Reconsidering Generic Composition: the Tag-then-Encrypt case

Francesco Berti, Olivier Pereira and Thomas Peters

ICTEAM/ELEN/Crypto Group, Université catholique de Louvain,
Louvain-la-neuve, Belgium

Objective

Obtain an Authenticated Encryption (AE) scheme composing:

- Encryption scheme
  - IV-based (ivE)
  - nonce-based (nE)
- PRF-MAC

Problem Distinguish secure from insecure combinations.

Objective

Obtain an Authenticated Encryption (AE) scheme composing:

- Encryption scheme
  - IV-based (ivE)
  - nonce-based (nE)
- PRF-MAC

Problem Distinguish secure from insecure combinations.

Objective

Obtain an Authenticated Encryption (AE) scheme composing:

- Encryption scheme
  - IV-based (ivE)
  - nonce-based (nE)
- PRF-MAC

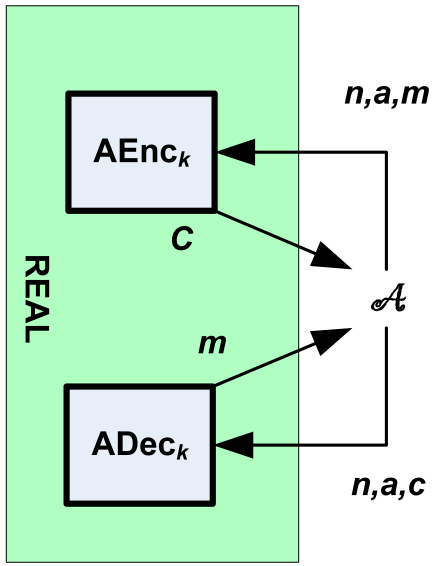
Problem Distinguish secure from insecure combinations.
NRS did most of the job (Eurocrypt 2014)
(160 [ivE] + 20 [nE] possible, 9 + 3 secure)
3+1 elusive in the Tag-then-Encrypt case

Outline

- Background
- Problem
- Results
- Attack on N4

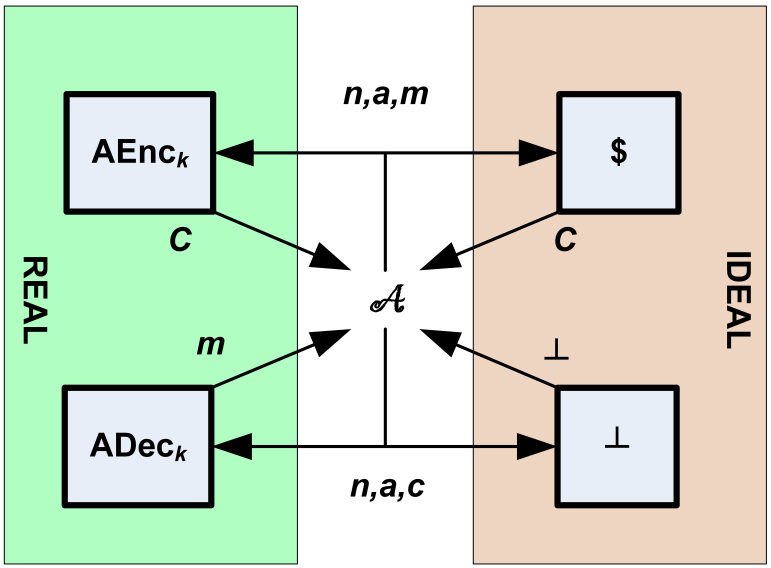
Authenticated Encryption

Objective: Provide privacy and authenticity to a message and associated data (AD) with scheme $\Pi = (\mathcal{K}, \mathrm{AEnc}, \mathrm{ADec})$



Authenticated Encryption

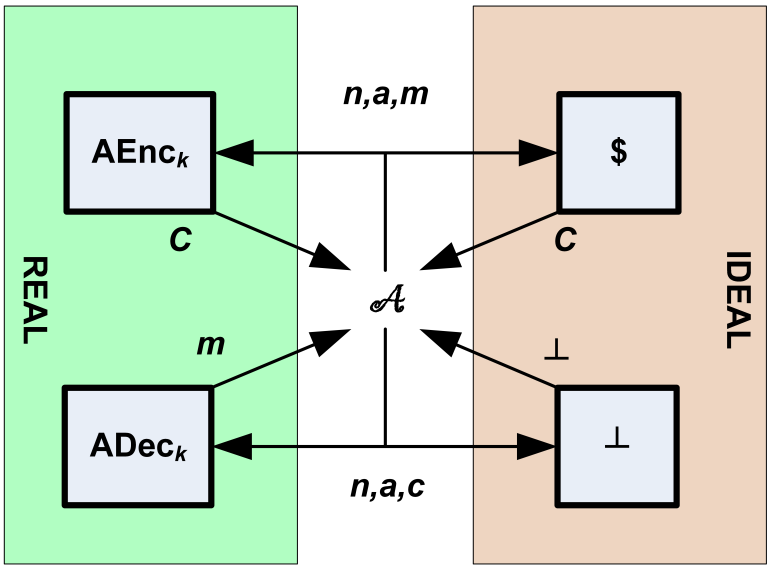
Objective: Provide privacy and authenticity to a message and associated data (AD) with scheme $\Pi = (\mathcal{K}, \text{AEnc}, \text{ADec})$



Real and Ideal should be indistinguishable. (nAE)
Not repeat n, if $c \leftarrow \text{AEnc}_k(n, a, m)$ not ask $\text{ADec}_k(n, a, c)$

Authenticated Encryption

Objective: Provide privacy and authenticity to a message and associated data (AD) with scheme $\Pi = (\mathcal{K}, \mathrm{AEnc}, \mathrm{ADec})$

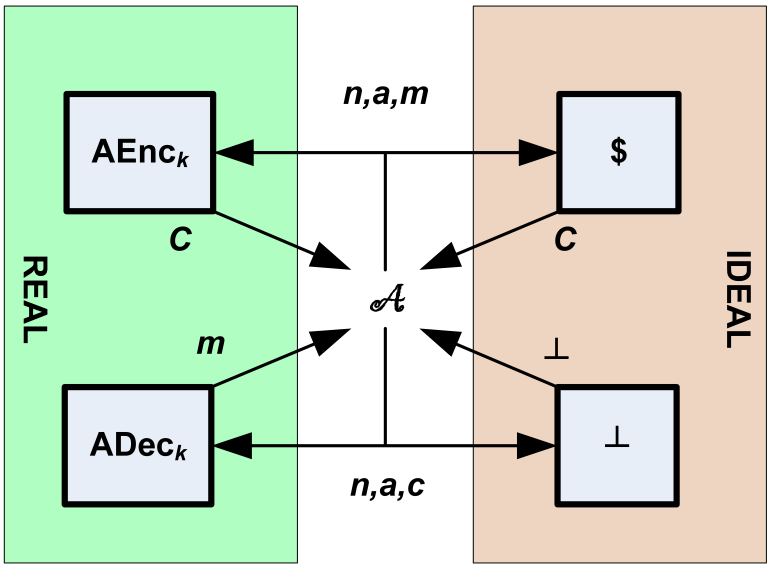


Correctness + Tidiness

$\mathrm{AEnc}_k^{n,a}(m) = c \Leftrightarrow \mathrm{ADec}_k^{n,a}(c) = m$ (Tidiness $\Leftarrow$)

