Online Authenticated Encryption

Reza Reyhanitabar

EPFL
Switzerland

ASK 2015
30 Sept - 3 Oct
Singapore

Agenda

I. The Emergence of Online-AE (OAE)

II. Definitions of Security Notions

III. Our New Security Definitions(s) and Construction(s)

IV. Conclusion

The emergence of online-AE (OAE)

Fleischmann, Forler, Lucks (FFL)
McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. FSE 2012. (Full version, with Wenzel, retitled "McOE: A Foolproof On-line Authenticated Encryption Scheme." Cryptology ePrint report 2011/644 (Nov 2011; Dec 2013)

Promised an AE notion & scheme that was

- **online** ← **single pass** encryption with **O(1) memory** and
- **misuse resistant** ← retain security in the presence of **nonce-reuse**

APE	Joltik	Prøst-APE	COBRA	ICEPOLE	MORUS
COPA	KIASU	Prøst-COPA	Minalpher	iFeed	NORX
ElmD	Marble	SHELL	Artemia	Jambu	STRIBOB
Deoxys	POET	++AE	CBEAM	Keyak	

↑ **original versions**

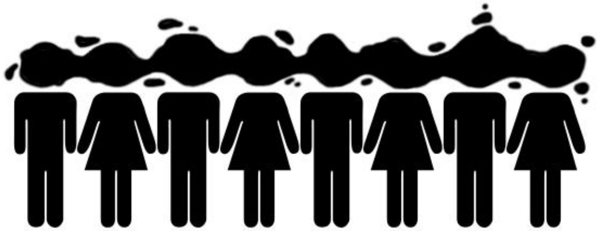
FFL-security claimed by authors

This claimed by others

Something **like** FFL-security claimed by authors

This claimed by others

Today



The FFL definition ("OAE1") has several issues.

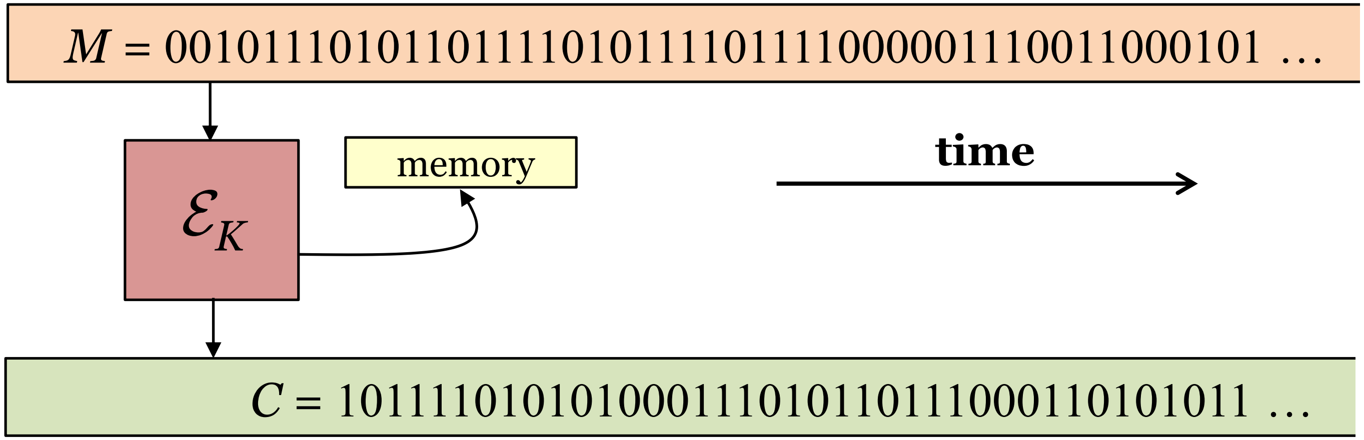
What does it **say**?
What's **problematic** with what it says?
What **should** a definition for online-AE say?

1) If we want it to be as nonce-reuse misuse-resistant as possible
2) If we don't care about nonce-reuse misuse resistance

This talk is based on the following paper:

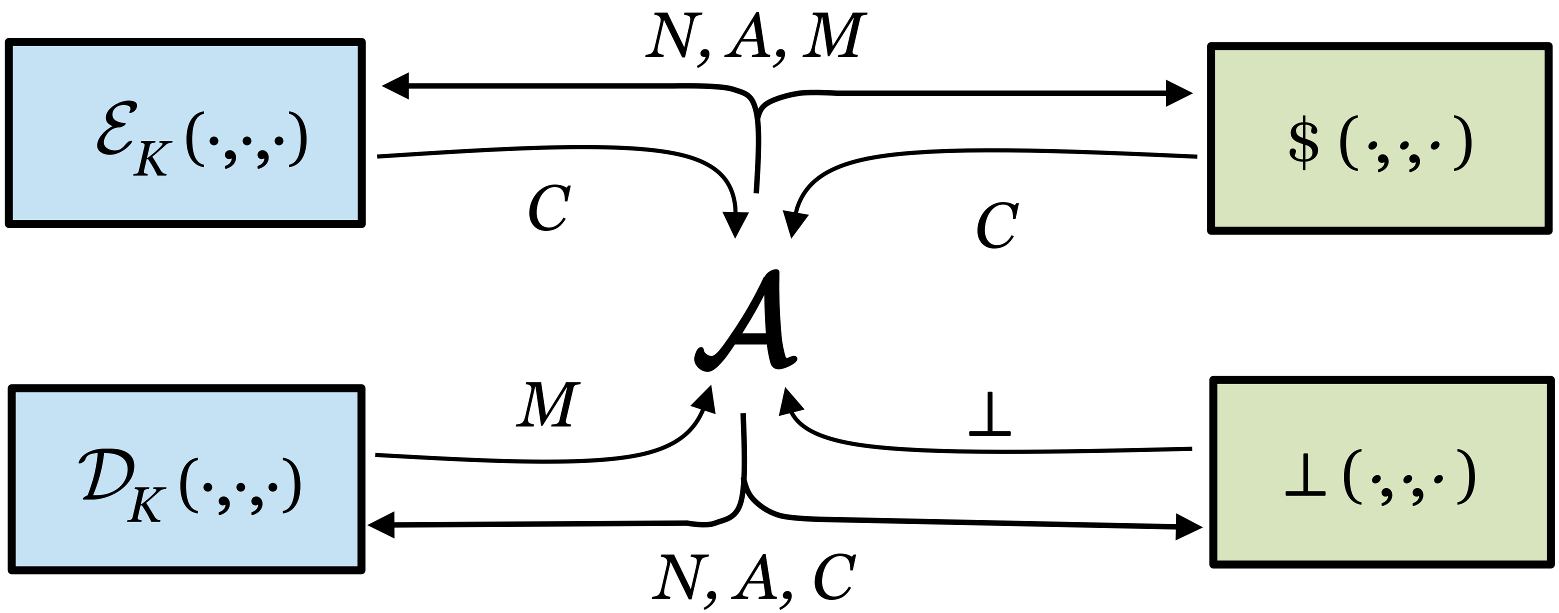
Viet Tung Hoang, Reza Reyhanitabar, Phillip Rogaway, Damian Vizár:
"Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance", CRYPTO 2015

Both
being online and
being nonce-reuse secure are good aims



nAE: Definition

All-in-one definition **[Rogaway, Shrimpton 2006].** Builds on a sequence of work beginning with **[Bellare-Rogaway 2000, Katz-Yung 2000]**

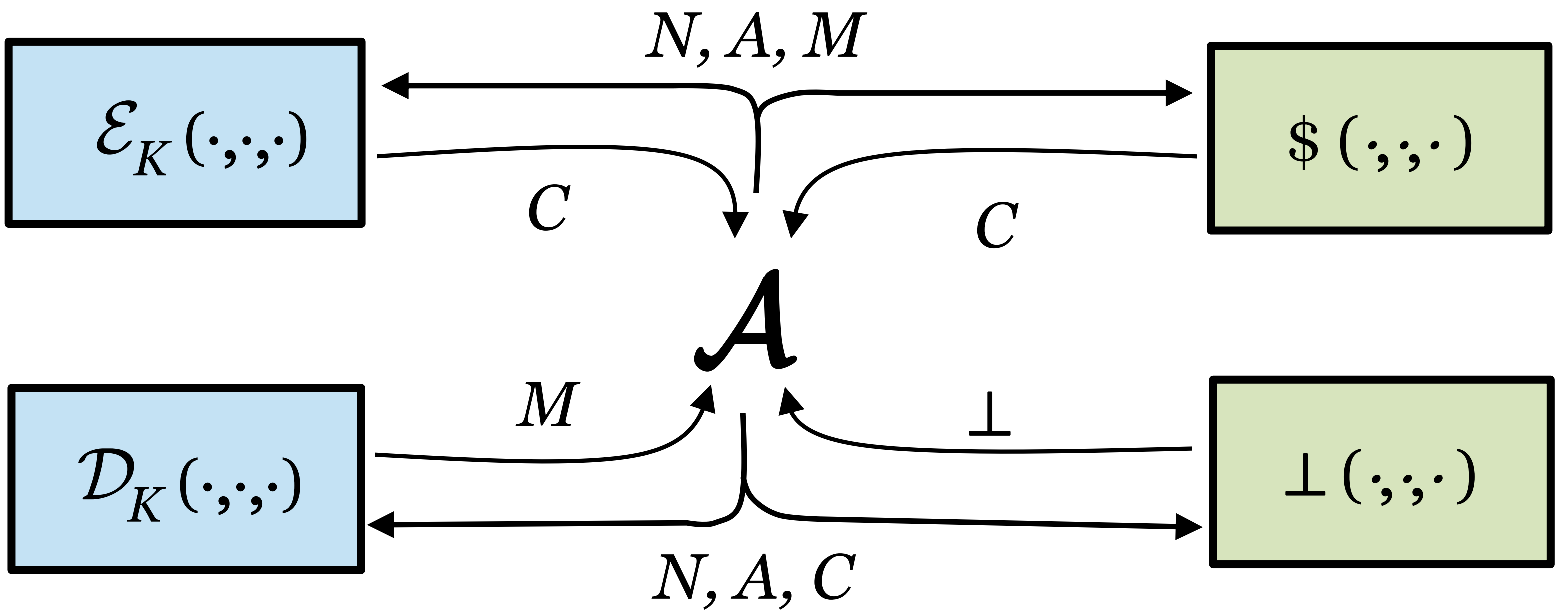


$$\mathbf{Adv}_{\Pi}^{\mathrm{nae}}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathcal{E}_K \mathcal{D}_K} \rightarrow 1] - \Pr[\mathcal{A}^{\$ \perp} \rightarrow 1]$$

