Online Authenticated Encryption and its Nonce-Reuse Misuse-Resistance

Viet Tung Hoang[1] Reza Reyhanitabar[2] Phillip Rogaway[3]

Damian Vizár[4]

[1] UC, Santa Barbara [2] NEC Laboratories Europe, Germany [3] UC Davis

[4] EPFL, Switzerland

6th Asian Workshop on Symmetric Key Cryptography

This work was partially supported by Microsoft Research

“Online Authenticated Encryption”

- **Popular topic**
  - Several definitional works related to online AE *(blockwise attacks, CCA definition and online decryption, nonce misuse resistance, streaming channels)*
- **Popular target**
  - CAESAR 1st round: $11 + 6$ schemes claim online nonce misuse-resistance (or a variant)
  - New OAE construction presented at DIAC 2016
- **Repeatedly a point of discussion**
  - Definitional works appearing over a large timespan (2003 - now)
  - When is an AE scheme online?
  - When is an AE scheme online and nonce misuse-resistant?

“Online Authenticated Encryption”

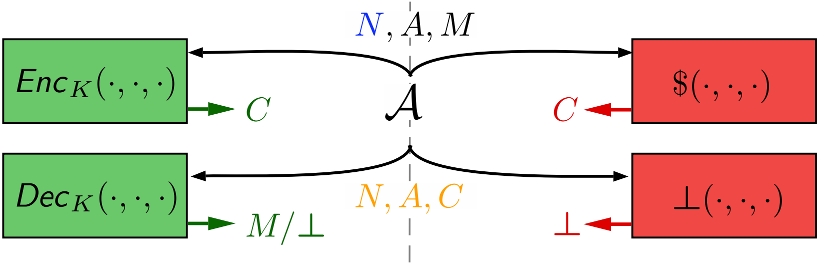
- **Popular topic**
  - Several definitional works related to online AE *(blockwise attacks, CCA definition and online decryption, nonce misuse resistance, streaming channels)*
- **Popular target**
  - CAESAR 1st round: $11 + 6$ schemes claim online nonce misuse-resistance (or a variant)
  - New OAE construction presented at DIAC 2016
- **Repeatedly a point of discussion**
  - Definitional works appearing over a large timespan (2003 - now)
  - When is an AE scheme online?
  - When is an AE scheme online and nonce misuse-resistant?

Nonce-based AEAD

[Rogaway 02]

$Enc : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \{0,1\}^*$ + decryptability

$Dec : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \{0,1\}^* \to \mathcal{M} \cup \{\perp\}$



N never repeats, (N, A, C) not trivially correct

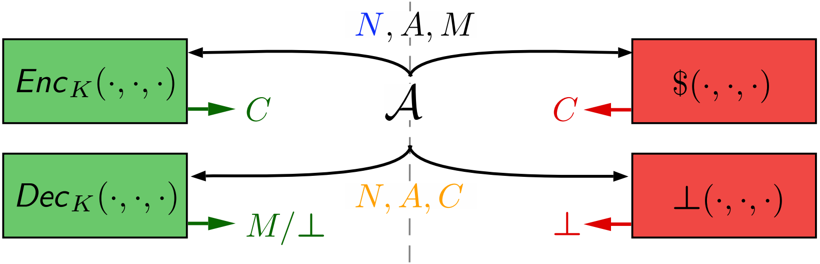
$$\mathbf{Adv}_{\Pi}^{nAE}(\boldsymbol{A}) = \Pr\left[\boldsymbol{A}^{Enc_K(\cdot,\cdot,\cdot),Dec_K(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{\$(\cdot,\cdot,\cdot),\perp(\cdot,\cdot,\cdot)} \Rightarrow 1\right]$$

Nonce-based AEAD

[Rogaway 02]

$Enc : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \{0,1\}^*$ + decryptability

$Dec : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \{0,1\}^* \to \mathcal{M} \cup \{\bot\}$



N never repeats, (N, A, C) not trivially correct

$$\mathbf{Adv}_{\Pi}^{nAE}(\boldsymbol{A}) = \Pr\left[\boldsymbol{A}^{Enc_K(\cdot,\cdot,\cdot),Dec_K(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{\$(\cdot,\cdot,\cdot),\bot(\cdot,\cdot,\cdot)} \Rightarrow 1\right]$$

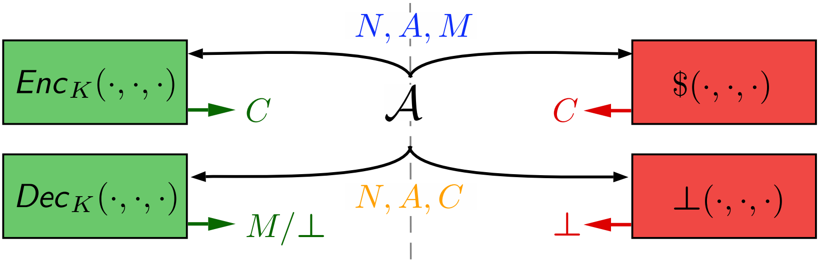
☺ **Efficient, good guarantees . . . unless nonces repeat** ☹

Nonce Misuse-Resistant AE

[Rogaway, Shrimpton 06]

Enc : $\mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \{0,1\}^*$ + decryptability

Dec : $\mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \{0,1\}^* \to \mathcal{M} \cup \{\bot\}$



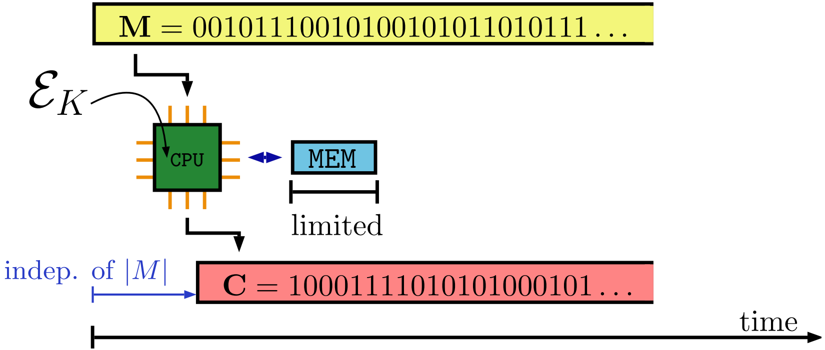
(N, A, M) never repeats, (N, A, C) not trivially correct

$$\mathbf{Adv}_{\Pi}^{MRAE}(\boldsymbol{A}) = \Pr\left[\boldsymbol{A}^{Enc_K(\cdot,\cdot,\cdot),Dec_K(\cdot,\cdot,\cdot)} \Rightarrow 1\right] - \Pr\left[\boldsymbol{A}^{\$(\cdot,\cdot,\cdot),\bot(\cdot,\cdot,\cdot)} \Rightarrow 1\right]$$

☺ **Only full repetitions of (N, A, M) are leaked now, full integrity**

Online Authenticated Encryption

Functionality Perspective



Extremely constrained devices

Performance-critical applications

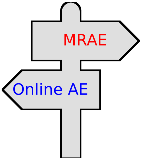
Jitter-sensitive applications

Latency-sensitive applications

Misuse-Resistant Online AE?