Authenticated Encryption

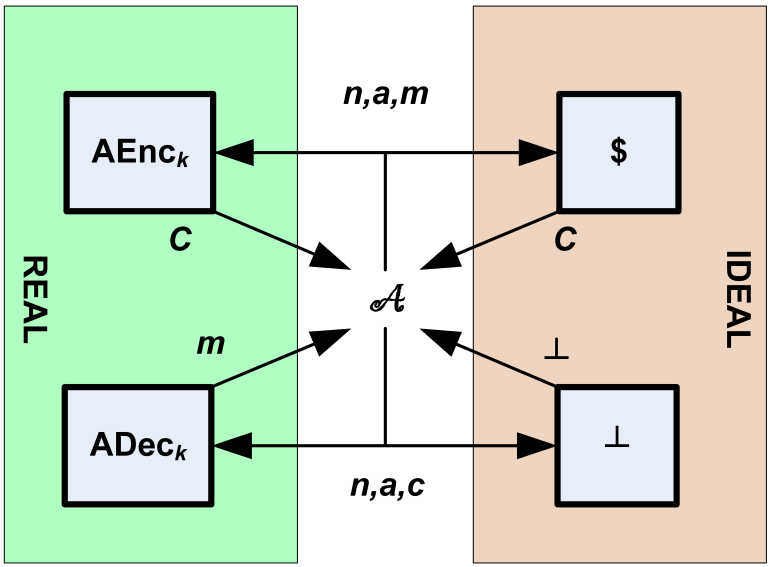
Objective: Provide privacy and authenticity to a message and associated data (AD) with scheme $\Pi = (\mathcal{K}, \text{AEnc}, \text{ADec})$



Privacy (nAE-E)
AEnc indistinguishable from \$.

Authenticated Encryption

Objective: Provide privacy and authenticity to a message and associated data (AD) with scheme $\Pi = (\mathcal{K}, \text{AEnc}, \text{ADec})$

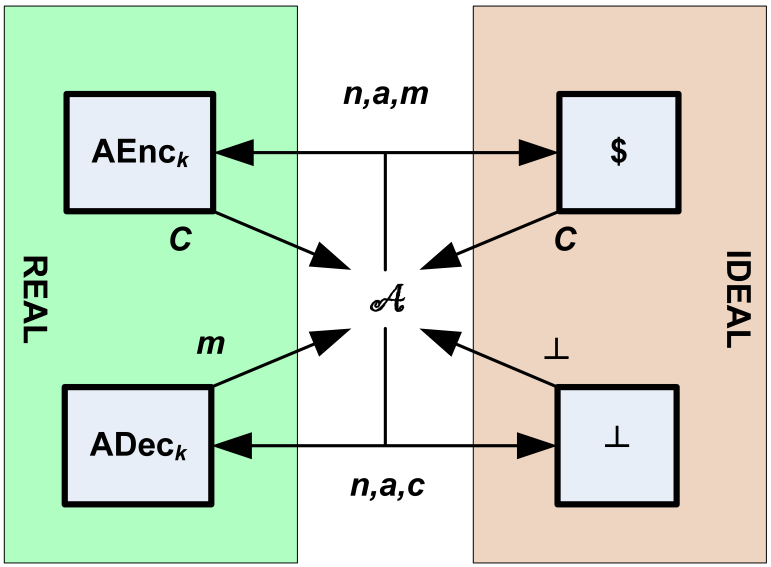


Authenticity

Difficult to provide a *valid and fresh* ciphertext c.

Authenticated Encryption

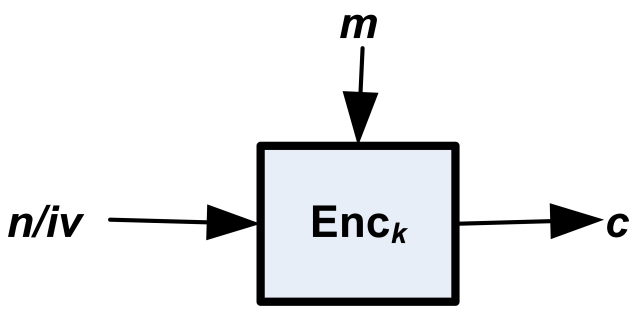
Objective: Provide privacy and authenticity to a message and associated data (AD) with scheme $\Pi = (\mathcal{K}, \mathrm{AEnc}, \mathrm{ADec})$



Privacy + **Authenticity** = nAE.

Encryption schemes

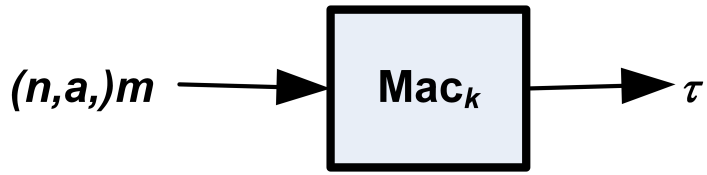
Scheme $\Pi = (\mathcal{K}_E, \mathrm{Enc}, \mathrm{Dec})$:



c should be **indistinguishable** from random

- if *n* is not repeated (nonce) [nE]
- if *iv* is picked randomly (iv) [ivE]

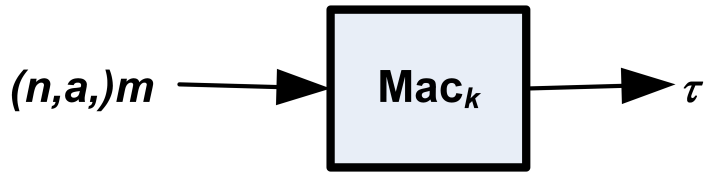
(PRF)-MAC



Security:

- τ should be *indistinguishable* from random (PRF-**security**)

(PRF)-MAC



Security:

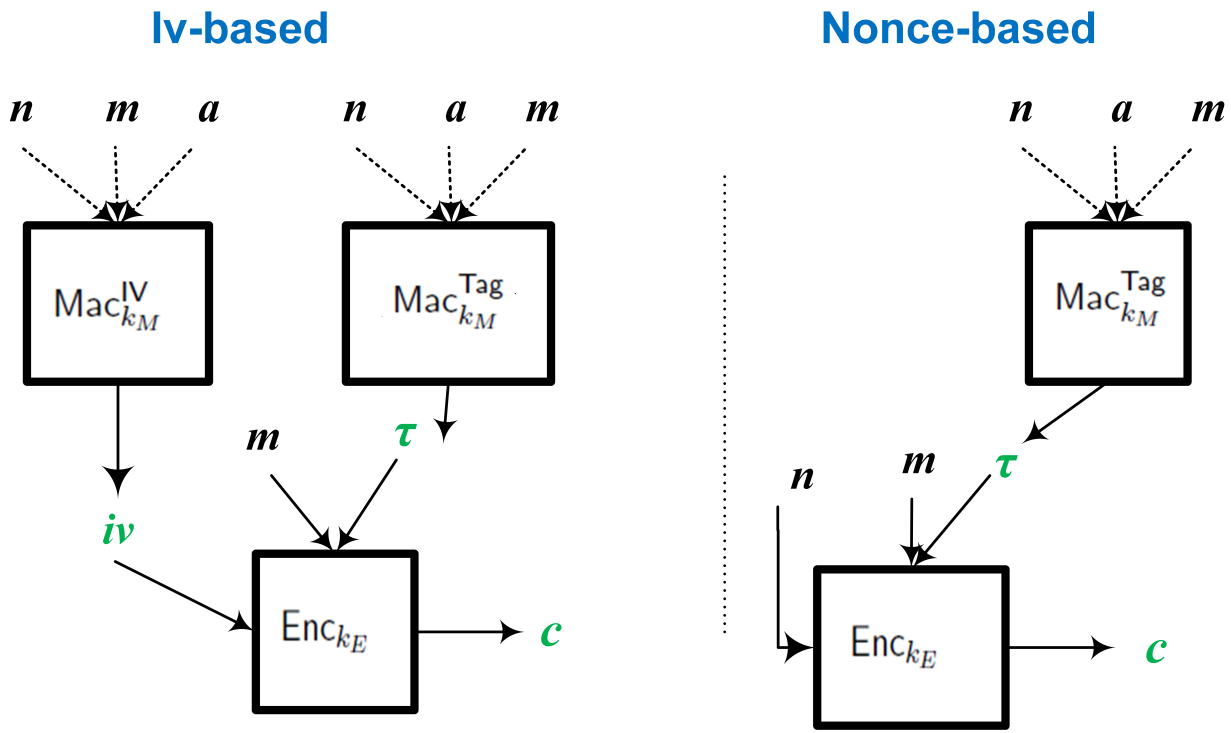
- τ should be *indistinguishable* from random (PRF-**security**)

PRF-**security** $\Rightarrow$ (**unforgeability**)

hard to find a fresh valid tag τ

Composition

Many possible ways:
MAC-then-Enc (other Enc-then-MAC and Enc-and-MAC)



Outline

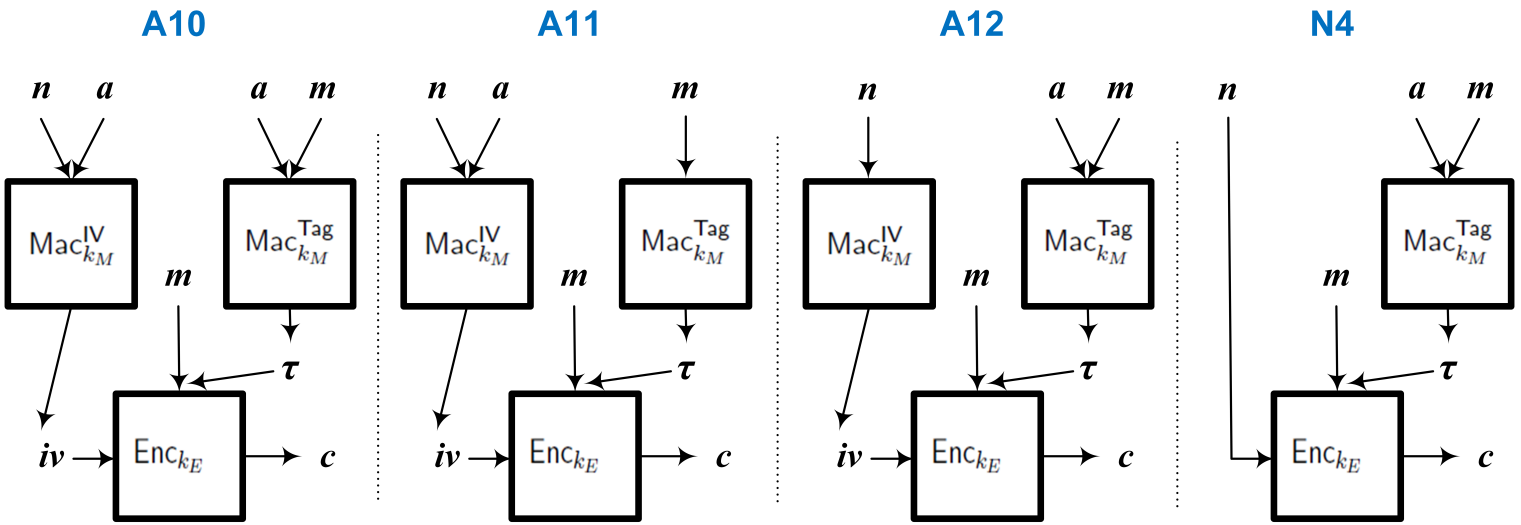
- Background
- *Problem*
- Results
- Attack on N4