$\mathcal{A}$ 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

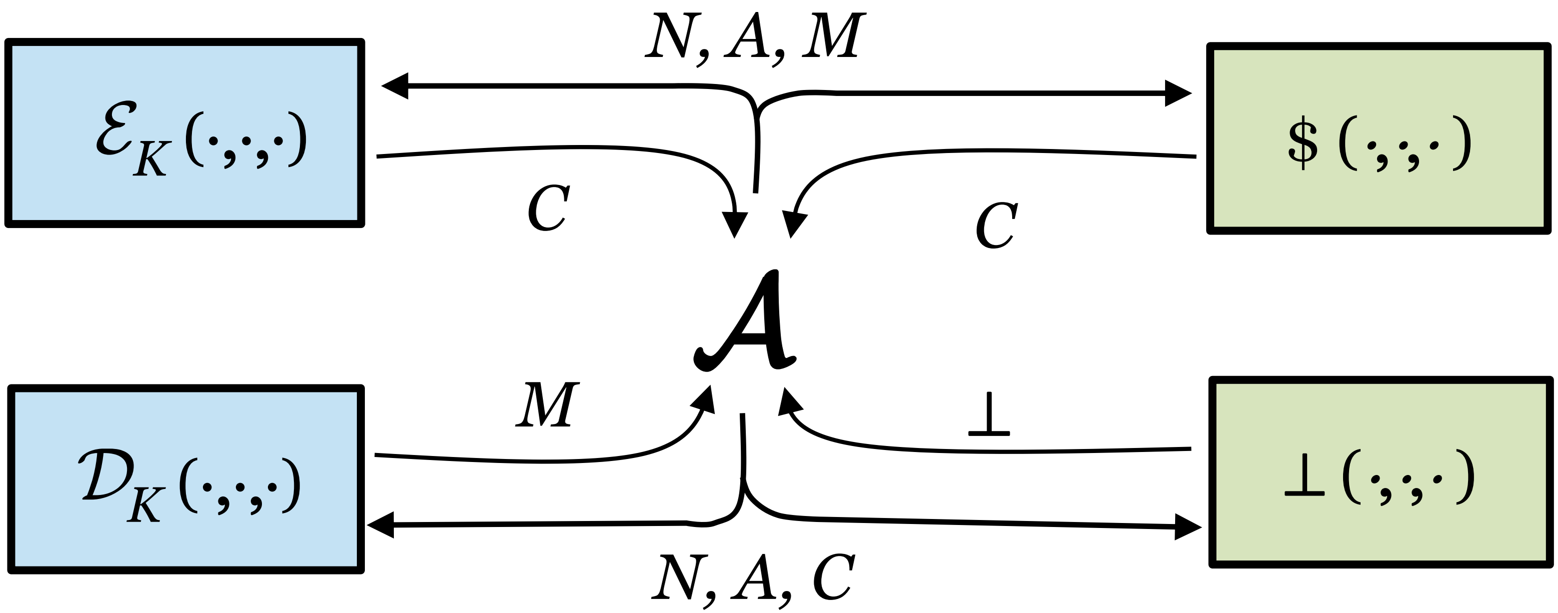
nAE: Assumptions



1. Atomicity of M
2. Atomicity of C
3. OK to demand non-repeating N

MRAE: Misuse-Resistant AE

[Rogaway, Shrimpton 2006]



$$\mathbf{Adv}_{\Pi}^{\mathrm{mrae}}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathcal{E}_K \mathcal{D}_K} \rightarrow 1] \; - \; \Pr[\mathcal{A}^{\$ \; \perp} \rightarrow 1]$$

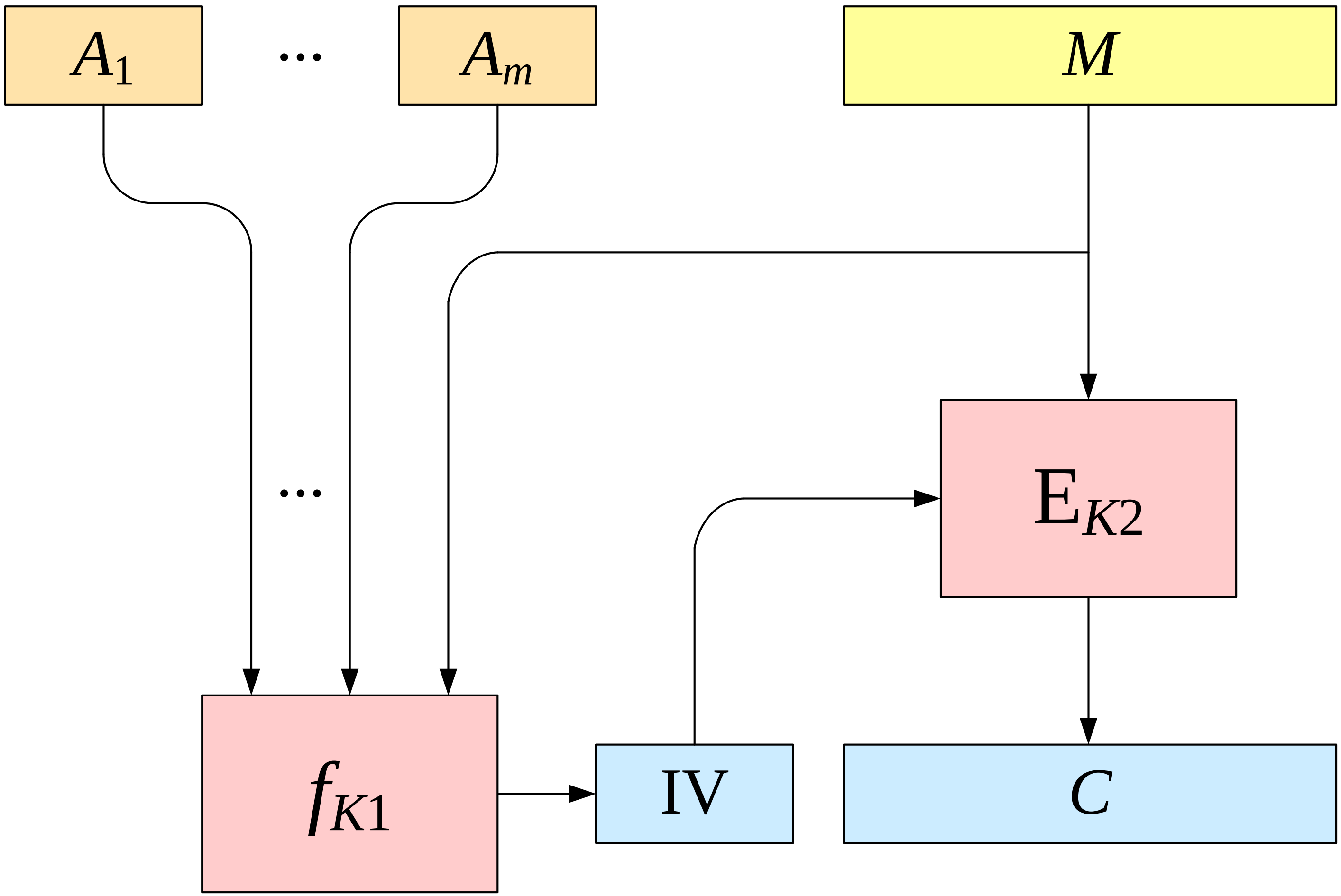
$\mathcal{A}$ may not:
- Repeat an Enc(N, A, M) query
- Ask Dec(N, A, C) after C is returned by an Enc(N, A, $\cdot$) query

If N repeats:
- authenticity is **undamaged**
- privacy is damaged to the extent that's **unavoidable**

MRAE schemes **can't** be online

SIV construction satisfies MRAE

[Rogaway and Shrimpton: Eurocrypt 2006]



MRAE

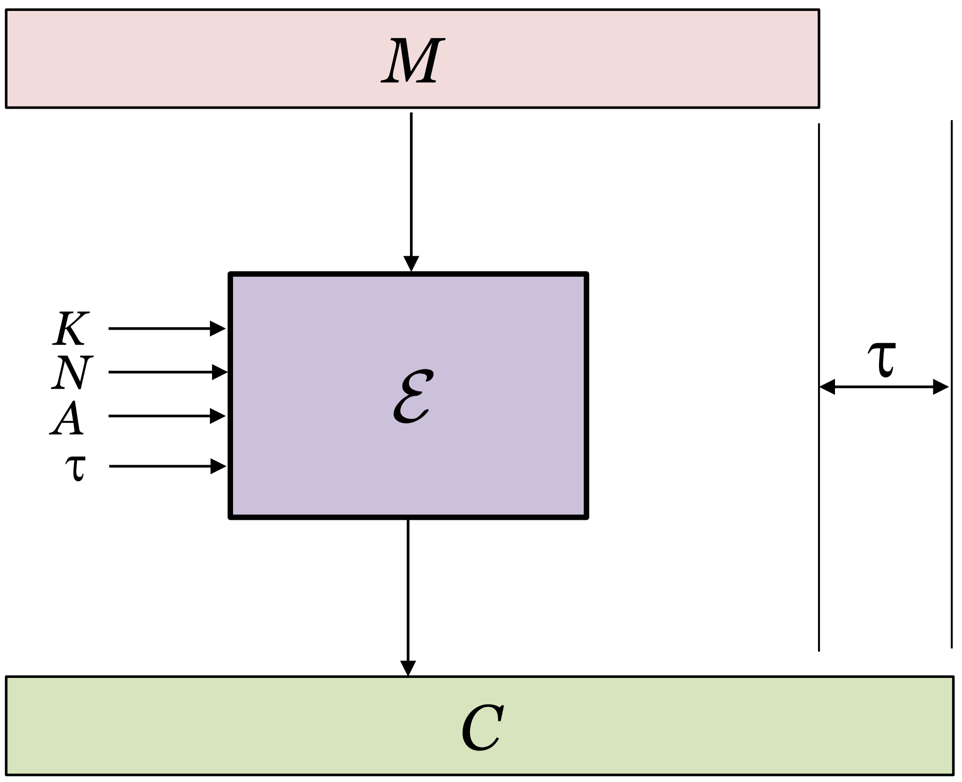
CAESAR candidates that satisfy **MRAE**:

- **AES-CMCC**
- **HS1-SIV**
- **Joltik v1.3** (has an MRAE mode)
- **Deoxys v1.3** (has an MRAE mode)

“robust-AE” (RAE)

[Hoang, Krovetz, Rogaway: Eurocrypt 2014]

RAE is a traditional AE notion, with atomic M and C.
What is new compared to MRAE is only that the user supplies τ, and it can be arbitrary.