Onlineness at odds with MRAE security:

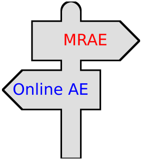
- MRAE: every bit of **C** must depend on all bits of **M**
- online AE: can't wait for all of **M** to compute **C**



Misuse-Resistant Online AE?

Onlineness at odds with MRAE security:

- MRAE: every bit of **C** must depend on all bits of **M**
- online AE: can't wait for all of **M** to compute **C**



Fleischmann, Forler, Lucks:
Online nonce misuse-resistant AE (OAE)

Promise a notion and schemes both

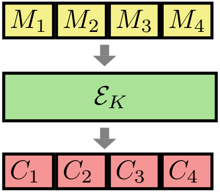
- nonce misuse-resistant: retains **security** in presence of **nonce repetition**
- online: **single-pass** encryption with **O(1) of memory**

$\rightarrow$ **Call it OAE1**

Online Ciphers

[Bellare, Boldyreva, Knudsen, Namprempre 01]

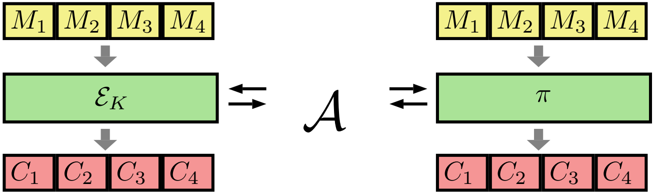
- Multiple of n strings $\boldsymbol{\mathcal{B}}_{\mathbf{n}}^{*}$ (with $\mathcal{B}_n = \{0,1\}^n$)
- Length preserving $\mathcal{E} : \mathcal{K} \times \mathcal{B}_n^* \to \mathcal{B}_n^*$



Online Ciphers

[Bellare, Boldyreva, Knudsen, Namprempre 01]

- Multiple of n strings $\mathcal{B}_{\mathbf{n}}^*$ (with $\mathcal{B}_n = \{0,1\}^n$)
- Length preserving $\mathcal{E} : \mathcal{K} \times \mathcal{B}_n^* \to \mathcal{B}_n^*$



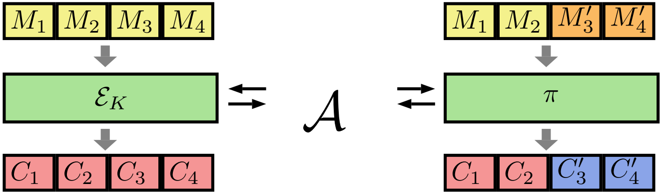
$$\mathbf{Adv}_{\mathcal{E}}^{oprp}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathcal{E}_K} \Rightarrow 1] - \Pr[\mathcal{A}^{\pi} \Rightarrow 1]$$

with $\pi \leftarrow\$ \mathrm{OPerm}[n]$

Online Ciphers

[Bellare, Boldyreva, Knudsen, Namprempre 01]

- Multiple of n strings $\mathcal{B}_{\mathbf{n}}^{*}$ (with $\mathcal{B}_n = \{0,1\}^n$)
- Length preserving $\mathcal{E} : \mathcal{K} \times \mathcal{B}_n^* \rightarrow \mathcal{B}_n^*$



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

with $\pi \leftarrow\$ \ \mathrm{OPerm}[n]$

OPerm[**n**] set of all ϕ s.t.

- ϕ is length preserving permutation over $\mathcal{B}_n$
- for all $X, Y, Y' \in \mathcal{B}_n$, $\phi(X \| Y)$ and $\phi(X, Y')$ share prefix of $|X|$ bits

OAE1

[Fleischman,Forler,Lucks 12]

A multiple of n AE cipher is a triplet $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathcal{E} : \mathcal{K} \times \mathcal{H} \times \mathcal{M} \to \{0,1\}^*$$
$$\mathcal{D} : \mathcal{K} \times \mathcal{H} \times \{0,1\}^* \to \mathcal{B}_n^* \cup \{\perp\}$$

with $\mathcal{M} = \mathcal{B}_n^*$ and decryptability condition. Assume $|C| = |M| + \tau$.

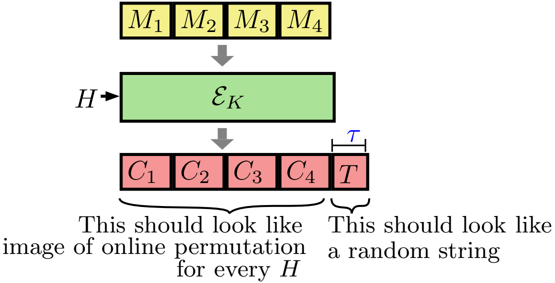
OAE1

[Fleischman,Forler,Lucks 12]

A multiple of *n* AE cipher is a triplet $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

$$\mathcal{E} : \mathcal{K} \times \mathcal{H} \times \mathcal{M} \rightarrow \{0,1\}^*$$
$$\mathcal{D} : \mathcal{K} \times \mathcal{H} \times \{0,1\}^* \rightarrow \mathcal{B}_n^* \cup \{\perp\}$$

with $\mathcal{M} = \mathcal{B}_n^*$ and decryptability condition. Assume $|C| = |M| + \tau$.