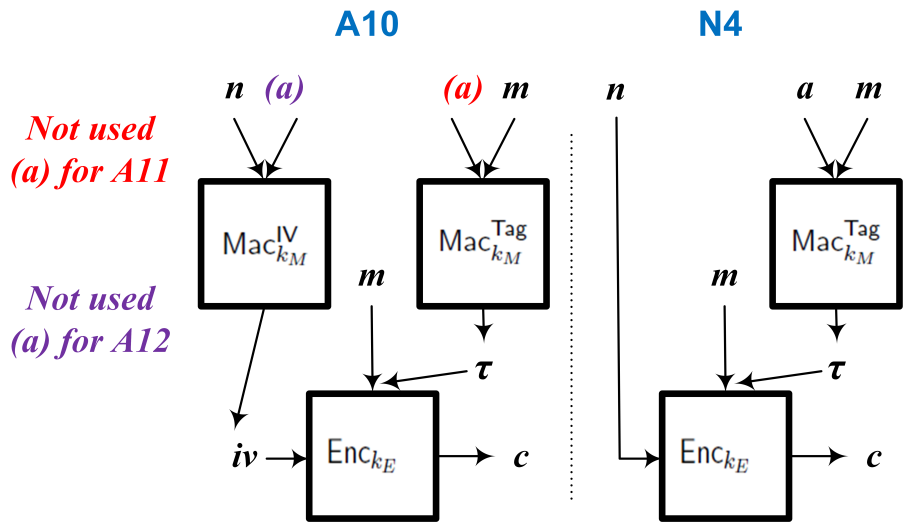
Problem

NRS14 left 3 ivE and 1 nE elusive schemes

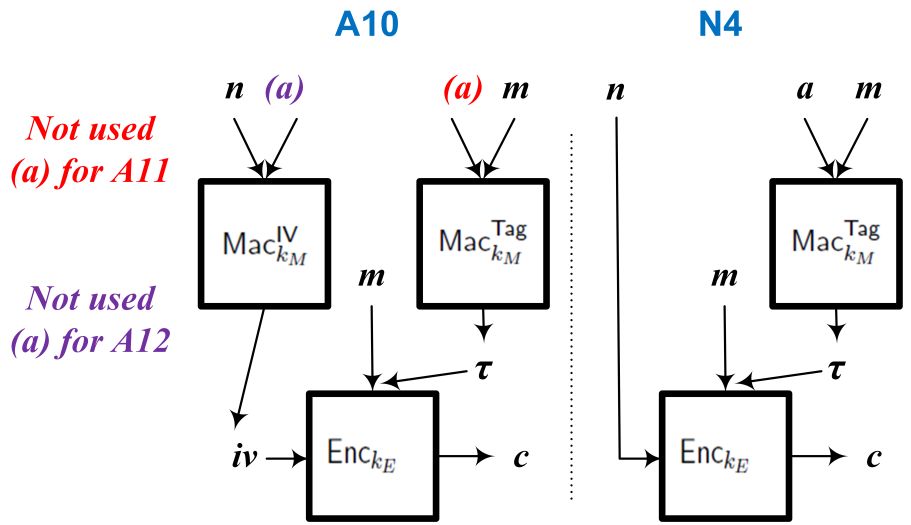
Problem

NRS14 left 3 ivE and 1 nE elusive schemes





Privacy nAE-E is easy to prove.
Unforgeability Difficult to produce a *valid and fresh* (n, a, c)



Privacy nAE-E is easy to prove.
Unforgeability Difficult to produce a *valid and fresh* (n, a, c)

- c is (pseudo)random
- if the iv or the tag τ are fresh then it is unforgeable

Problem When iv and τ are not fresh, it may be used to forge a fresh valid c

Outline

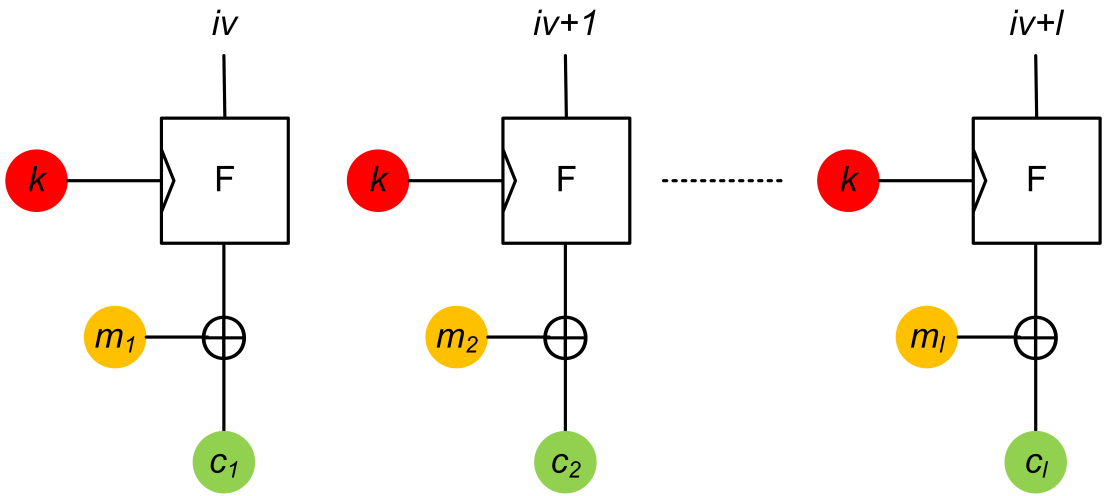
- Background
- Problem
- *Results*
- Attack on N4

Results

- A10, A11, A12 are either all secure or insecure
- A10, A11, A12 are secure if
  - Enc is “message-malleable”
  - Enc is “misuse-resistant”
- A10, A11, A12 are insecure if
  - Enc is stateful
  - Enc is not tidy
- N4 is insecure