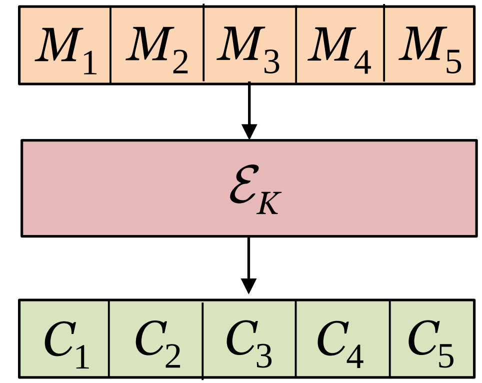


CAESAR candidate **AEZ** satisfy RAE

Online ciphers

[Bellare, Boldyreva, Knudsen, Namprempre 2001]

Fix some n. Let $B_n = \{0,1\}^n$ = all possible blocks.
Let B_n^* = all strings of blocks.



A **multiple-of-n cipher** is a map $\mathcal{E}\colon \mathcal{K} \times B_n^* \to B_n^*$ where $\mathcal{E}(K, \cdot)$ is a length-preserving permutation for each $K \in \mathcal{K}$.

OPerm[n] = all multiple-of-n ciphers π where the i-th block of $\pi(X)$ depends only on the first i blocks of X.

<u>**Good online cipher**</u>: multiple-of-n cipher $\mathcal{E}$ where $\mathcal{E}(K, \cdot)$ is indistinguisable from $\pi \twoheadleftarrow$OPerm[n]

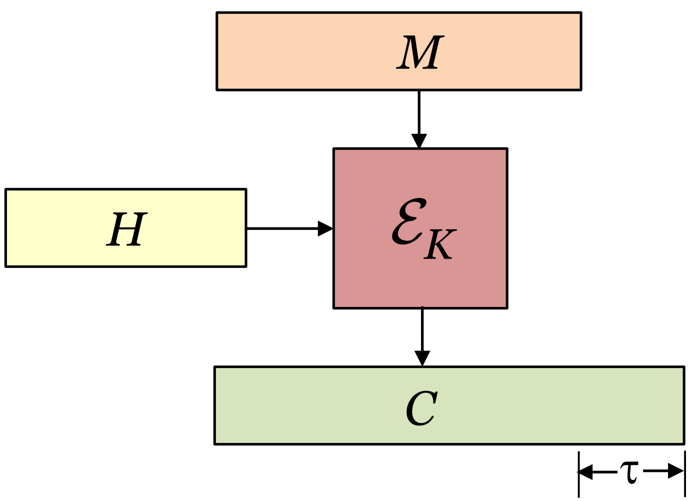
FFL's syntax for AE

Fix some n. A **multiple-of-n AE scheme** is a triple $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with

$$\mathcal{E}: \mathcal{K} \times \mathcal{H} \times \mathcal{M} \rightarrow \{0,1\}^*$$

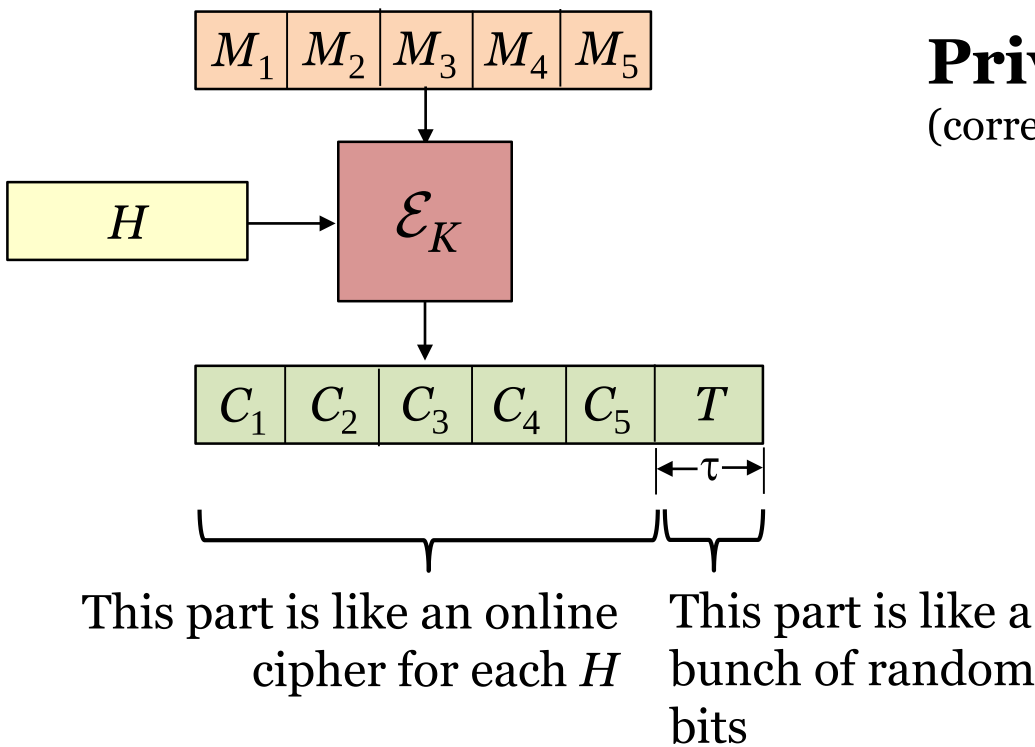
$$\mathcal{D}: \mathcal{K} \times \mathcal{H} \times \{0,1\}^* \rightarrow \mathcal{M} \cup \{\bot\}$$

with $\mathcal{M} = B_n^*$ and the decryptability condition.



Assume $|C| = |M| + \tau$

FFL definition: OAE1



Privacy

(corrected from FFL)

+Authenticity

Unforgeability

FFL definition: OAE1

proc initialize
$K \twoheadleftarrow \mathcal{K}$

proc $\mathrm{Enc}(H, M)$
if $H \notin \mathcal{H}$ **or** $M \notin \mathsf{B}_n^*$ **then**
  return $\perp$
return $\mathcal{E}(K, H, M)$

proc $\mathrm{Dec}(H, C)$
if $H \notin \mathcal{H}$ **then return** $\perp$
return $\mathcal{D}(K, H, C)$

proc initialize
for $H \in \mathcal{H}$ **do** $\pi_H \twoheadleftarrow \mathrm{OPerm}[n]$
for $(H, M) \in \mathcal{H} \times \mathsf{B}_n^*$ **do** $R_{H,M} \twoheadleftarrow \{0,1\}^\tau$

proc $\mathrm{Enc}(H, M)$
if $H \notin \mathcal{H}$ **or** $M \notin \mathsf{B}_n^*$ **then return** $\perp$
return $\pi_H(M) \,\|\, R_{H,M}$

proc $\mathrm{Dec}(H, C)$
return $\perp$

$\mathcal{A}$

Not allowed to ask Dec(H, C) after Enc(H, M) returns C

Def: a multiple-of-n AE scheme Π is OAE1-secure if

$$\mathbf{Adv}_{\Pi}^{\mathrm{oae1}}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathrm{Left}} \rightarrow 1] - \Pr[\mathcal{A}^{\mathrm{Right}} \rightarrow 1]$$

is "small" for "reasonable" adversaries $\mathcal{A}$.

OAE1 is weak: the "trivial attack"

- LCP[n]: C_i only depends on K, H, $M_1 \cdots M_i$
- Want to decrypt C $= \mathcal{E}(K, H, M)$
- Assume: an oracle that encrypts with K, H

Eg: n=1

0 $\xrightarrow{\text{Enc}}$

$M_1 0$ $\xrightarrow{\text{Enc}}$

$M_1 M_2 0$ $\xrightarrow{\text{Enc}}$

$\vdots$

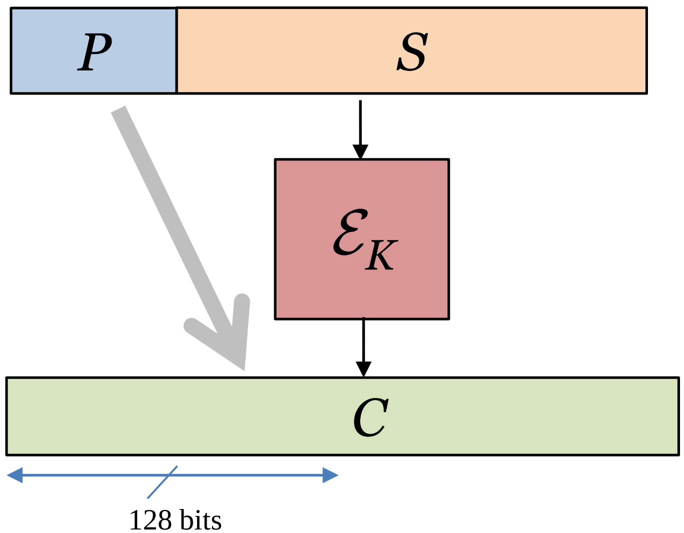
m=$|C|$ encryption queries to recover M

In general, $\frac{m}{n}(2^n - 1)$ queries to recover M

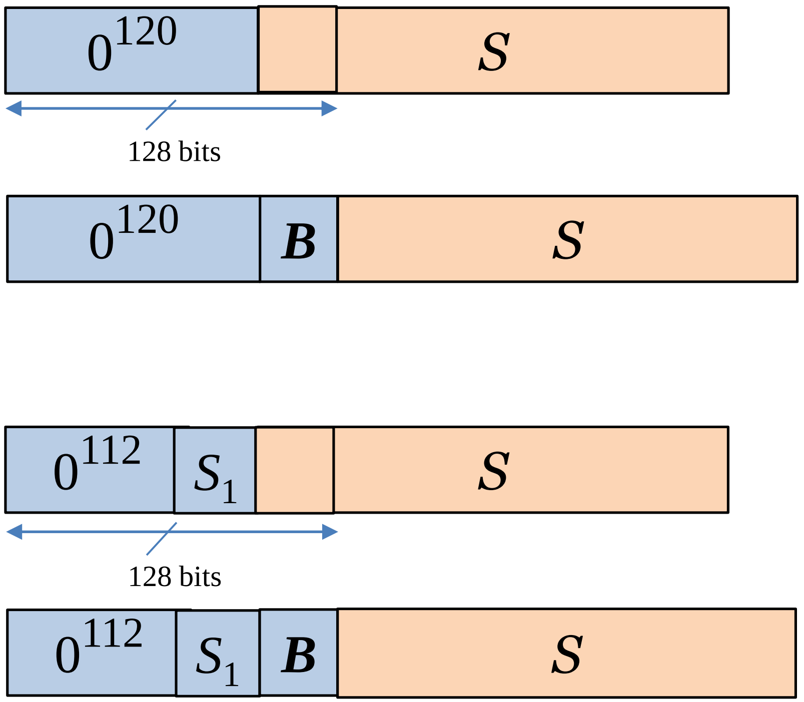
- OAE1 is quite insecure for small n
- Crucial to identify n when speaking of security

