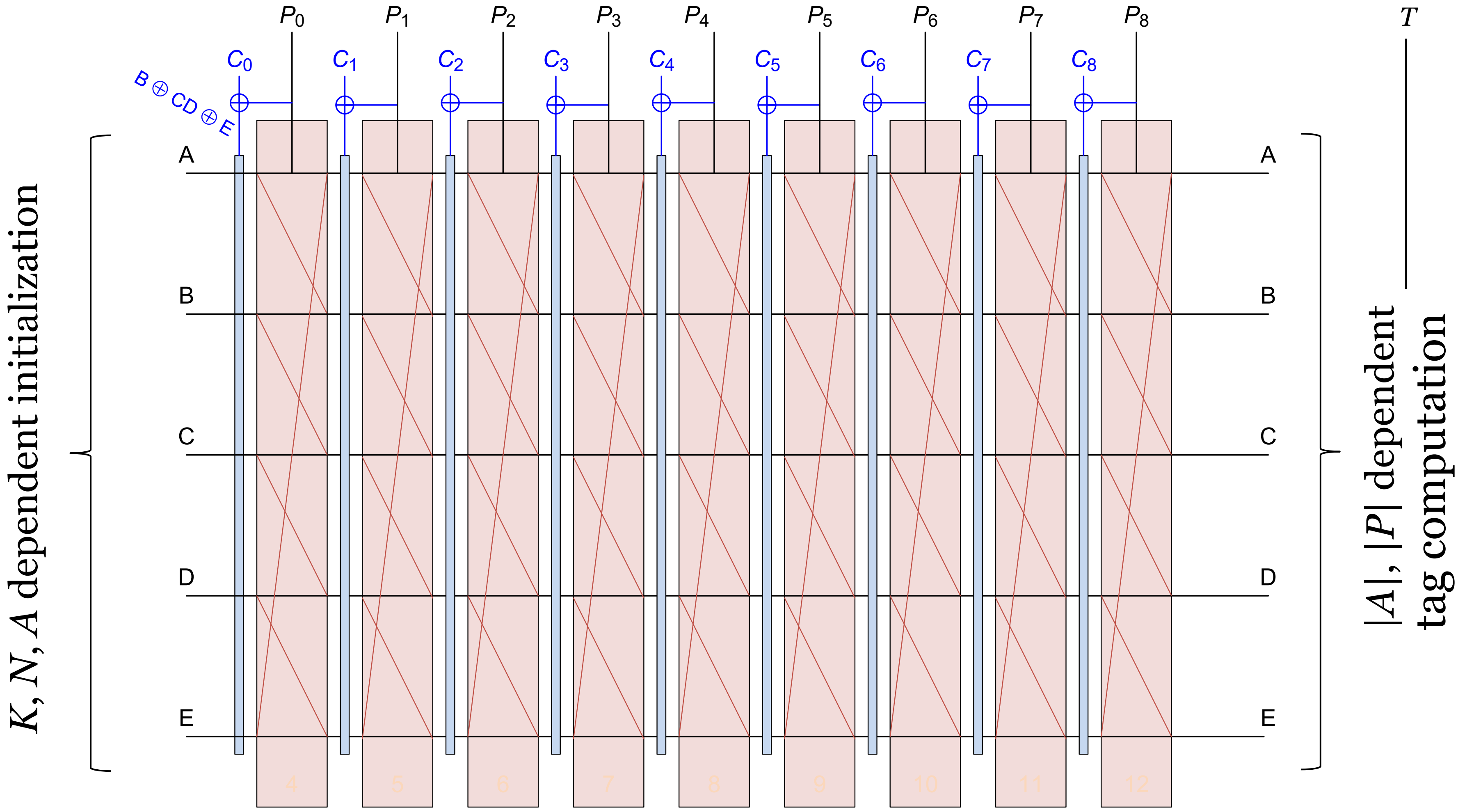
7 finalists
(Mar 2018)