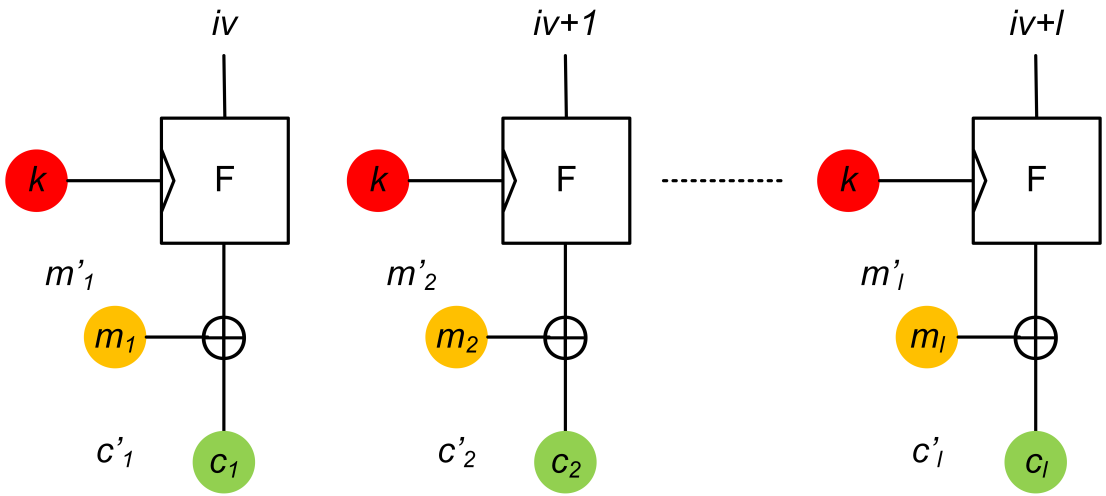
A10 with Message malleability

A10 is secure if ivE is message malleable. Example CTR



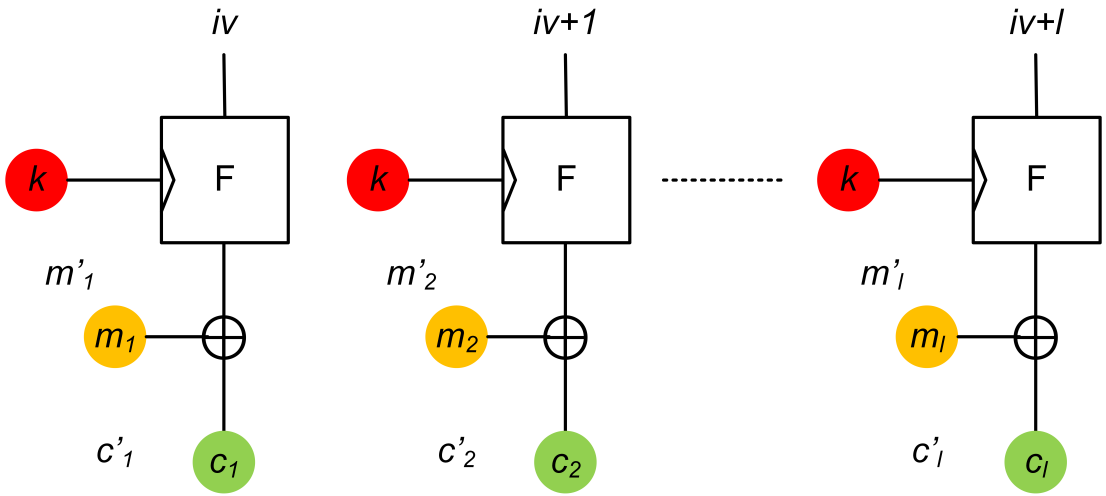
A10 with Message malleability

A10 is secure if ivE is message malleable. Example CTR



A10 with Message malleability

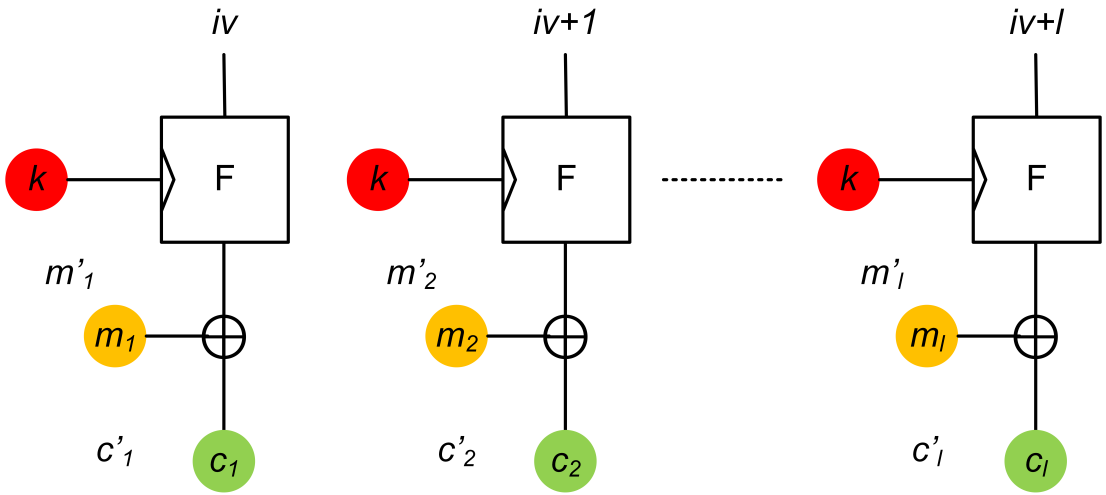
A10 is secure if ivE is message malleable. Example CTR



$$c' = c \oplus m \oplus m'$$

A10 with Message malleability

A10 is secure if ivE is message malleable. Example CTR



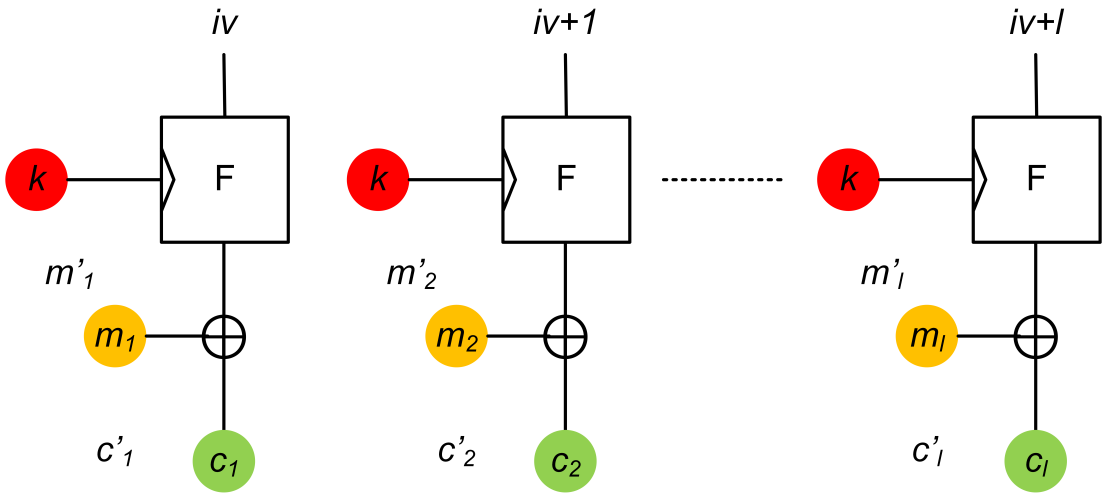
$c' = c \oplus m \oplus m'$

A10 is secure if ivE is implemented with CTR.

Idea: an adversary vs CTR may distinguish valid from invalid ciphertexts.

A10 with Message malleability

A10 is secure if ivE is message malleable. Example CTR



$c' = c \oplus m \oplus m'$

A10 is secure if ivE is implemented with CTR.

Idea: an adversary vs CTR may distinguish valid from invalid ciphertexts.

Rember the only possible forgery is with iv and τ repeated.

Message-malleability

We can generalize:

Message-malleability

We can generalize:

Definition

An ivE scheme is *message malleable* if given (iv, m, c) with $c \leftarrow \mathrm{Enc}^{iv}(m)$ then
$\forall c'$ an adversary can compute $m' \leftarrow \mathrm{Dec}^{iv}(c')$.