OAE1 is weak: the CPSS attack

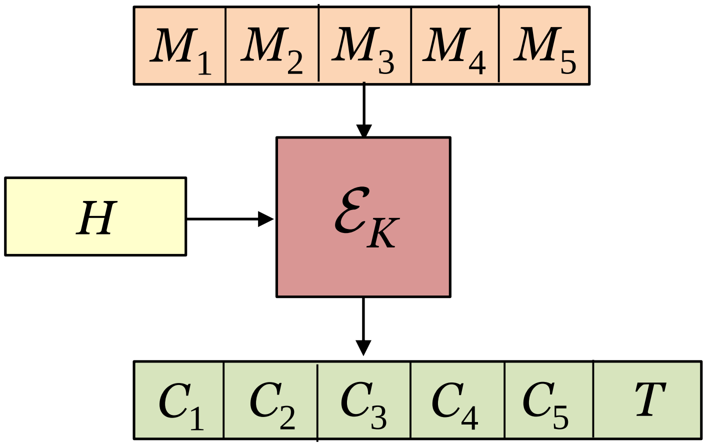
Assume LCP[n] (say n=128)



chosen-prefix/secret-suffix
(any byte string) (want to learn it)



But the real problem isn't these attacks. It's a failure to capture the underlying goal.



1. **Blocksize *n* should be a <u>user-selectable</u> value, not a scheme-dependent constant.** *It arises from a resource constraint of a user. It shouldn't be related to an implementing technology.*

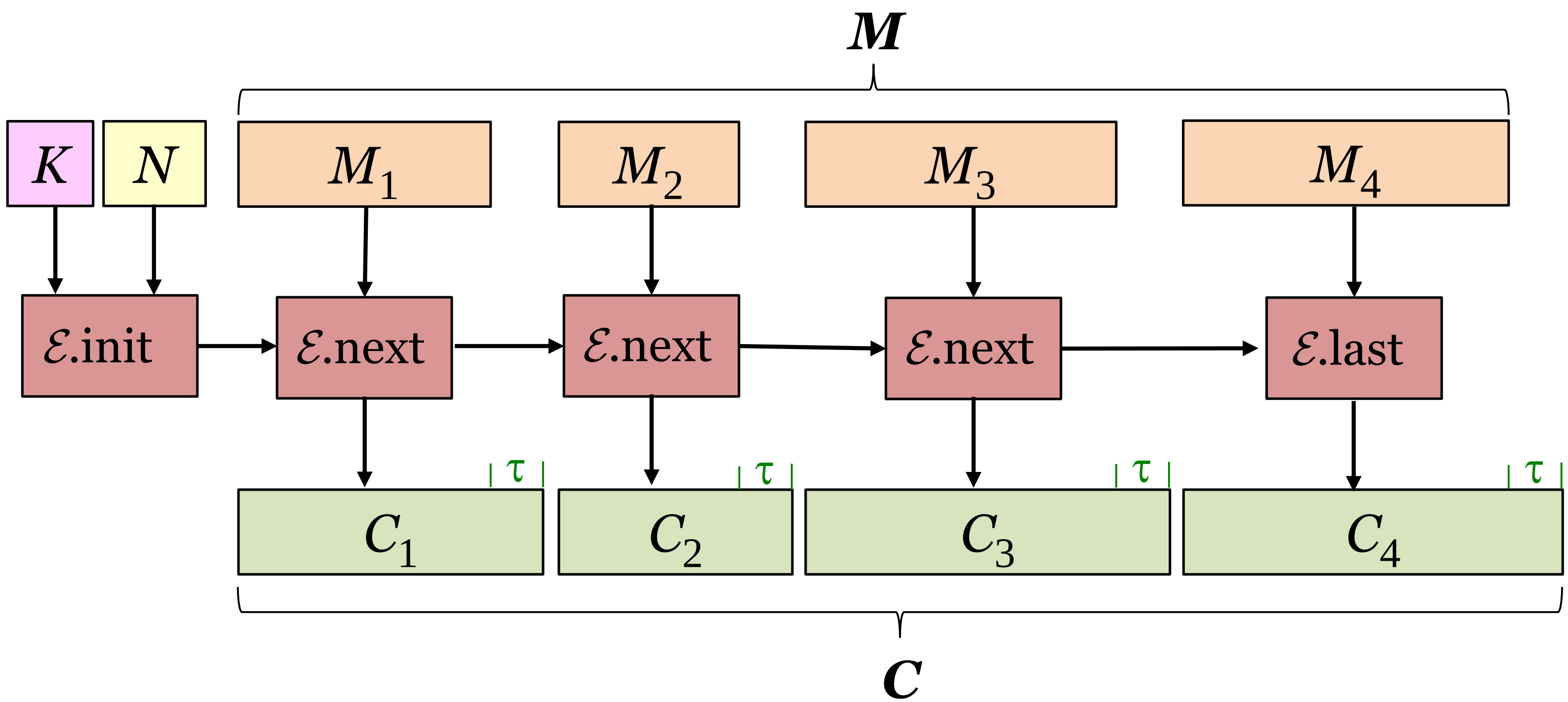
2. **Security needs to be defined for strings of <u>all</u> lengths, not just multiples-of-*n*.** *Saying one will pad begs the question.*

3. **Decryption <u>too</u> should be online** *How useful is it to have online-encryption if the receiver has to buffer the entire ciphertext?*

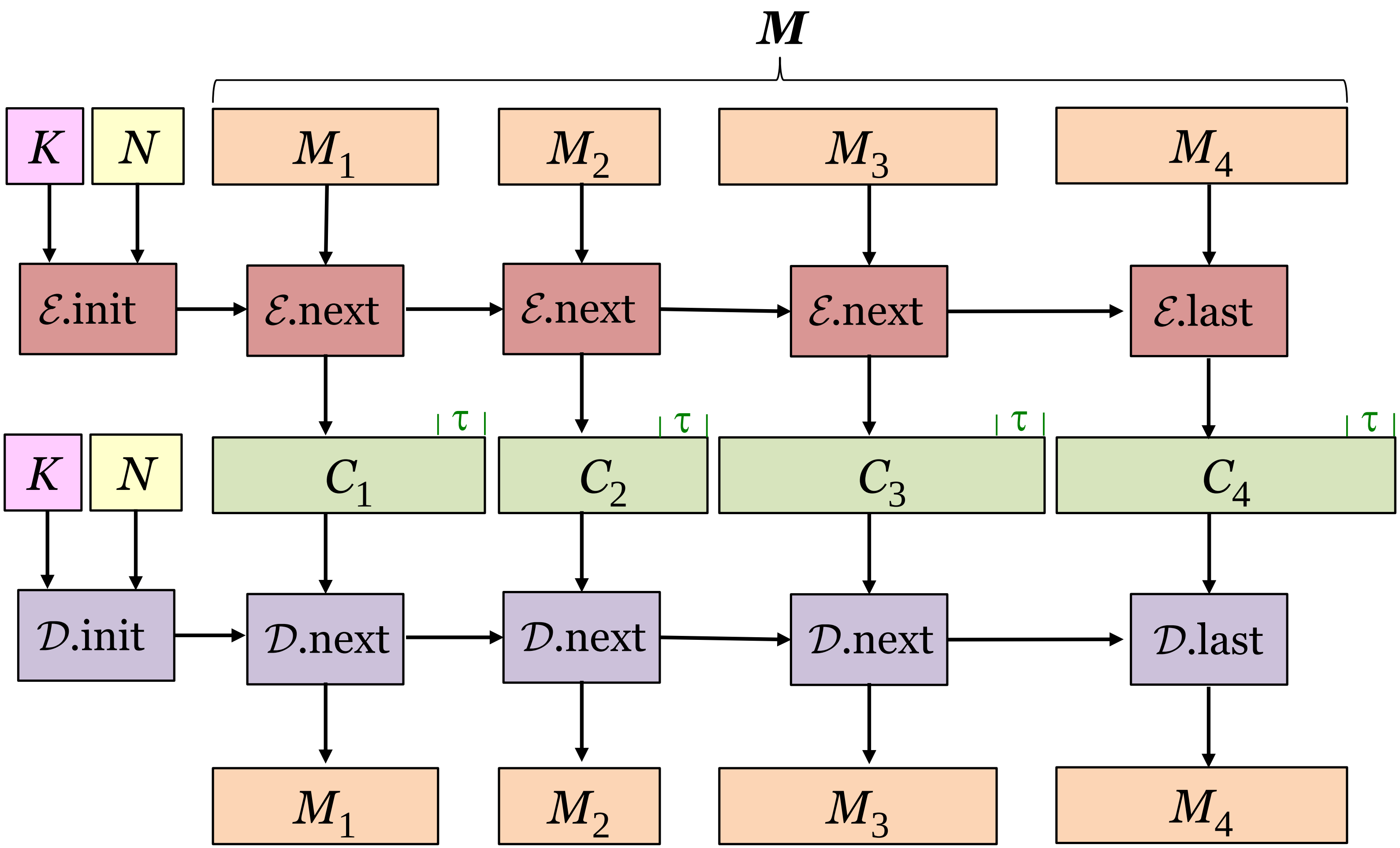
4. **The reference object is <u>not</u> ideal.** *Why an online cipher followed by random bits? We could do better with a different reference object.*