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

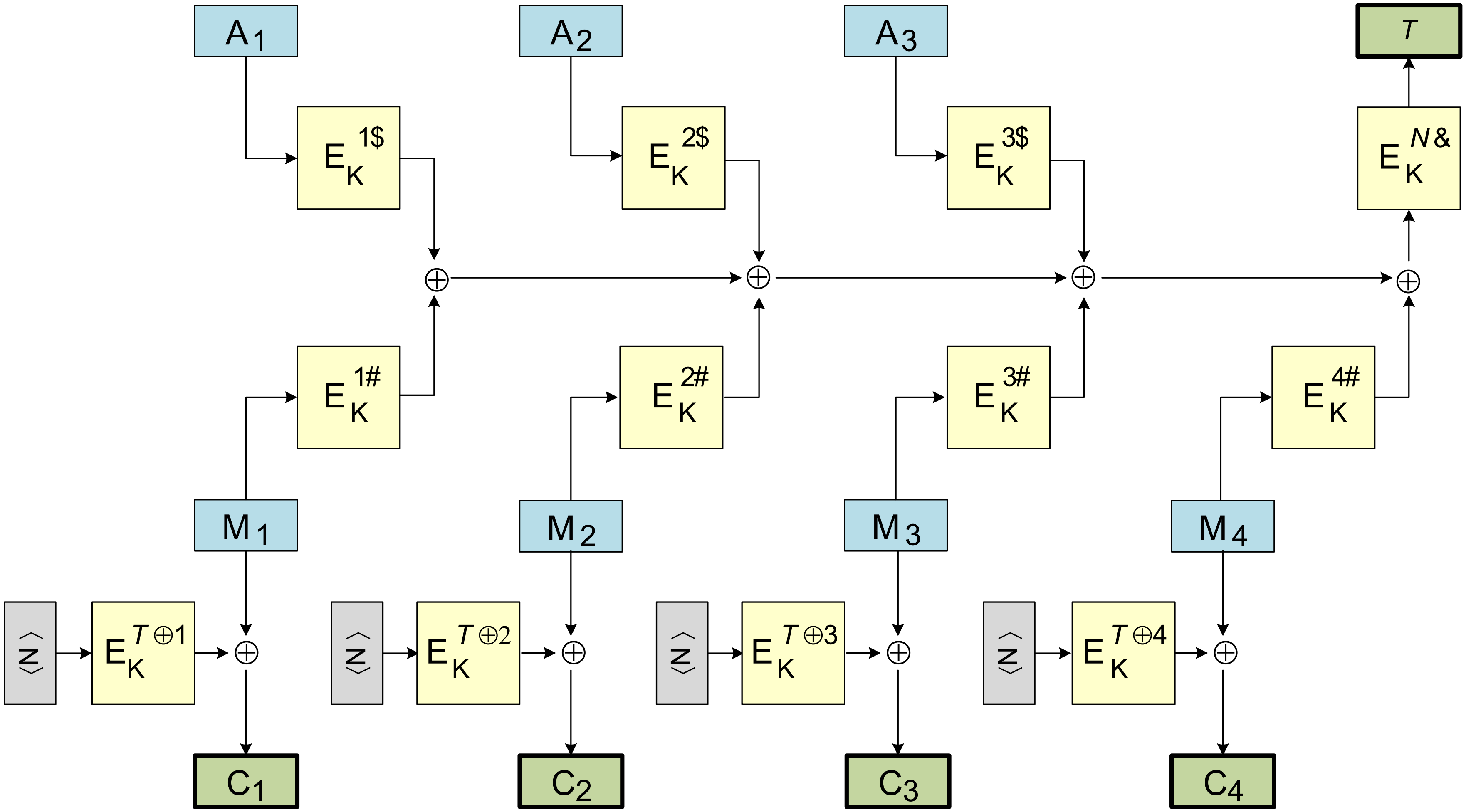
$|A|, |P|$ dependent
tag computation

~~Thm~~: No proofs

Deoxys-II

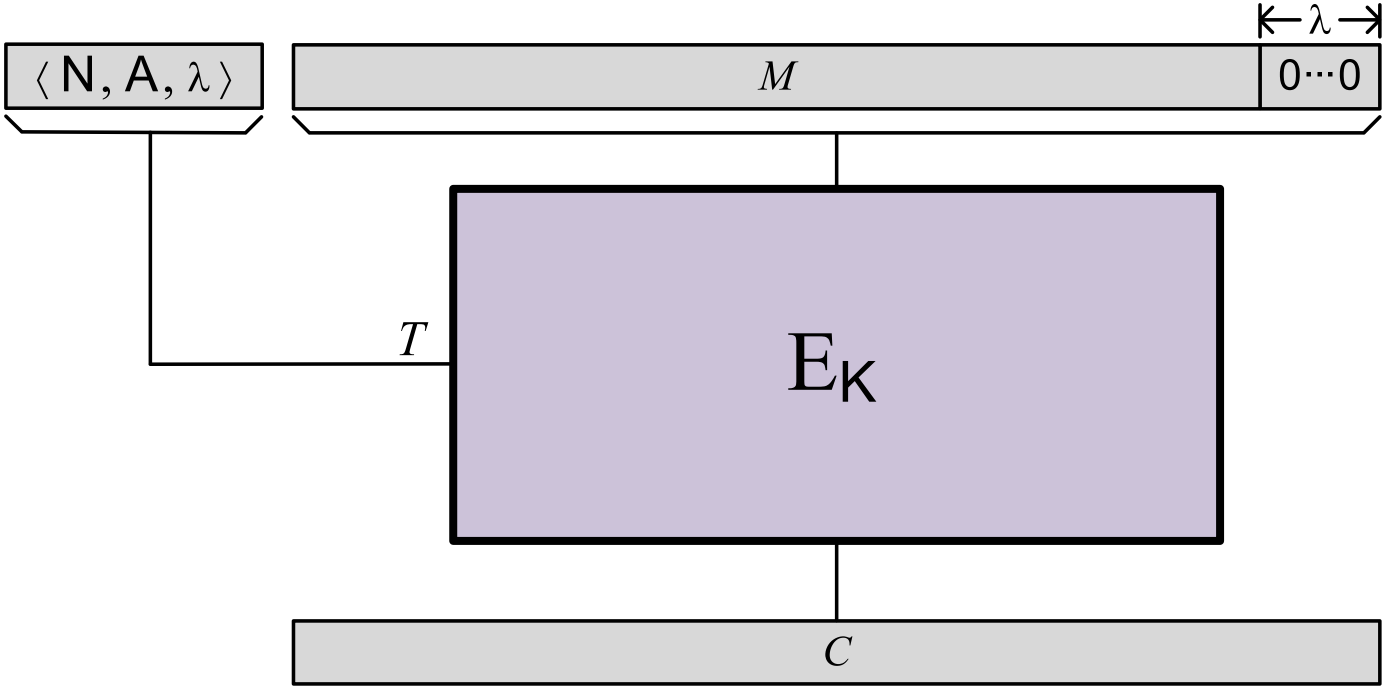
Jean, Nikolić,
Peyrin, Seurin

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



AEZ encrypts by enciphering

[Hoang, Krovetz, Rogaway 2014]
following **[Bellare, Rogaway 2000]**
[Shrimpton, Terashima 2013]