Privacy

OPerm[n] + random tag

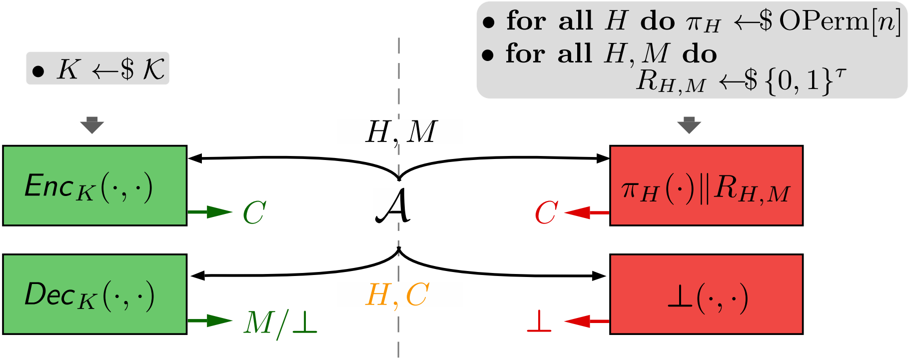
+

Authenticity

Unforgeability

OAE1

Security Notion



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

H, C must not be obtained via previous encryption

OAE1

Attacks

Trivial Attack: OAE1 schemes preserve LCP[n]

- for $X, Y \in \mathcal{B}_n^*$, LCP[n](X, Y) is longest common blockwise prefix

OAE1

Attacks

Trivial Attack: OAE1 schemes preserve LCP[n]

- for $X, Y \in \mathcal{B}_n^*$, LCP[n](X, Y) is longest common blockwise prefix

Given $\mathbf{C} = \mathbf{Enc}(\mathbf{H}, \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3})$ obtain $\mathbf{M} = \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3}$

C_1	C_2	C_3	T

1. $M \leftarrow \varepsilon$
2. for $i = 1$ to 3
    1. find $B \in \mathcal{B}_n$ s.t.
       $\mathrm{LCP}[n](C, Enc(H, M \| B)) = 1$
    2. $M \leftarrow M \| B$
3. return M

OAE1

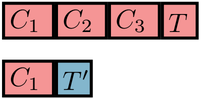
Attacks

Trivial Attack: OAE1 schemes preserve LCP[n]

- for $X, Y \in \mathcal{B}_n^*$, LCP[n](X, Y) is longest common blockwise prefix

Given $\mathbf{C} = \mathbf{Enc}(\mathbf{H}, \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3})$ **obtain** $\mathbf{M} = \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3}$

1. $M \leftarrow \varepsilon$
2. for $i = 1$ to 3
    1. find $B \in \mathcal{B}_n$ s.t.
       $\text{LCP}[n](C, Enc(H, M \| B)) = 1$
    2. $M \leftarrow M \| B$
3. return M



OAE1

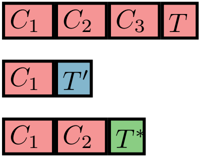
Attacks

Trivial Attack: OAE1 schemes preserve LCP[n]

- for $X, Y \in \mathcal{B}_n^*$, LCP[n](X, Y) is longest common blockwise prefix

Given $\mathbf{C} = \mathbf{Enc}(\mathbf{H}, \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3})$ **obtain** $\mathbf{M} = \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3}$

1. $M \leftarrow \varepsilon$
2. for $i = 1$ to 3
    1. find $B \in \mathcal{B}_n$ s.t.
       $\text{LCP}[n](C, Enc(H, M \| B)) = 1$
    2. $M \leftarrow M \| B$
3. return M



OAE1

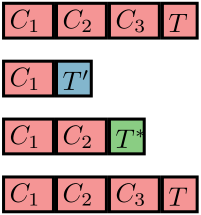
Attacks

Trivial Attack: OAE1 schemes preserve LCP[n]

- for $X, Y \in \mathcal{B}_n^*$, LCP[n](X, Y) is longest common blockwise prefix

Given $\mathbf{C} = \mathbf{Enc}(\mathbf{H}, \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3})$ obtain $\mathbf{M} = \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3}$

1. $M \leftarrow \varepsilon$
2. for $i = 1$ to 3
   1. find $B \in \mathcal{B}_n$ s.t. $\text{LCP}[n](C, Enc(H, M \| B)) = 1$
   2. $M \leftarrow M \| B$
3. return M



OAE1

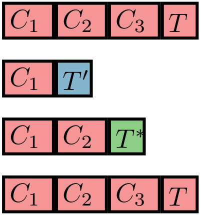
Attacks

Trivial Attack: OAE1 schemes preserve LCP[n]

- for $X, Y \in \mathcal{B}_n^*$, LCP[n](X, Y) is longest common blockwise prefix

Given $\mathbf{C} = \mathbf{Enc}(\mathbf{H}, \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3})$ **obtain** $\mathbf{M} = \mathbf{M_1} \| \mathbf{M_2} \| \mathbf{M_3}$

1. $M \leftarrow \varepsilon$
2. for $i = 1$ to 3
   1. find $B \in \mathcal{B}_n$ s.t. LCP[n]$(C, Enc(H, M\|B)) = 1$
   2. $M \leftarrow M\|B$
3. return M



Finding each **B** takes at most $\mathbf{2^n - 1}$ Enc queries: **Decryption of** ℓ **block message with** $\ell \times (\mathbf{2^n - 1})$ **Enc queries**

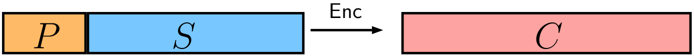
Small n ?! (e.g. 40 bits)

OAE1

Attacks

CPSS attack Inspired by the BEAST attack [Duong Rizzo 11]

Setting: e.g. block size $n = 128$ bits, byte-oriented strings



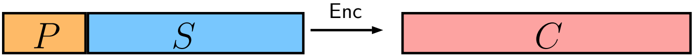
Chosen prefix under control and secret suffix to recover

1. Get $Enc(P_0 \| S)$ with $P_0 \in \{0,1\}^{120}$
2. Find first byte S_0 using LCP[n]
3. Get $Enc(P_1 \| S)$ with $P_1 \in \{0,1\}^{112}$
4. Find second byte S_1 using LCP[n]
5. etc

OAE1
Attacks

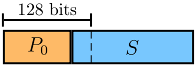
CPSS attack Inspired by the BEAST attack [Duong Rizzo 11]

Setting: e.g. block size $n = 128$ bits, byte-oriented strings



Chosen prefix under control and secret suffix to recover

1. Get $Enc(P_0 \| S)$ with $P_0 \in \{0,1\}^{120}$
2. Find first byte S_0 using LCP[n]
3. Get $Enc(P_1 \| S)$ with $P_1 \in \{0,1\}^{112}$
4. Find second byte S_1 using LCP[n]
5. etc

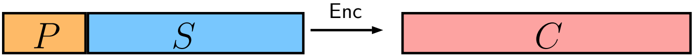


OAE1

Attacks

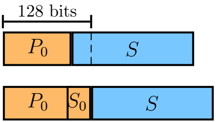
CPSS attack Inspired by the BEAST attack [Duong Rizzo 11]