Towards OAE2
User-selectable segmentation

[Tsang, Solomakhin, Smith 2009]
[Bertoni, Daemen, Peeters,Van Assche 2010/2012]

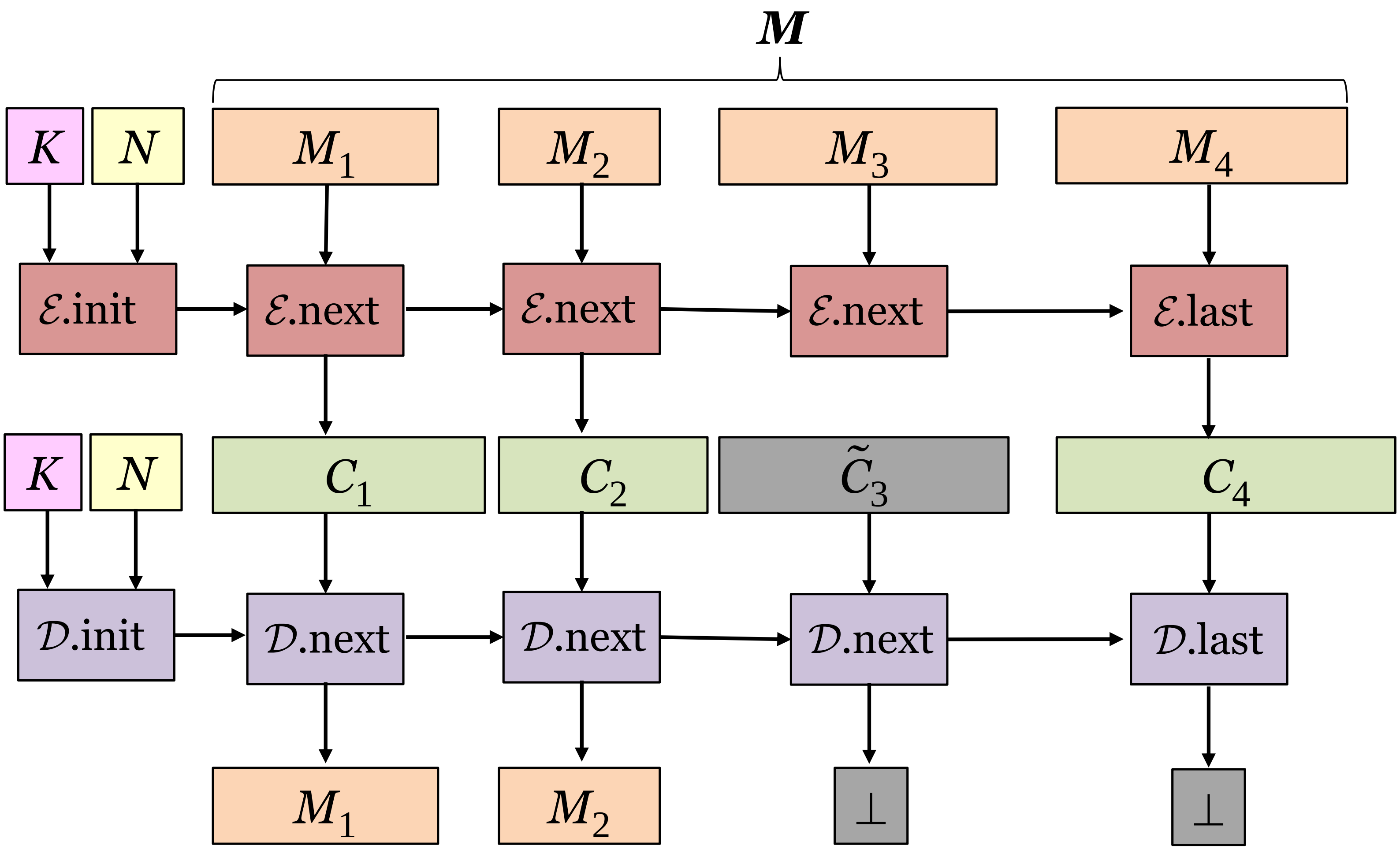


Towards OAE2
User-selectable segmentation

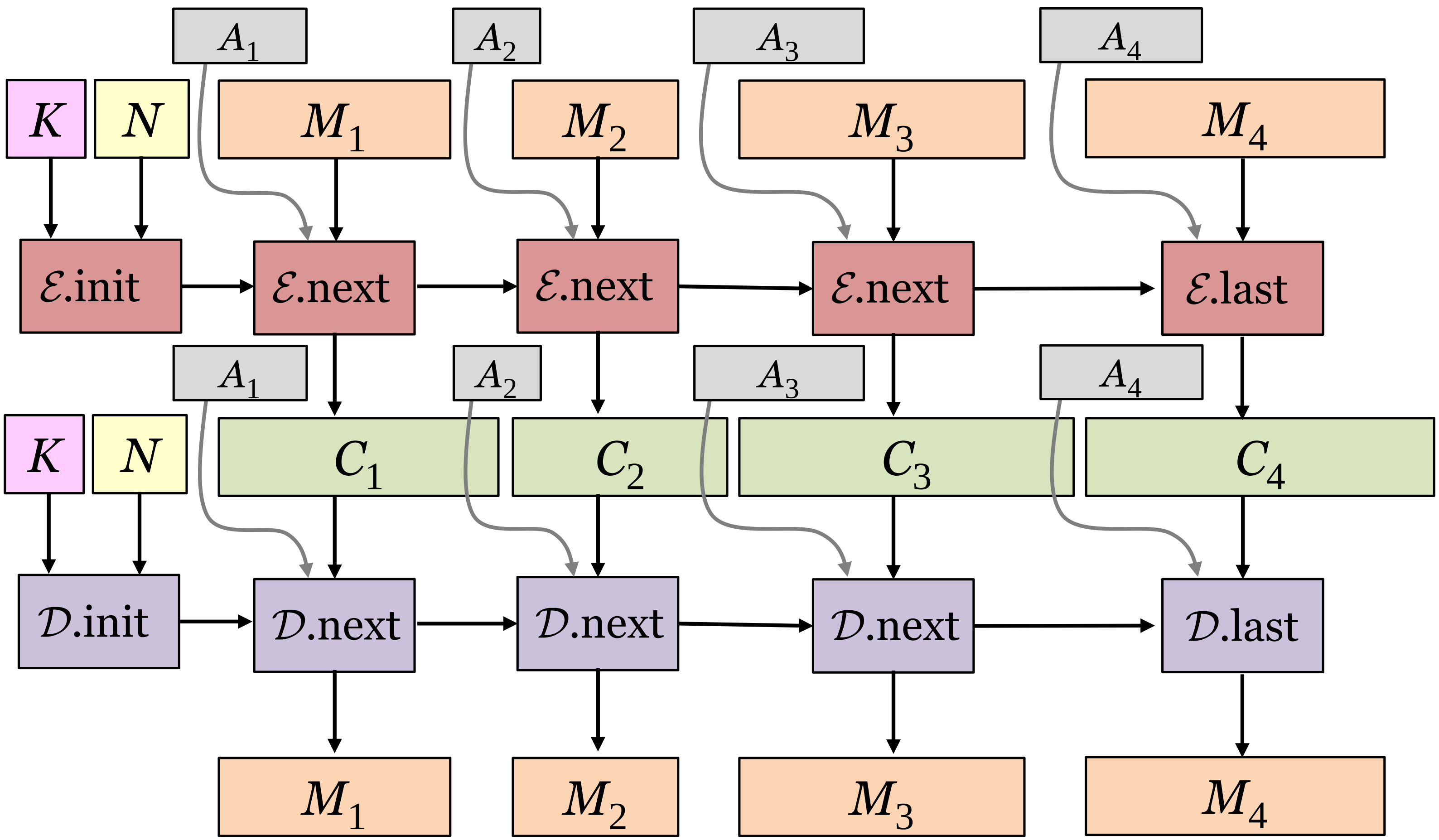


Towards OAE2

User-selectable segmentation



Towards OAE2
User-selectable segmentation



Towards OAE2
Syntax

Def: A **segmented-AE scheme** is a tuple $\Pi=(\mathcal{K},\mathcal{E},\mathcal{D})$ where

$\mathcal{K}$ is a distribution on strings and

$\mathcal{E} = (\mathcal{E}.\text{init}, \mathcal{E}.\text{next}, \mathcal{E}.\text{last})$ and

$\mathcal{D}=(\mathcal{D}.\text{init}, \mathcal{D}.\text{next}, \mathcal{D}.\text{last})$

are triples of deterministic algorithms:

$\mathcal{E}.\text{init}: \mathcal{K} \times \mathcal{N} \to \mathcal{S}$

$\mathcal{E}.\text{next}: \mathcal{S} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C} \times \mathcal{S}$

$\mathcal{E}.\text{last}: \mathcal{S} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C}$

$\mathcal{D}.\text{init}: \mathcal{K} \times \mathcal{N} \to \mathcal{S}$

$\mathcal{D}.\text{next}: \mathcal{S} \times \mathcal{A} \times \mathcal{C} \to (\mathcal{M} \times \mathcal{S}) \cup \{\perp\}$

$\mathcal{D}.\text{last}: \mathcal{S} \times \mathcal{A} \times \mathcal{C} \to \mathcal{M} \cup \{\perp\}$

$\mathcal{A} = \mathcal{M} = \mathcal{C} = \{0,1\}^*$ $\quad \mathcal{N} \subseteq \{0,1\}^*$

Formulating security

- **OAE2**: basic notion: best-possible security even if nonces get reused.
- **dOAE**: intermediate notion adapted from "Dupexing the Sponge" paper of [Bertoni, Daemen, Peeters, Van Assche 2010/2012]
- **nOAE**: weakening: equivalent in the cases that nonces are *not* reused.