Message-malleability

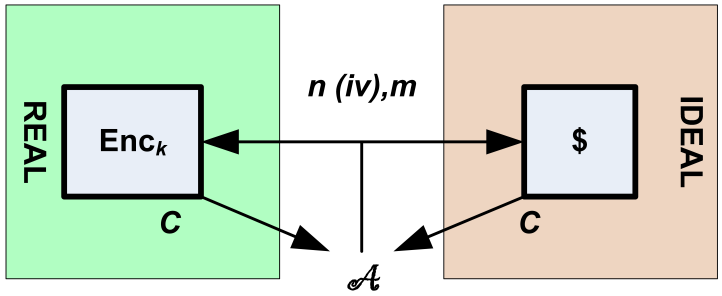
We can generalize:

Definition

An ivE scheme is *message malleable* if given (iv, m, c) with $c \leftarrow \mathrm{Enc}^{iv}(m)$ then
$\forall c'$ an adversary can compute $m' \leftarrow \mathrm{Dec}^{iv}(c')$.

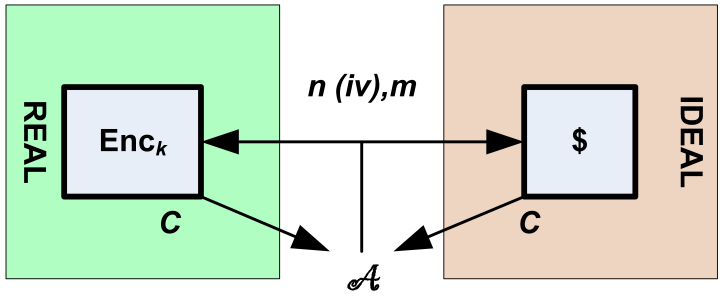
If ivE is message malleable then A10 is secure.

Misuse-resistant



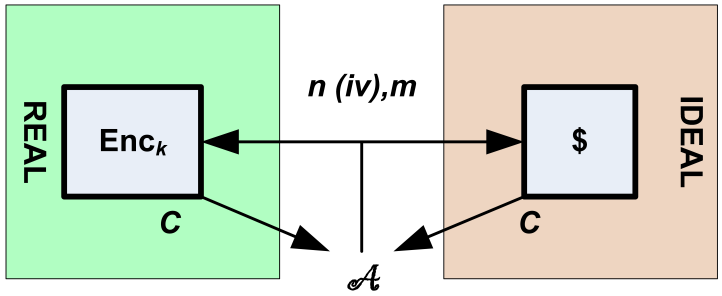
Indistinguishable even if n (or iv) is repeated.

Misuse-resistant



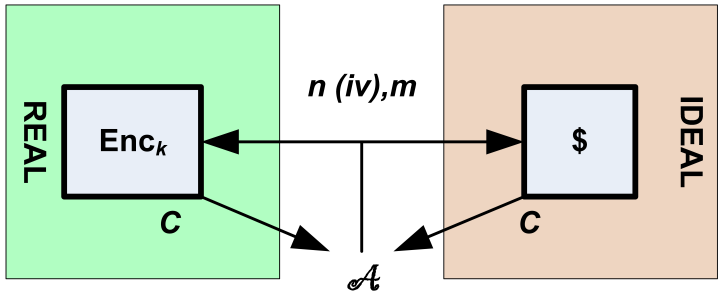
Indistinguishable even if n (or iv) is repeated. In such a case A10 is secure.

Misuse-resistant

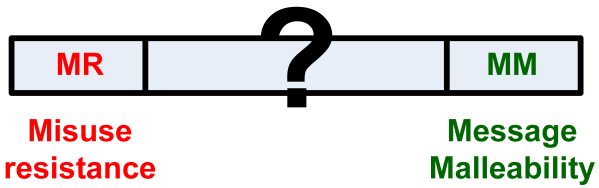


Indistinguishable even if n (or iv) is repeated. In such a case A10 is secure.
Interestingly message malleability and nonce-misuse are opposite.

Misuse-resistant



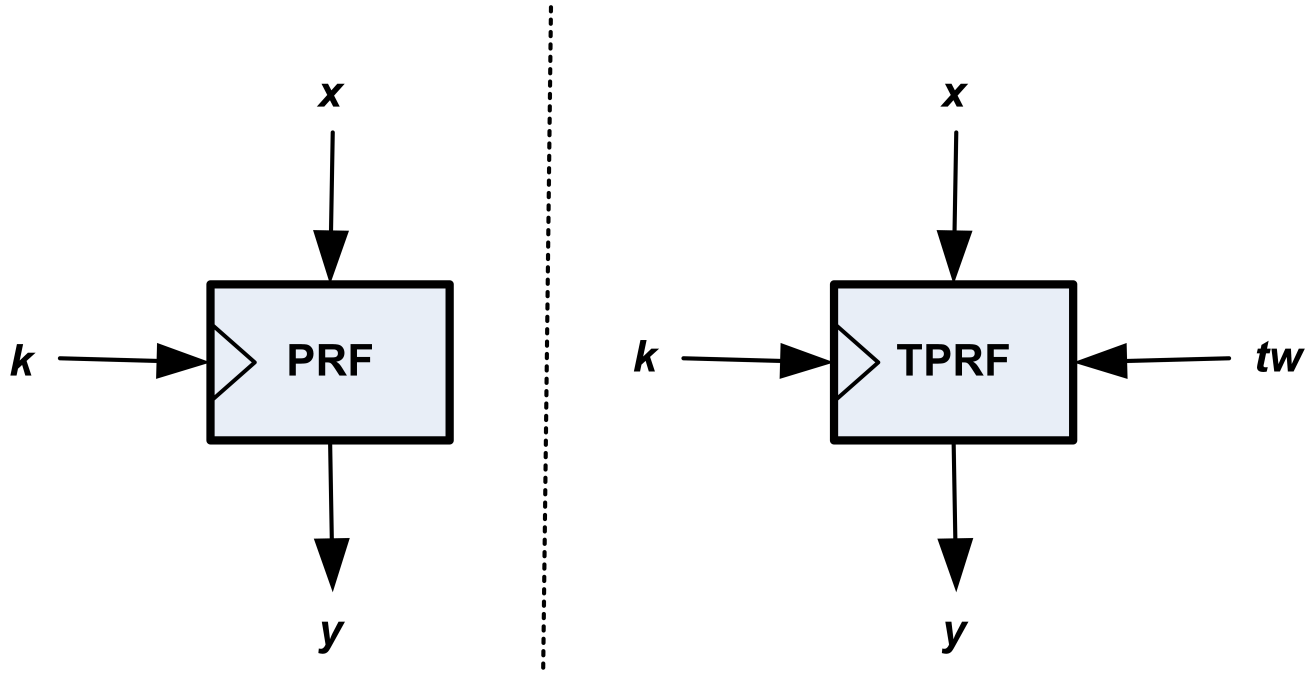
Indistinguishable even if n (or iv) is repeated. In such a case A10 is secure.
Interestingly message malleability and nonce-misuse are opposite.