Setting: e.g. block size $n = 128$ bits, byte-oriented strings



Chosen prefix under control and secret suffix to recover

1. Get $Enc(P_0 \| S)$ with $P_0 \in \{0,1\}^{120}$
2. Find first byte S_0 using LCP[n]
3. Get $Enc(P_1 \| S)$ with $P_1 \in \{0,1\}^{112}$
4. Find second byte S_1 using LCP[n]
5. etc

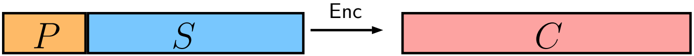


OAE1

Attacks

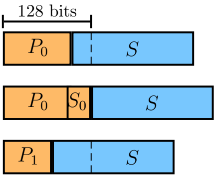
CPSS attack Inspired by the BEAST attack [Duong Rizzo 11]

Setting: e.g. block size $n = 128$ bits, byte-oriented strings



Chosen prefix under control and secret suffix to recover

1. Get $Enc(P_0 \| S)$ with $P_0 \in \{0,1\}^{120}$
2. Find first byte S_0 using LCP[n]
3. Get $Enc(P_1 \| S)$ with $P_1 \in \{0,1\}^{112}$
4. Find second byte S_1 using LCP[n]
5. etc

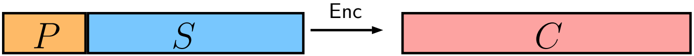


OAE1

Attacks

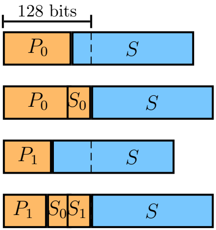
CPSS attack Inspired by the BEAST attack [Duong Rizzo 11]

Setting: e.g. block size $n = 128$ bits, byte-oriented strings



Chosen prefix under control and secret suffix to recover

1. Get $Enc(P_0 \| S)$ with $P_0 \in \{0,1\}^{120}$
2. Find first byte S_0 using LCP[n]
3. Get $Enc(P_1 \| S)$ with $P_1 \in \{0,1\}^{112}$
4. Find second byte S_1 using LCP[n]
5. etc



OAE1
Attacks

CPSS Generalizes to:

- Chosen **part** of prefix under control
- Left and right part of prefix known
- Secret **part** of suffix to recover
- Arbitrary remainder of suffix

$\Rightarrow$ Corresponds to HTTP

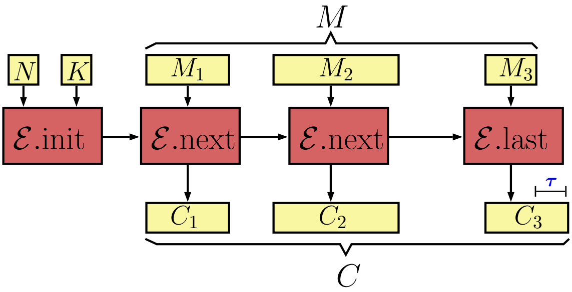
Beyond Attacks

- **What about online decryption?**
  - Online encryption necessary due to constraints; don't these apply to decryption as well?
- **What about arbitrary length string?**
  - Must be processed in reality, security must be defined for **all** inputs!
- **Why should the blocksize n be determined by the designer?**
  - Online processing necessary due to resource constraints; the user should be able to select the blocksize according to its resources!

⇒ **Why refer to an online cipher followed by a random tag? Is this ideal?**
  - We can make better!

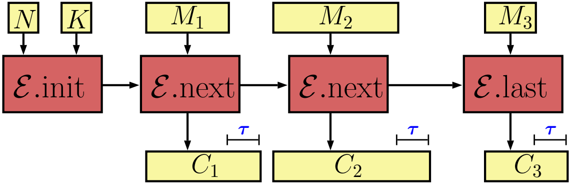
Key Ideas

- User selectable segmentation
  - Possibly non-uniform segments
  - Arbitrary segment length



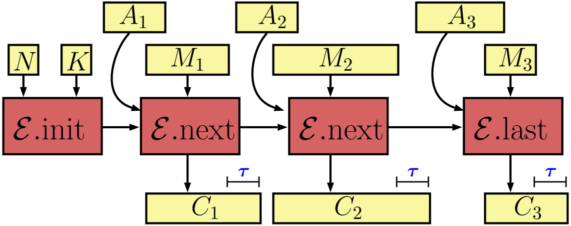
Key Ideas

- User selectable segmentation
  - Possibly non-uniform segments
  - Arbitrary segment length
- Expand *every block*

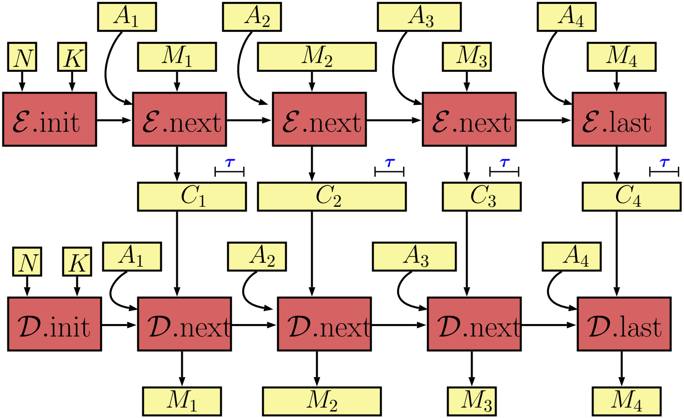


Key Ideas

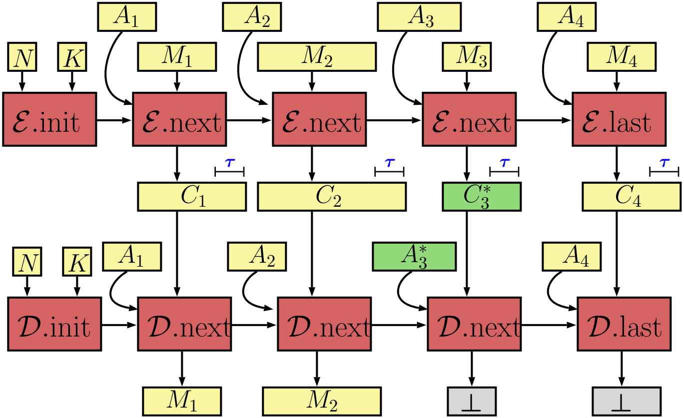
- User selectable segmentation
  - Possibly non-uniform segments
  - Arbitrary segment length
- Expand *every block*
- Segment AD as well