strength ↑

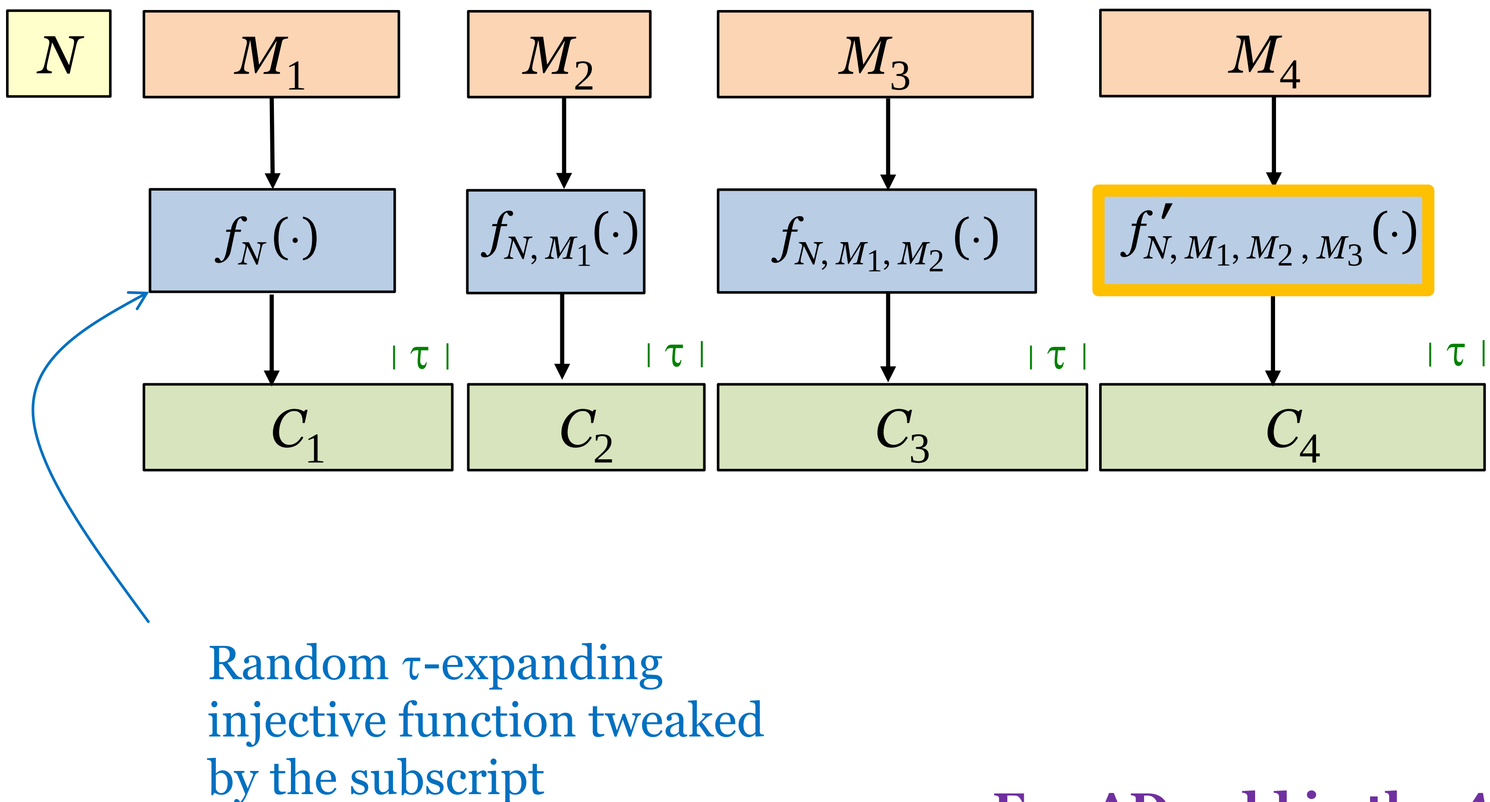
OAE2 — Can ask anything of the encryption oracle except $(N, \boldsymbol{A}, \boldsymbol{M})$ then $(N, \boldsymbol{A}, \boldsymbol{M})$

dOAE — Can ask anything of the encryption oracle except $(N, \boldsymbol{A}, \boldsymbol{M} \,\|\, M)$ then $(N, \boldsymbol{A}, \boldsymbol{M} \,\|\, M')$

nOAE — Can ask anything of the encryption oracle except $(N, \boldsymbol{A}, \boldsymbol{M})$ then $(N, \boldsymbol{A}', \boldsymbol{M}')$

Towards OAE2

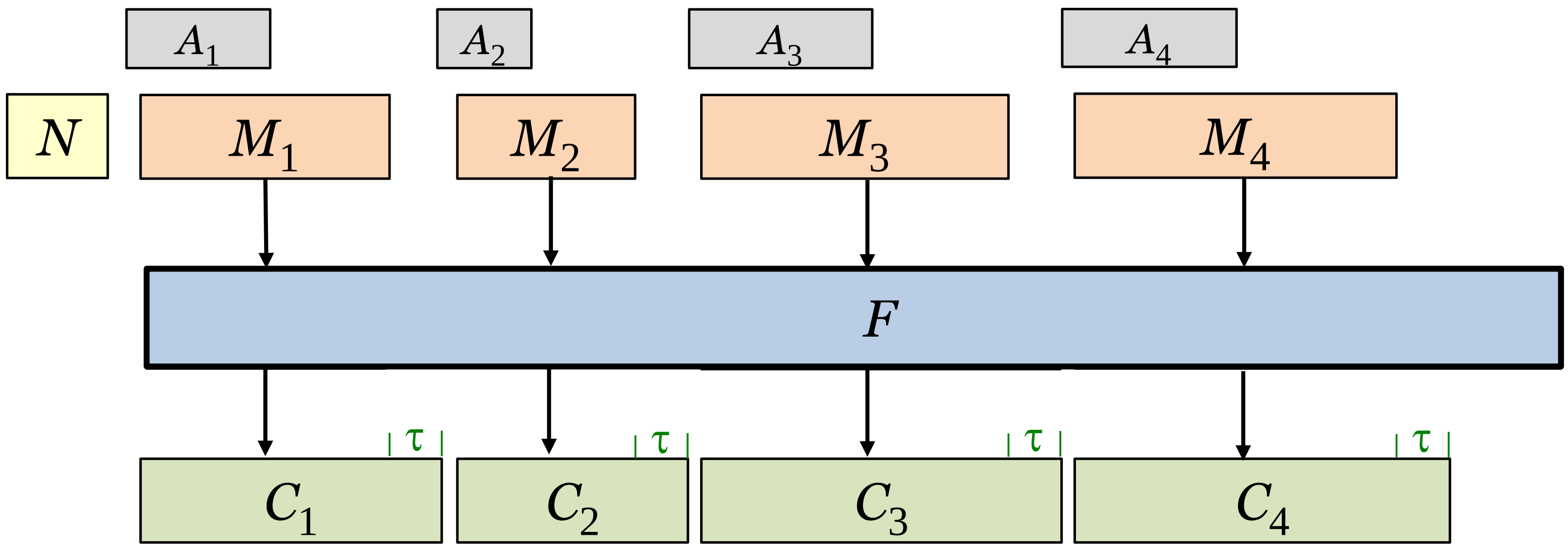
Ideal behavior



For AD: add in the A_i to each subscript

Towards OAE2

Ideal behavior



$F\,(N, \boldsymbol{A}, \boldsymbol{M}, \delta) \longmapsto \boldsymbol{C}$

$F \twoheadleftarrow \mathrm{IdealOAE}[\tau]$

for $m \in \mathbb{Z}^+,\ N \in \{0,1\}^*,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{M} \in (\{0,1\}^*)^{m-1}$ **do**

$\quad f_{N,\boldsymbol{A},\boldsymbol{M},0} \twoheadleftarrow \mathrm{Inj}(\tau);\quad f_{N,\boldsymbol{A},\boldsymbol{M},1} \twoheadleftarrow \mathrm{Inj}(\tau)$

for $m \in \mathbb{Z}^+,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{X} \in (\{0,1\}^*)^m,\ \delta \in \{0,1\}$ **do**

$$F(N, \boldsymbol{A}, \boldsymbol{X}, \delta) \leftarrow (\ f_{N,\boldsymbol{A}[1..1],\Lambda,0}(\boldsymbol{X}[1]),\ f_{N,\boldsymbol{A}[1..2],\boldsymbol{X}[1..1],0}(\boldsymbol{X}[2]),\ f_{N,\boldsymbol{A}[1..3],\boldsymbol{X}[1..2],0}(\boldsymbol{X}[3]), \ldots,\ f_{N,\boldsymbol{A}[1..m-1],\boldsymbol{X}[1..m-2],0}(\boldsymbol{X}[m-1]),\ f_{N,\boldsymbol{A}[1..m],\boldsymbol{X}[1..m-1],\delta}(\boldsymbol{X}[m]))$$

return F

Formalizing OAE2

proc initialize
$K \twoheadleftarrow \mathcal{K}$

proc Enc$(N, \boldsymbol{A}, \boldsymbol{M})$
if $N \notin \mathcal{N}$ **or** $|\boldsymbol{A}| \neq |\boldsymbol{M}|$ **then return** $\perp$
return $\boldsymbol{\mathcal{E}}(K, N, \boldsymbol{A}, \boldsymbol{M})$

proc Dec$(N, \boldsymbol{A}, \boldsymbol{C})$
if $N \notin \mathcal{N}$ **or** $|\boldsymbol{A}| \neq |\boldsymbol{M}|$ **then return** $\perp$
return $\boldsymbol{\mathcal{D}}(K, N, \boldsymbol{A}, \boldsymbol{C})$

proc initialize
$F \twoheadleftarrow \text{IdealOAE}(\tau)$

proc Enc$(N, \boldsymbol{A}, \boldsymbol{M})$
if $N \notin \mathcal{N}$ **or** $|\boldsymbol{A}| \neq |\boldsymbol{M}$ **then return** $\perp$
return $F(N, \boldsymbol{A}, \boldsymbol{M}, 1)$

proc Dec$(N, \boldsymbol{A}, \boldsymbol{C})$
if $N \notin \mathcal{N}$ **or** $|\boldsymbol{A}| \neq |\boldsymbol{M}|$ **then return** $\perp$
if $\exists \boldsymbol{M}$ s.t. $F(N, \boldsymbol{A}, \boldsymbol{M}, 1) = \boldsymbol{C}$ **then return** $\boldsymbol{M}$
$\boldsymbol{M} \leftarrow$ the longest vector in
$\{\boldsymbol{M}: \; F(N, \boldsymbol{A}, \boldsymbol{M}, 0)[i] = \boldsymbol{C}[i] \text{ for } i \in [1..|\boldsymbol{M}| - 1]\}$
return $\boldsymbol{M}$

The adversary $\mathcal{A}$ should be unable to distinguish the green and blue games

Three formulations of OAE2

Why?