Outline

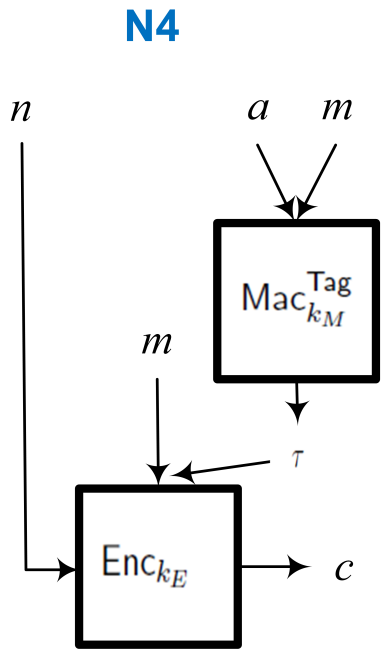
- Background
- Problem
- Results
- *Attack vs N4*
  - PRF and TPRF
  - Attack.

PRF / TPRF



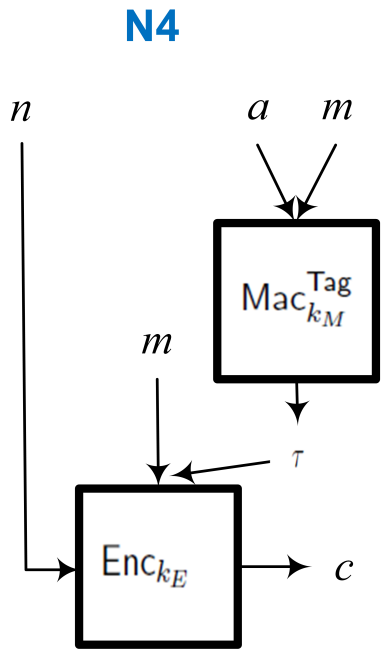
The output should be *indistinguishable* from random.

Attack N4 (1/2)



We give a counterexample.

Attack N4 (1/2)



We give a counterexample.
Let $\mathcal{M} = \{0,1\}^l$ for AEnc, thus Enc $(m \| \tau)$.

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$
$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$
$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$,

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$
$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$

$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$

  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$
$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$
  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$
- if $n = 1, 2 \wedge m = v^*$, $c_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau$

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$
$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$
  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$
- if $n = 1, 2 \wedge m = v^*$, $c_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau$
  else $c_2 = \mathsf{F}^{2,0}_k(n) \oplus \tau$

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$

$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$

  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$
- if $n = 1, 2 \wedge m = v^*$, $c_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau$

  else $c_2 = \mathsf{F}^{2,0}_k(n) \oplus \tau$

Forgery:

- $(1, a, m)$ obtaining $c^1 = (v^*, c^1_1, c^2_1)$ $[v^*, \mathsf{F}^{1,0}_k(1)]$
- $(2, a, v^*)$ obtaining $c^2 = (c^2_0, c^1_1, c^2_2)$ $[\mathsf{F}^{2,1}_k(v^*) \oplus \tau]$

Output $(1, a, c = [v^*, c^1_1 \oplus m \oplus v^*, c^2_2])$.

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$

$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$

  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$
- if $n = 1, 2 \vee m = v^*$, $c_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau$

  else $c_2 = \mathsf{F}^{2,0}_k(n) \oplus \tau$

Forgery:

- $(1, a, m)$ obtaining $c^1 = (v^*, c^1_1, c^2_1)$ $[v^*, \mathsf{F}^{1,0}_k(1)]$
- $(2, a, v^*)$ obtaining $c^2 = (c^2_0, c^1_1, c^2_2)$ $[\mathsf{F}^{2,1}_k(v^*) \oplus \tau]$

Output $(1, a, c = [v^*, c^1_1 \oplus m \oplus v^*, c^2_2])$.

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$

$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$

  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$
- if $n = 1, 2 \vee m = v^*$, $c_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau$

  else $c_2 = \mathsf{F}^{2,0}_k(n) \oplus \tau$

Forgery:

- $(1, a, m)$ obtaining $c^1 = (v^*, c^1_1, c^2_1)$ $[v^*, \mathsf{F}^{1,0}_k(1)]$
- $(2, a, v^*)$ obtaining $c^2 = (c^2_0, c^1_1, c^2_2)$ $[\mathsf{F}^{2,1}_k(v^*) \oplus \tau]$

Output $(1, a, c = [v^*, c^1_1 \oplus m \oplus v^*, c^2_2])$.

Attack N4 (2/2)

Key: k (key TPRF F), $v^* \in \mathcal{M}$

$\mathsf{Enc}^n_{k,v^*}(m \| \tau)$:

- if $n = 1$, $c_0 = v^*$, else $c_0 = \mathsf{F}^{0,0}_k(n)$

  $c_1 = \mathsf{F}^{1,0}_k(n) \oplus m$
- if $n = 1, 2 \vee m = v^*$, $c_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau$

  else $c_2 = \mathsf{F}^{2,0}_k(n) \oplus \tau$

Forgery:

- $(1, a, m)$ obtaining $c^1 = (v^*, c^1_1, c^2_1)$ $[v^*, \mathsf{F}^{1,0}_k(1)]$
- $(2, a, v^*)$ obtaining $c^2 = (c^2_0, c^1_1, c^2_2)$ $[\mathsf{F}^{2,1}_k(v^*) \oplus \tau]$

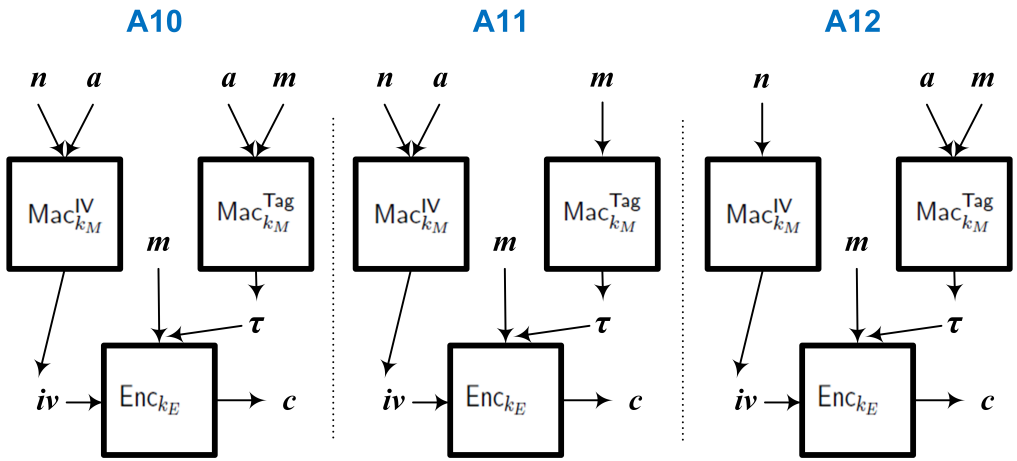
Output $(1, a, c = [\ v^*\ , \mathsf{F}^{1,0}_k(1) \oplus v^*, c^2_2 = \mathsf{F}^{2,1}_k(v^*) \oplus \tau\ ])$.