Unforgeability

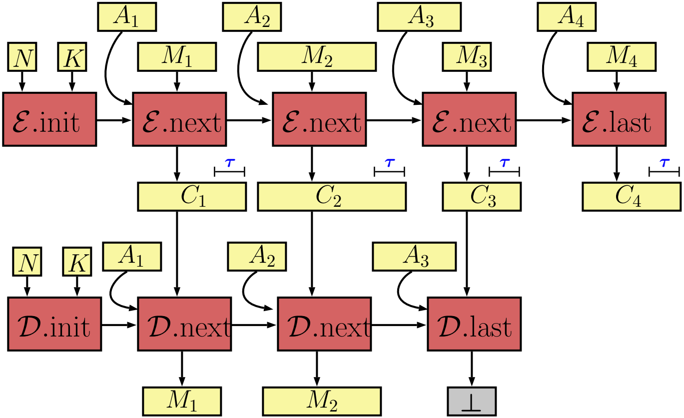


Unforgeability



Online decryption returns nothing after first authentication failure

Unforgeability



Obtaining $(A, B, C, D) \xrightarrow{\mathcal{E}_K} (W, X, Y, Z)$ should not allow
$(W, X, Y) \xrightarrow{\mathcal{D}_K} (A, B, C)$!

OAE2

Syntax

An OAE2 scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

- $\rightarrow$ $\mathcal{K}$ a distribution on strings
- $\rightarrow$ $\mathcal{E} = (\mathcal{E}.\text{init}, \mathcal{E}.\text{next}, \mathcal{E}.\text{last})$ 3 deterministic algorithms
- $\rightarrow$ $\mathcal{D} = (\mathcal{D}.\text{init}, \mathcal{D}.\text{next}, \mathcal{D}.\text{last})$ 3 deterministic algorithms

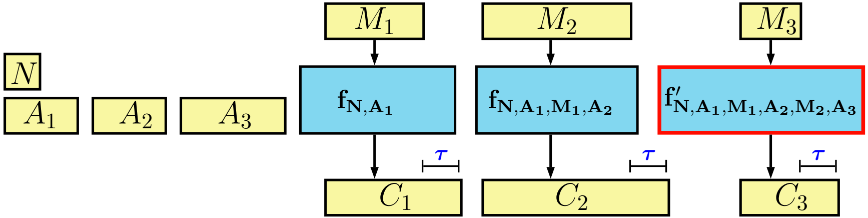
- $\mathcal{E}.\text{init} : \mathcal{K} \times \mathcal{N} \rightarrow \mathcal{S}$
- $\mathcal{E}.\text{next} : \mathcal{S} \times \mathcal{A} \times \mathcal{M} \rightarrow \mathcal{C} \times \mathcal{S}$
- $\mathcal{E}.\text{last} : \mathcal{S} \times \mathcal{A} \times \mathcal{M} \rightarrow \mathcal{C}$

- $\mathcal{D}.\text{init} : \mathcal{K} \times \mathcal{N} \rightarrow \mathcal{S}$
- $\mathcal{D}.\text{next} : \mathcal{S} \times \mathcal{A} \times \mathcal{C} \rightarrow (\mathcal{M} \times \mathcal{S}) \cup \{\perp\}$
- $\mathcal{D}.\text{last} : \mathcal{S} \times \mathcal{A} \times \mathcal{C} \rightarrow \mathcal{M} \cup \{\perp\}$

$\Rightarrow$ Π “online” if $|\mathcal{S}|$ is finite and representation fits in memory

OAE2

Ideal Reference



$\mathbf{f}_{\langle\cdot\rangle} : \{\mathbf{0},\mathbf{1}\}^* \rightarrow \{\mathbf{0},\mathbf{1}\}^*$ is a τ expanding random injection tweaked by everything in $\langle\cdot\rangle$

OAE2

Ideal Reference

Formally $F \leftarrow\!\!\$\ \mathrm{IdealOAE}(\tau)$ means

$$
\begin{array}{l}
\textbf{for } m \in \mathbb{Z}^+,\ N \in \{0,1\}^*,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{M} \in (\{0,1\}^*)^{m-1} \textbf{ do} \\
\quad f_{N,\boldsymbol{A},\boldsymbol{M},0} \leftarrow\!\!\$\ \textbf{Inj}(\tau);\quad f_{N,\boldsymbol{A},\boldsymbol{M},1} \leftarrow\!\!\$\ \textbf{Inj}(\tau) \\
\\
\textbf{for } m \in \mathbb{Z}^+,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{X} \in (\{0,1\}^*)^m,\ \delta \in \{0,1\} \textbf{ do} \\
\quad F(N,\boldsymbol{A},\boldsymbol{X},\delta) \leftarrow (f_{N,\boldsymbol{A}[1..1],\Lambda,0}(\boldsymbol{X}[1]),\ f_{N,\boldsymbol{A}[1..2],\boldsymbol{X}[1..1],0}(\boldsymbol{X}[2]), \\
\qquad\qquad f_{N,\boldsymbol{A}[1..3],\boldsymbol{X}[1..2],0}(\boldsymbol{X}[3]),\ \ldots,\ f_{N,\boldsymbol{A}[1..m-1],\boldsymbol{X}[1..m-2],0}(\boldsymbol{X}[m-1]), \\
\qquad\qquad f_{N,\boldsymbol{A}[1..m],\boldsymbol{X}[1..m-1],\delta}(\boldsymbol{X}[m])) \\
\textbf{return } F
\end{array}
$$

where

- $(\{0,1\}^*)^m$ is the set of all lists of m strings
- Λ is an empty list,
- $\mathbf{X}[i]$ is i^{th} string, $\mathbf{X}[i..j]$ is a sublist