- Very different approaches → *essentially equivalent* definitions
- Clarify the *extent* to which they are equivalent

OAE2a – The definition I just sketched..
Conceptually simplest.
Meant to formalize best *possible security*:
fix τ and ask how well can you do.

OAE2b – Tighter definition: model adversary's ability
to ask incremental queries.
Grow chains instead of asking vector-valued queries.

OAE2c – Easiest to work with,
measures distance from random bits.
Aspirational – only works for "large" τ.
Illustrates why τ ought to be large.

Formalizing OAE2

Version-b (OAE2b)

proc initialize
$I, J \leftarrow 0$; $\boxed{K \twoheadleftarrow \mathcal{K}}$

proc Enc.init(N)
if $N \notin \mathcal{N}$ **then return** $\bot$
$I \leftarrow I + 1$; $S_I \leftarrow \mathcal{E}.\text{init}(K, N)$
return I

proc Enc.next(i, A, M)
if $i \notin [1..I]$ **or** $S_i = \bot$ **then return** $\bot$
$(C, S_i) \leftarrow \mathcal{E}.\text{next}(S_i, A, M)$
return C

proc Enc.last(i, A, M)
if $i \notin [1..I]$ **or** $S_i = \bot$ **then return** $\bot$
$C \leftarrow \mathcal{E}.\text{last}(S_i, A, M)$
$S_i \leftarrow \bot$; **return** C

proc Dec.init(N)
if $N \notin \mathcal{N}$ **then return** $\bot$
$J \leftarrow J + 1$; $S'_J \leftarrow \mathcal{D}.\text{init}(K, N)$
return J

proc Dec.next(j, A, C)
if $j \notin [1..J]$ **or** $S'_j = \bot$ **then return** $\bot$
$(M, S'_j) \leftarrow \mathcal{D}.\text{next}(S'_j, A, C)$
return M

proc Dec.last(j, A, C)
if $j \notin [1..J]$ **or** $S'_j = \bot$ **then return** $\bot$
$M \leftarrow \mathcal{D}.\text{last}(S'_j, A, C)$
$S'_j \leftarrow \bot$
return M

$\mathcal{A}$

proc initialize
$I, J \leftarrow 0$; $\boxed{F \twoheadleftarrow \text{IdealOAE}(\tau)}$

proc Enc.init(N)
if $N \notin \mathcal{N}$ **then return** $\bot$
$I \leftarrow I + 1$; $N_I \leftarrow N$; $\mathbf{A}_I \leftarrow \Lambda$; $\mathbf{M}_I \leftarrow \Lambda$
return I

proc Enc.next(i, A, M)
if $i \notin [1..I]$ **or** $\mathbf{M}_i = \bot$ **then return** $\bot$
$\mathbf{A}_i \leftarrow \mathbf{A}_i \parallel A$; $\mathbf{M}_i \leftarrow \mathbf{M}_i \parallel M$; $m \leftarrow |\mathbf{M}_i|$
$\mathbf{C} \leftarrow F(N_i, \mathbf{A}_i, \mathbf{M}_i, 0)$; **return** $\mathbf{C}[m]$

proc Enc.last(i, A, M)
if $i \notin [1..I]$ **or** $\mathbf{M}_i = \bot$ **then return** $\bot$
$\mathbf{A}_i \leftarrow \mathbf{A}_i \parallel A$; $\mathbf{M}_i \leftarrow \mathbf{M}_i \parallel M$; $m \leftarrow |\mathbf{M}_i|$
$\mathbf{C} \leftarrow F(N_i, \mathbf{A}_i, \mathbf{M}_i, 1)$; $\mathbf{M}_i \leftarrow \bot$; **return** $\mathbf{C}[m]$

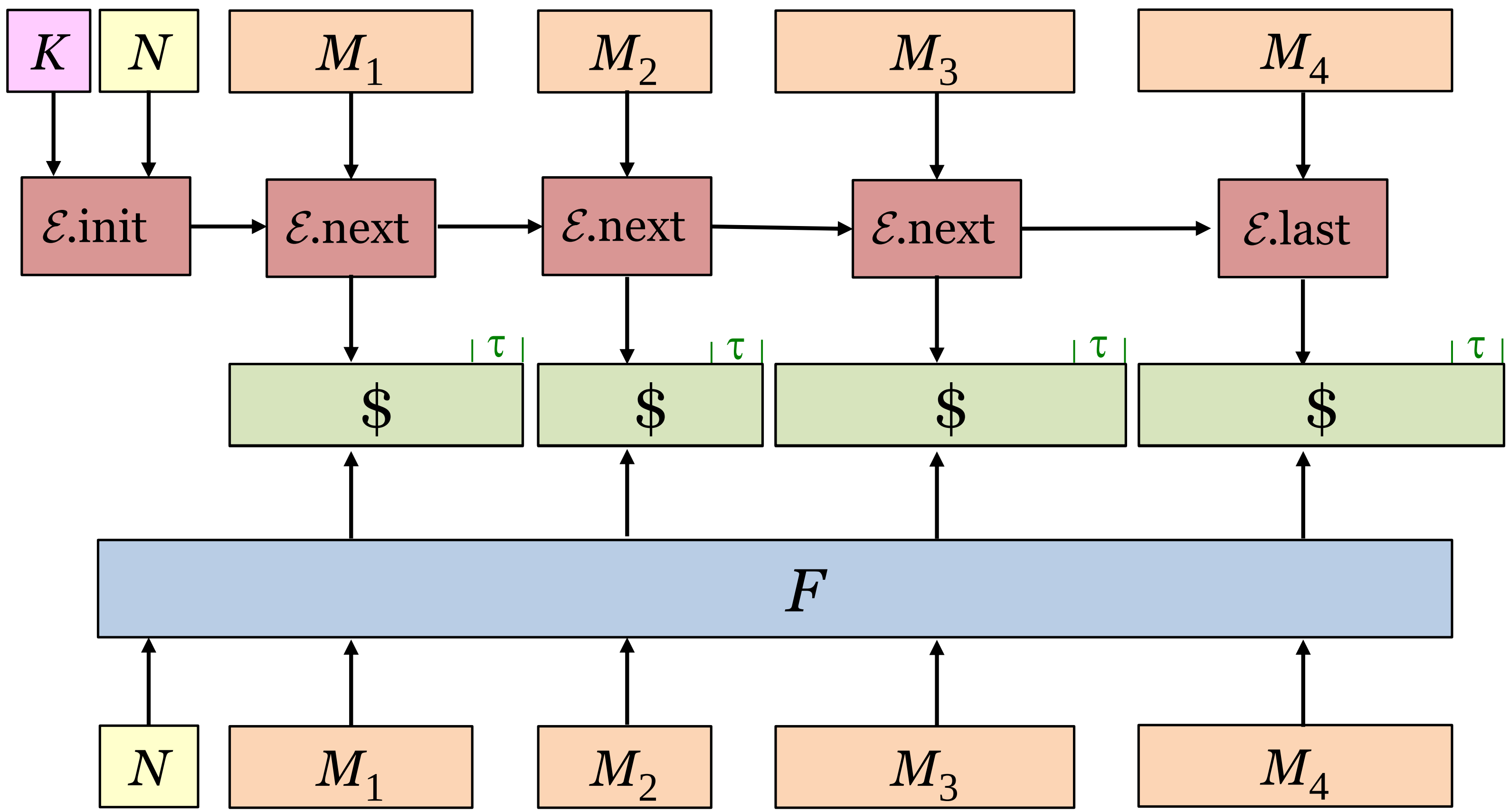
proc Dec.init(N)
if $N \notin \mathcal{N}$ **then return** $\bot$
$J \leftarrow J + 1$; $N'_J \leftarrow N$; $\mathbf{A}'_j \twoheadleftarrow \Lambda$; $\mathbf{C}_J \leftarrow \Lambda$
return J

proc Dec.next(j, A, C)
if $j \notin [1..J]$ **or** $\mathbf{C}_j = \bot$ **then return** $\bot$
$\mathbf{A}'_j \leftarrow \mathbf{A}_j \parallel A$; $\mathbf{C}_j \leftarrow \mathbf{C}_j \parallel C$; $m \leftarrow |\mathbf{C}_j|$
if $\exists \mathbf{M}$ s.t. $F(N'_j, \mathbf{A}'_j, \mathbf{M}, 0) = \mathbf{C}_j$
then return $\mathbf{M}[m]$
else $\mathbf{C}_j \leftarrow \bot$; **return** $\bot$; **fi**

proc Dec.last(j, A, C)
if $j \notin [1..J]$ **or** $\mathbf{C}_j = \bot$ **then return** $\bot$
$\mathbf{A}'_j \leftarrow \mathbf{A} \parallel A$; $\mathbf{C}_j \leftarrow \mathbf{C}_j \parallel C$; $m \leftarrow |\mathbf{C}_j|$
if $\exists \mathbf{M}$ s.t. $F(N'_j, \mathbf{A}'_j, \mathbf{M}_j, 1) = \mathbf{C}_j$
then $\mathbf{C}_j \leftarrow \bot$; **return** $\mathbf{M}[m]$
else $\mathbf{C}_j \leftarrow \bot$; **return** $\bot$ **fi**

Formalizing OAE2

Version-c (OAE2c)