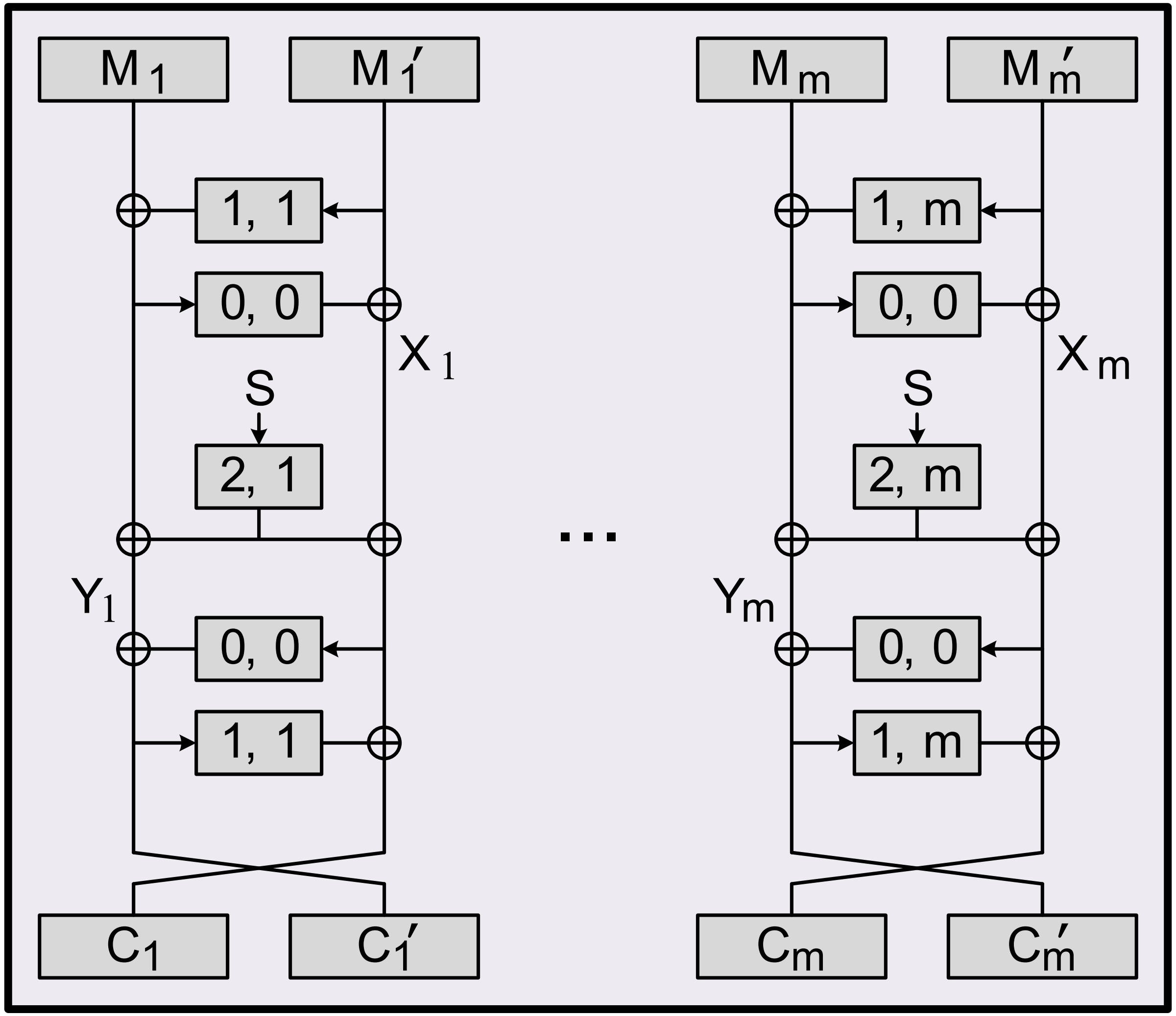
$|K|, |N|, |A|, |M|, \lambda$
arbitrary

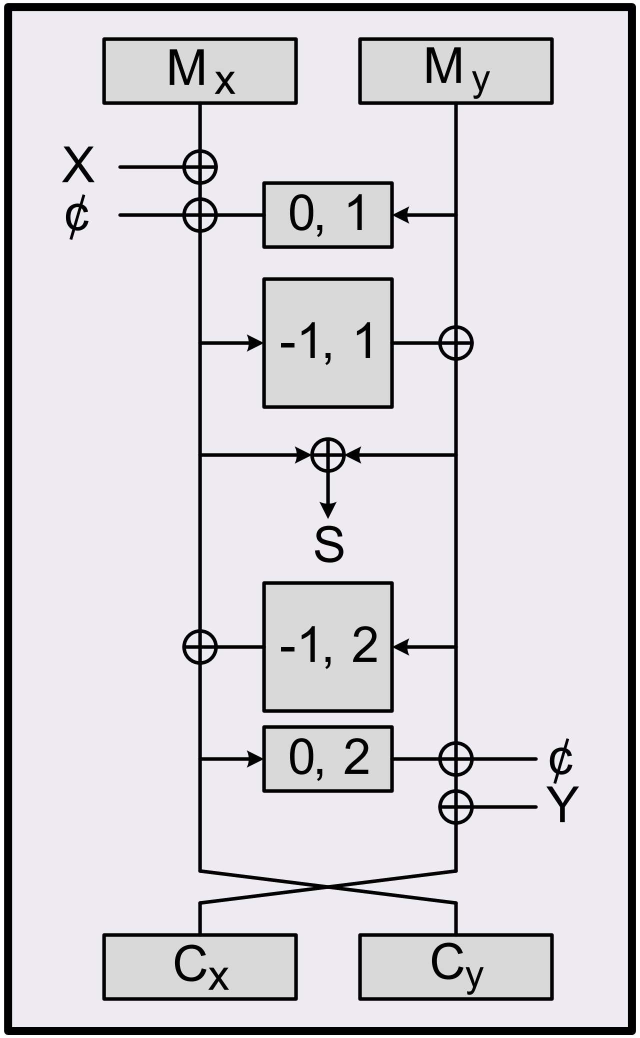
RAE: Approximate a random λ -increasing PRI

[Hoang, Krovetz, Rogaway 2014]

AEZ-core

Messages with an **even** number of blocks, all of them **full**





Conclusions

Sym enc that is insecure, untrusted, easy to misuse, or underused

→

Sym enc that is secure, trusted, easy to correctly use, and ubiquitous

Definitions **aren’t a goal in themselves**. They are a **key component** for transforming theory **and** practice. You **also** need good

- Schemes
- Proofs
- Standards
- Implementations
- Systems (physical, institutional, organizational)

The Rise of Authenticated Encryption

Abstract. To many theory-oriented cryptographers, symmetric encryption is among our most passé of problems. Yet from the point of view of providing a useful theory and desirable schemes, the area is very much alive. For this talk I'll explore the long dialectic that has taken us from semantic security to robust authenticated-encryption. I'll trace the history of AE, explaining why it emerged, how it has evolved, and what some modern AE schemes now look like.