OAE2

Ideal Reference

Formally $F \leftarrow\$ \mathrm{IdealOAE}(\tau)$ means

$$
\begin{array}{l}
\textbf{for } m \in \mathbb{Z}^+,\ N \in \{0,1\}^*,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{M} \in (\{0,1\}^*)^{m-1} \textbf{ do} \\
\quad f_{N,\boldsymbol{A},\boldsymbol{M},0} \leftarrow\$\ \mathbf{Inj}(\tau);\quad f_{N,\boldsymbol{A},\boldsymbol{M},1} \leftarrow\$\ \mathbf{Inj}(\tau) \\
\\
\textbf{for } m \in \mathbb{Z}^+,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{X} \in (\{0,1\}^*)^m,\ \delta \in \{0,1\} \textbf{ do} \\
\quad F(N,\boldsymbol{A},\boldsymbol{X},\delta) \leftarrow (f_{N,\boldsymbol{A}[1..1],\Lambda,0}(\boldsymbol{X}[1]),\ f_{N,\boldsymbol{A}[1..2],\boldsymbol{X}[1..1],0}(\boldsymbol{X}[2]), \\
\qquad\qquad f_{N,\boldsymbol{A}[1..3],\boldsymbol{X}[1..2],0}(\boldsymbol{X}[3]),\ \ldots,\ f_{N,\boldsymbol{A}[1..m-1],\boldsymbol{X}[1..m-2],0}(\boldsymbol{X}[m-1]), \\
\qquad\qquad f_{N,\boldsymbol{A}[1..m],\boldsymbol{X}[1..m-1],\delta}(\boldsymbol{X}[m])) \\
\textbf{return } F
\end{array}
$$

where

- $(\{0,1\}^*)^m$ is the set of all lists of m strings
- Λ is an empty list,
- $\mathbf{X}[i]$ is i^{th} string, $\mathbf{X}[i..j]$ is a sublist

OAE2

Ideal Reference

Formally $F \leftarrow\!\$\ \mathrm{IdealOAE}(\tau)$ means

$$
\begin{array}{l}
\textbf{for } m \in \mathbb{Z}^+,\ N \in \{0,1\}^*,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{M} \in (\{0,1\}^*)^{m-1} \textbf{ do} \\
\quad f_{N,\boldsymbol{A},\boldsymbol{M},0} \leftarrow\!\$\ \mathbf{Inj}(\tau);\quad f_{N,\boldsymbol{A},\boldsymbol{M},1} \leftarrow\!\$\ \mathbf{Inj}(\tau) \\
\\
\textbf{for } m \in \mathbb{Z}^+,\ \boldsymbol{A} \in (\{0,1\}^*)^m,\ \boldsymbol{X} \in (\{0,1\}^*)^m,\ \delta \in \{0,1\} \textbf{ do} \\
\quad F(N,\boldsymbol{A},\boldsymbol{X},\delta) \leftarrow (f_{N,\boldsymbol{A}[1..1],\Lambda,0}(\boldsymbol{X}[1]),\ f_{N,\boldsymbol{A}[1..2],\boldsymbol{X}[1..1],0}(\boldsymbol{X}[2]), \\
\qquad\qquad f_{N,\boldsymbol{A}[1..3],\boldsymbol{X}[1..2],0}(\boldsymbol{X}[3]),\ \ldots,\ f_{N,\boldsymbol{A}[1..m-1],\boldsymbol{X}[1..m-2],0}(\boldsymbol{X}[m-1]), \\
\qquad\qquad f_{N,\boldsymbol{A}[1..m],\boldsymbol{X}[1..m-1],\delta}(\boldsymbol{X}[m])) \\
\textbf{return } F
\end{array}
$$

where

- $(\{0,1\}^*)^m$ is the set of all lists of m strings
- Λ is an empty list,
- $\mathbf{X}[i]$ is i^{th} string, $\mathbf{X}[i..j]$ is a sublist

OAE2

The Definitions

Three definitions that are $\approx$*equivalent*:

$\rightarrow$ Different approaches $\rightarrow$ Clarify the quantitative relationship

- **OAE2a** Simplest definition, succinctly captures *best possible* security of online AE schemes
  - Adversary submits and receives segmented strings
- **OAE2b** Captures the capabilities of an adversary more realistically
  - Adversary can submit queries segment-by-segment, immediately observing the outputs
- **OAE2c** *Aspirational* notion, captures ideal, albeit unachievable security
  - Separates privacy and authenticity
  - nAEAD-like privacy