Formalizing OAE2

Version-c (OAE2c)

proc initialize
$I \leftarrow 0$; $K \twoheadleftarrow \mathcal{K}$
$\mathcal{Z} \leftarrow \emptyset$

proc Enc.init(N)
if $N \notin \mathcal{N}$ **then return** $\bot$
$I \leftarrow I+1$; $S_I \leftarrow \mathcal{E}.\text{init}(K,N)$
$N_I \leftarrow N$; $\boldsymbol{A}_I \leftarrow \boldsymbol{M}_I \leftarrow \boldsymbol{C}_I \leftarrow \Lambda$
return I

proc Enc.next(i, A, M)
if $i \notin [1..I]$ **or** $S_i = \bot$ **then return** $\bot$
$(C, S_i) \leftarrow \mathcal{E}.\text{next}(S_i, A, M)$
$\boldsymbol{A}_i \leftarrow \boldsymbol{A}_i \parallel A$; $\boldsymbol{M}_i \leftarrow \boldsymbol{M}_i \parallel M$; $\boldsymbol{C}_i \leftarrow \boldsymbol{C}_i \parallel C$
$\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(N_i, \boldsymbol{A}_i, \boldsymbol{C}_i, 0)\}$
return C

proc Enc.last(i, A, M)
if $i \notin [1..I]$ **or** $S_i = \bot$ **then return** $\bot$
$C \leftarrow \mathcal{E}.\text{last}(S_i, A, M)$; $S_i \leftarrow \bot$
$\boldsymbol{A}_i \leftarrow \boldsymbol{A}_i \parallel A$; $\boldsymbol{M}_i \leftarrow \boldsymbol{M}_i \parallel M$; $\boldsymbol{C}_i \leftarrow \boldsymbol{C}_i \parallel C$
$\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(N_i, \boldsymbol{A}_i, \boldsymbol{C}_i, 1)\}$
return C

$\mathcal{A}$

proc initialize
$I \leftarrow 0$
$E(x) \leftarrow$ undef for all x

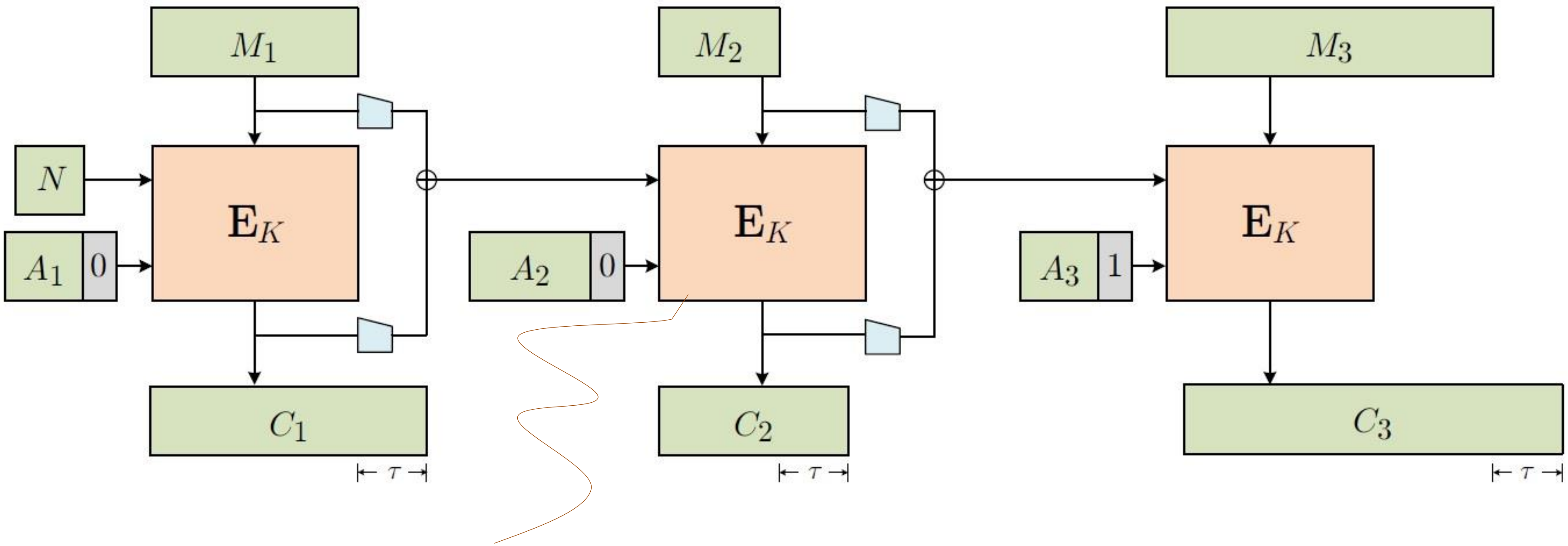
proc Enc.init(N)
if $N \notin \mathcal{N}$ **then return** $\bot$
$I \leftarrow I+1$
$N_I \leftarrow N$; $\boldsymbol{A}_i \leftarrow \boldsymbol{M}_i \leftarrow \Lambda$
return I

proc Enc.next(i, A, M)
if $i \notin [1..I]$ **or** $N_i = \bot$ **then return** $\bot$
$\boldsymbol{A}_i \leftarrow \boldsymbol{A}_i \parallel A$; $\boldsymbol{M}_i \leftarrow \boldsymbol{M}_i \parallel M$
if $E(N_i, \boldsymbol{A}_i, \boldsymbol{M}_i, 0) =$ undef
  then $E(N_i, \boldsymbol{A}_i, \boldsymbol{M}_i, 0) \twoheadleftarrow \{0,1\}^{|M|+\tau}$
$C \leftarrow E(N_i, \boldsymbol{A}_i, \boldsymbol{M}_i, 0)$; **return** C

proc Enc.last(i, A, M)
if $i \notin [1..I]$ **or** $N_i = \bot$ **then return** $\bot$
$\boldsymbol{A}_i \leftarrow \boldsymbol{A}_i \parallel A$; $\boldsymbol{M}_i \leftarrow \boldsymbol{M}_i \parallel M$
if $E(N_i, \boldsymbol{A}_i, \boldsymbol{M}_i, 1) =$ undef
  then $E(N_i, \boldsymbol{A}_i, \boldsymbol{M}_i, 1) \twoheadleftarrow \{0,1\}^{|M|+\tau}$
$C \leftarrow E(N_i, \boldsymbol{A}_i, \boldsymbol{M}_i, 1)$; $N_i \leftarrow \bot$; **return** C

proc finalize $(N, \boldsymbol{A}, \boldsymbol{C}, b)$
if $|\boldsymbol{A}| \neq |\boldsymbol{C}|$ **or** $|\boldsymbol{A}| = 0$ **or** $(N, \boldsymbol{A}, \boldsymbol{C}, b) \in \mathcal{Z}$ **then return** false
$S \leftarrow \mathcal{D}.\text{init}(K, N)$; $m \leftarrow |\boldsymbol{C}|$
for $i \leftarrow 1$ **to** $m - b$ **do**
  $(M, S) \leftarrow \mathcal{D}.\text{next}(S, \boldsymbol{A}[i], \boldsymbol{C}[i])$
  if $M = \bot$ **then return** false
if $b = 1$ **and** $\mathcal{D}.\text{last}(S, \boldsymbol{A}[m], \boldsymbol{C}[m]) = \bot$ **then return** false
return true

Achieving OAE2
The CHAIN construction

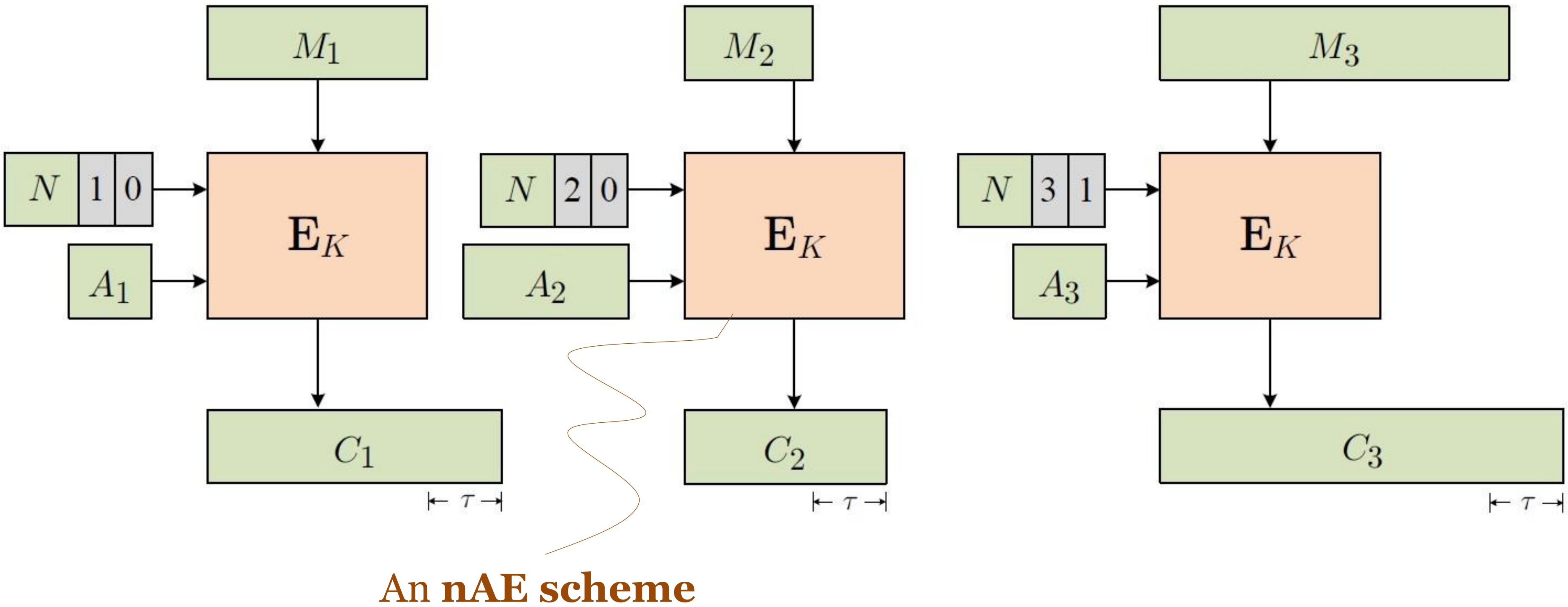


An **MRAE** scheme for large τ;
an **RAE** scheme for general τ

Why can't one use an **nAE** scheme?
OAE2 degenerates to **MRAE** when there's one segment and large τ; and a **strong PRP** with one segment and τ=0

Achieving nOAE2
The STREAM construction

Assume a large τ



Achieves the (weaker) nOAE notion.
Roughly what's done in the Netflix protocol.

Conclusions, suggestions, puzzles

- OAE should never have been about nonce-reuse MR. Historical artifact.

- Beware of the escalation of rhetoric. [FFL12] was circumspect in what they promised of OAE1. Soon morphed into claims as strong as OAE1 schemes being “nonce-free”.

- How does an immature definition quickly become the definitional target for so much constructive work?