Observation of the attack

- N4 is secure if message malleable
- N4 is secure if nonce-misuse resistant
- The nE scheme just used is message malleable if the following does not happen:
  - $n = 1$ or 2 AND
  - $m = v^*$

Conclusions

Are A10, A11 and A12 secure?



Stateful generic composition

Questions?

Results

- A10, A11, A12 are either all secure or insecure
- A10, A11, A12 are secure if
  - Enc is “message-malleable”
  - Enc is “misuse-resistant”
- A10, A11, A12 are insecure if
  - Enc is stateful
  - Enc is not tidy
- N4 is insecure

Stateful

- **Stateful** The encryption algorithm uses a *state* which is
  - used only by Enc
  - kept in memory by Enc after executions
  - updated at every execution

Stateful

- **Stateful** The encryption algorithm uses a *state* which is
  - used only by Enc
  - kept in memory by Enc after executions
  - updated at every execution
- A10 is not secure if ivE is stateful
  - Attack similar to N4

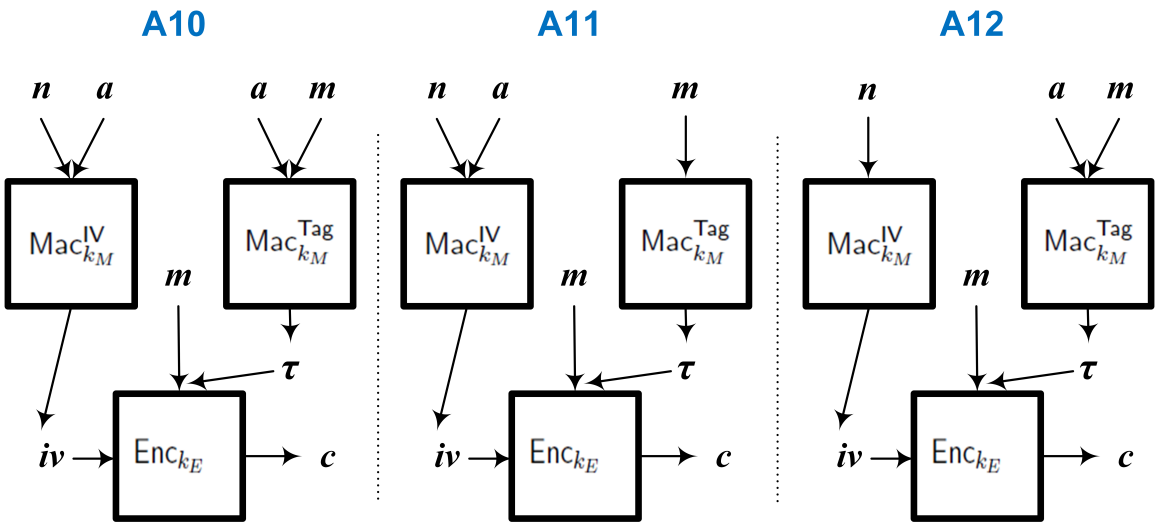
Unitidy

Untidy means

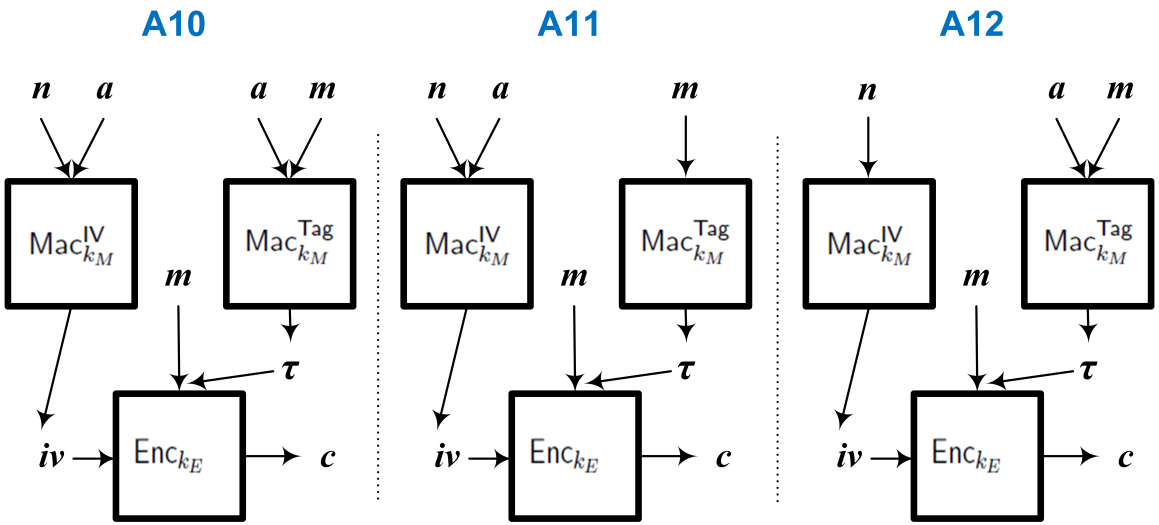
$$\mathsf{Dec}_k(iv, c) = m \nRightarrow \mathsf{Enc}_k(iv, m) = c$$

A10 in this case is not secure:

- $\mathsf{Enc}_k(iv, m) := (\mathsf{Enc}'_k(iv, m) \| \mathsf{Enc}'''_k(iv, m))$
- $\mathsf{Dec}_k(iv, c', c'') = \mathsf{Dec}_k(iv, c')$



We prove that: either all 3 are secure or all 3 are not secure.



We prove that: either all 3 are secure or all 3 are not secure.

Idea:

- Observe that $\mathrm{Mac}^{\mathrm{iv}}(n) = \mathrm{Mac}^{\mathrm{iv}}(n, a)$ since n not repeated.
- Replace n with $n' = n \| \mathrm{H}(a)$
- Replace m with $m' = \mathrm{H}(a) \| m$

N4