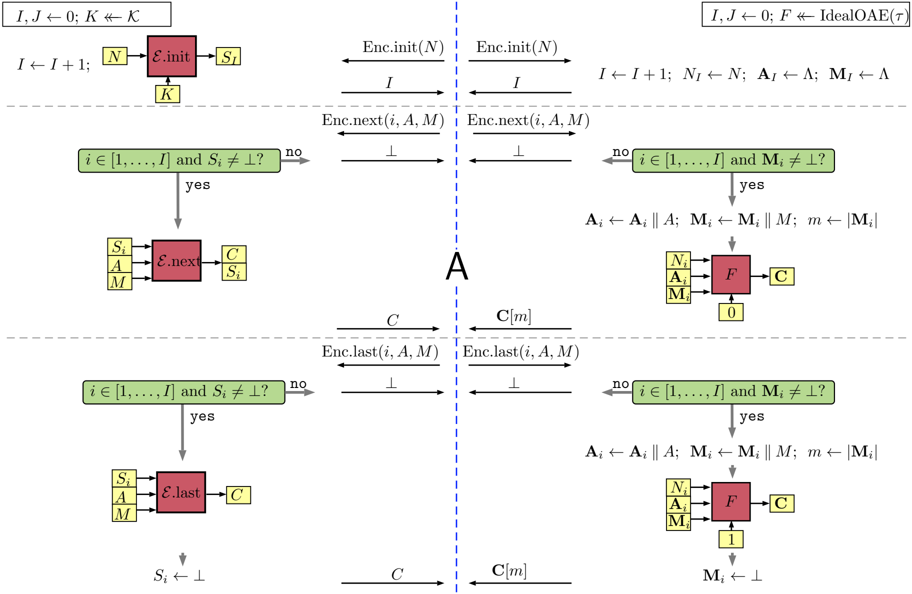
OAE2

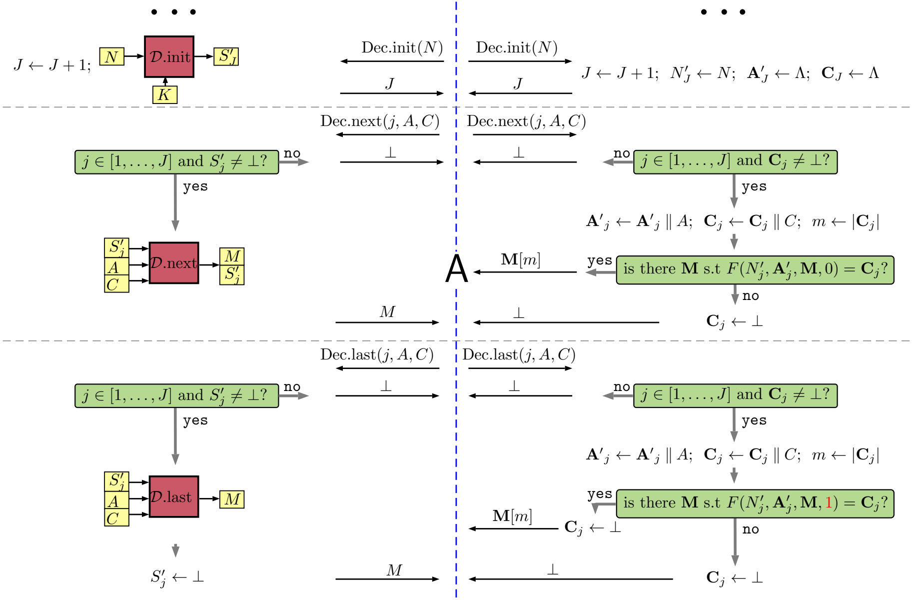
The Definitions

Three definitions that are $\approx$*equivalent*:

$\rightarrow$ Different approaches $\rightarrow$ Clarify the quantitative relationship

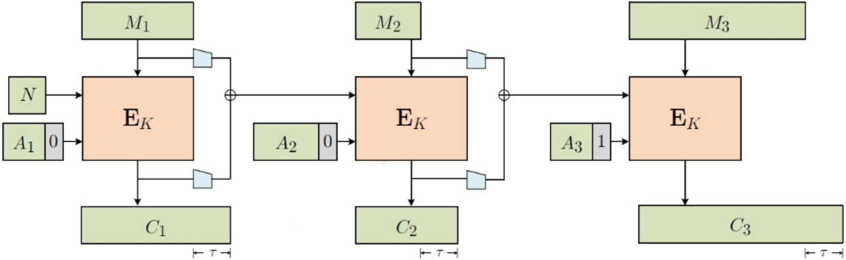
- **OAE2a** Simplest definition, succinctly captures *best possible* security of online AE schemes **Presented at CRYPTO2015**
  - Adversary submits and receives segmented strings
- **OAE2b** Captures the capabilities of an adversary more realistically
  - Adversary can submit queries segment-by-segment, immediately observing the outputs
- **OAE2c** *Aspirational* notion, captures ideal, albeit unachievable security
  - Separates privacy and authenticity
  - nAEAD-like privacy


$I, J \leftarrow 0;\ K \twoheadleftarrow \mathcal{K}$
$I \leftarrow I+1;$
N
$\mathcal{E}$.init
S_I
K
Enc.init(N)
I
Enc.init(N)
I
$I, J \leftarrow 0;\ F \twoheadleftarrow \mathrm{IdealOAE}(\tau)$
$I \leftarrow I+1;\ N_I \leftarrow N;\ \mathbf{A}_I \leftarrow \Lambda;\ \mathbf{M}_I \leftarrow \Lambda$
Enc.next(i, A, M)
$\perp$
Enc.next(i, A, M)
$\perp$
$i \in [1, \ldots, I]$ and $S_i \neq \perp$?
no
yes
S_i
A
M
$\mathcal{E}$.next
C
S_i
A
C
$\mathbf{C}[m]$
no
$i \in [1, \ldots, I]$ and $\mathbf{M}_i \neq \perp$?
yes
$\mathbf{A}_i \leftarrow \mathbf{A}_i \parallel A;\ \mathbf{M}_i \leftarrow \mathbf{M}_i \parallel M;\ m \leftarrow |\mathbf{M}_i|$
N_i
$\mathbf{A}_i$
$\mathbf{M}_i$
F
$\mathbf{C}$
0
Enc.last(i, A, M)
$\perp$
Enc.last(i, A, M)
$\perp$
$i \in [1, \ldots, I]$ and $S_i \neq \perp$?
no
yes
S_i
A
M
$\mathcal{E}$.last
C
$S_i \leftarrow \perp$
C
$\mathbf{C}[m]$
no
$i \in [1, \ldots, I]$ and $\mathbf{M}_i \neq \perp$?
yes
$\mathbf{A}_i \leftarrow \mathbf{A}_i \parallel A;\ \mathbf{M}_i \leftarrow \mathbf{M}_i \parallel M;\ m \leftarrow |\mathbf{M}_i|$
N_i
$\mathbf{A}_i$
$\mathbf{M}_i$
F
$\mathbf{C}$
1
$\mathbf{M}_i \leftarrow \perp$



$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2}}(\boldsymbol{A}) = \Pr[\boldsymbol{A}^{\mathrm{OAE2bReal}} \Rightarrow 1] - \Pr[\boldsymbol{A}^{\mathrm{OAE2bIdeal}} \Rightarrow 1]$$

Achieving OAE2: the CHAIN construction



Use a τ-expanding PRI in place of $\mathbf{E}_K$

- For large τ (e.g. 128 bits) MRAE can be used!
- For general τ use RAE

Conclusions, Remarks

- Online AE isn't just blockwise *encryption* that preserves prefix!
  - Online decryption as important as online encryption
  - Segment size should suit the user, not designer
- Even for OAE2, CPSS still applies
  - Best possible defense far from comfortable
  - Must insist on using nonces (vs header only schemes)
- Other variants possible
  - Different expansion for last segment
  - Give up nonce misuse-resistance (**nOAE,dOAE**)
- Arbitrary segmentation: a tool, **not** expected capability of channel
  - E.g. *arbitrary* but *constant* to prevent decryption leakage

Questions?

Thank you for your attention!

OAE2a

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 $\boldsymbol{\mathcal{E}}(K, N, \boldsymbol{A}, \boldsymbol{M})$

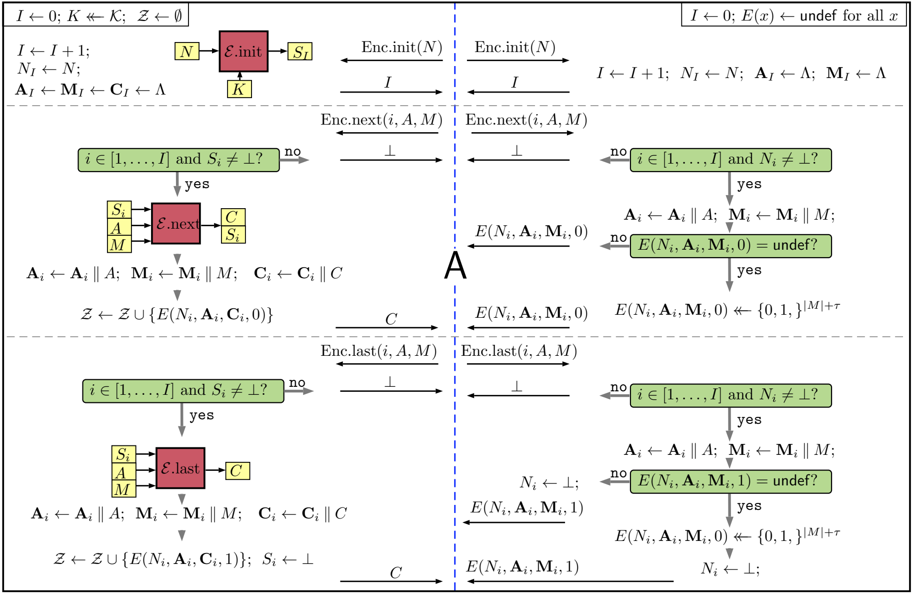
proc Dec$(N, \boldsymbol{A}, \boldsymbol{C})$
if $N \notin \mathcal{N}$ **or** $|\boldsymbol{A}| \neq |\boldsymbol{M}|$ **then return** $\perp$
return $\boldsymbol{\mathcal{D}}(K, N, \boldsymbol{A}, \boldsymbol{C})$

proc initialize
$F \twoheadleftarrow$ IdealOAE(τ)

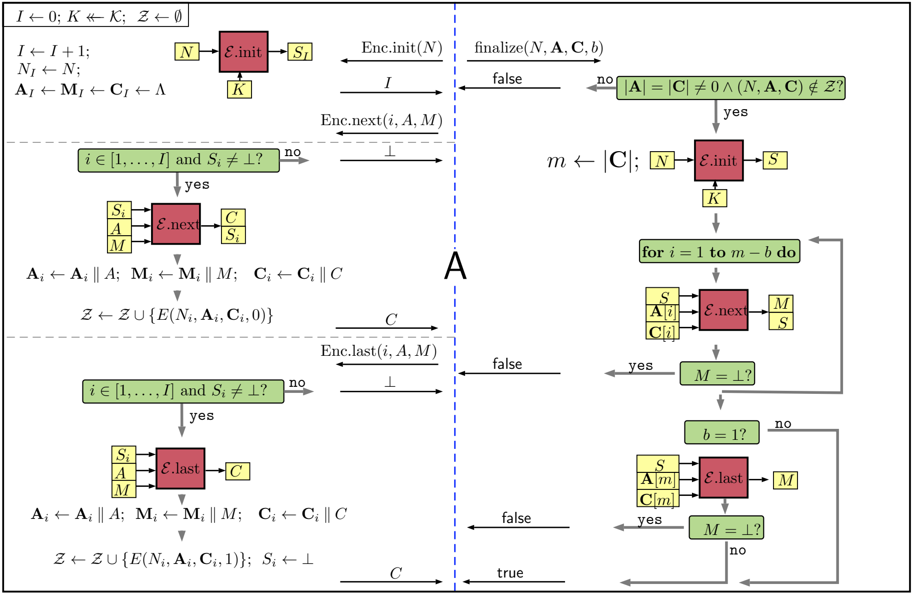
proc Enc$(N, \boldsymbol{A}, \boldsymbol{M})$
if $N \notin \mathcal{N}$ **or** $|\boldsymbol{A}| \neq |\boldsymbol{M}$ **then return** $\perp$
return $F(N, \boldsymbol{A}, \boldsymbol{M}, 1)$

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 $\boldsymbol{M}$

$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2a}}(\boldsymbol{A}) = \Pr[\boldsymbol{A}^{OAE2a-real} \Rightarrow 1] - \Pr[\boldsymbol{A}^{OAE2a-ideal} \Rightarrow 1]$$



$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2}}(\boldsymbol{A}) = \Pr[\boldsymbol{A}^{\mathrm{OAE2cReal}} \Rightarrow 1] - \Pr[\boldsymbol{A}^{\mathrm{OAE2cIdeal}} \Rightarrow 1]$$



$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2}}(\boldsymbol{A}) = \Pr[\boldsymbol{A}^{\mathrm{OAE2cForge}} \Rightarrow \texttt{true}]$$

Relations between OAE2a, OAE2b and OAE2c

$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2b}}(\boldsymbol{A}_1) \leq \mathbf{Adv}_{\Pi}^{\mathrm{OAE2c-priv}}(\boldsymbol{B}_{1,1}) + p \cdot \mathbf{Adv}_{\Pi}^{\mathrm{OAE2c-auth}}(\boldsymbol{B}_{1,2}) + \frac{q^2}{2^\tau}$$

p number of Dec chains, q total number of queries of $\boldsymbol{A}_1$; $\boldsymbol{A}_1, \boldsymbol{B}_{1,1}, \boldsymbol{B}_{1,2}$ use ≈same resources

$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2c-priv}}(\boldsymbol{A}_{2,1}) \leq \mathbf{Adv}_{\Pi}^{\mathrm{OAE2b}}(\boldsymbol{B}_{2,1}) + \frac{q^2}{2^\tau}$$

$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2c-auth}}(\boldsymbol{A}_{2,2}) \leq \mathbf{Adv}_{\Pi}^{\mathrm{OAE2b}}(\boldsymbol{B}_{2,2}) + \frac{\ell}{2^\tau}$$

q number of $\boldsymbol{A}_{2,1}$'s queries, ℓ number of segments in $\boldsymbol{A}_{2,2}$'s output. $\boldsymbol{A}_{2,1}$ and $\boldsymbol{B}_{2,1}$ use ≈same resources (same for $\boldsymbol{A}_{2,2}$ and $\boldsymbol{B}_{2,2}$)

$$\mathbf{Adv}_{\Pi}^{\mathrm{OAE2a}}(\boldsymbol{A}_{3,1}) \leq \mathbf{Adv}_{\Pi}^{\mathrm{OAE2b}}(\boldsymbol{B}_{3,1}) \qquad \mathbf{Adv}_{\Pi}^{\mathrm{OAE2b}}(\boldsymbol{B}_{3,2}) \leq \mathbf{Adv}_{\Pi}^{\mathrm{OAE2a}}(\boldsymbol{A}_{3,2})$$

$\boldsymbol{A}_{3,1}$ and $\boldsymbol{B}_{3,1}$ use ≈same resources, but running time and number of queries of $\boldsymbol{A}_{3,2}$ is increased quadratically compared to $\boldsymbol{A}_{3,2}$