KATHOLIEKE UNIVERSITEIT LEUVEN

Security Aspects of Authenticated Encryption

Elena Andreeva

COSIC, KU Leuven

Summer school on design and security of cryptographic algorithms and devices for real-world applications

Croatia, 05/06/2014

Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - nonce-based AE
  - nonce misuse resistant AE
- Further challenges

Security Goal

Confidentiality

+

Authenticity

Ways to Build AE Schemes?

1. Generic **AE** composition

off the shelf primitives

Symmetric **Authentication (MAC)**

+

Symmetric **Encryption**

2. Dedicated **AE** scheme (AE designs from scratch)
3. Something in between ☺ (state of the art)

Generic Composition [BN'00]

1. Ways of composing

Enc then MAC	secure
MAC then Enc	insecure
Enc and MAC	insecure

Caveat: **Careful with interpretations!**

Conventional Encryption

- **Enc =** (Kg, Enc, Dec)

  Key generation: $K \leftarrow_{\$} Kg$

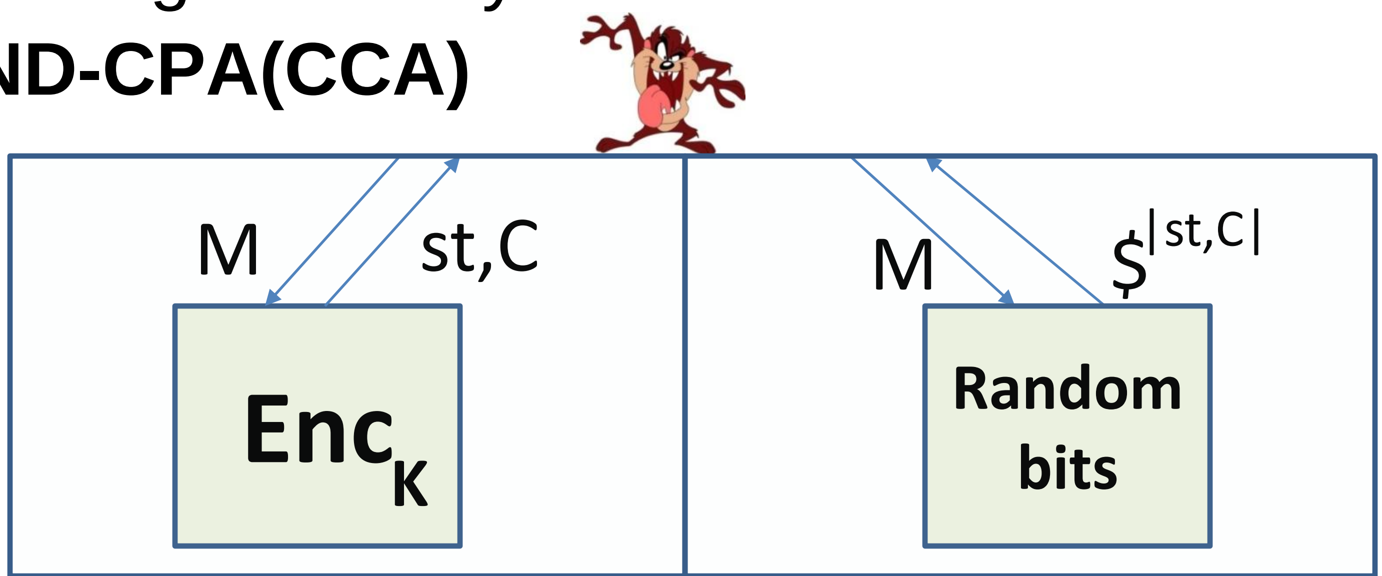
  Encryption: $(st, C) \leftarrow_{\$} Enc^{st}_{K}(M)$ (randomized or stateful)

  Decryption: $M \leftarrow Dec_{K}(st, C)$ (deterministic)

  Correctness: $Dec_{K}(Enc_{K}(M)) = M$

- Indistinguishability

  $IND-CPA(CCA)



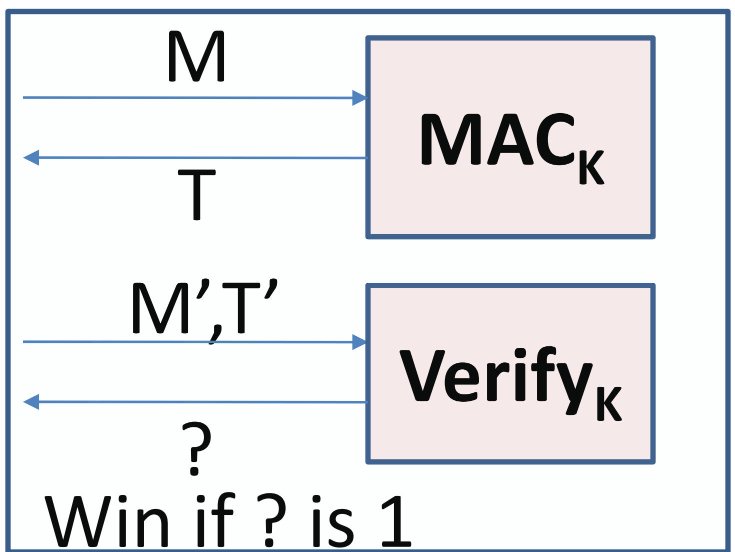
MAC

- **MAC =** (Kg, MAC, Verify)

Key generation: $K \leftarrow_{\$} Kg$
Authentication: $T \leftarrow MAC_K(M)$ (any)
Verification: $1/0 \leftarrow Verify_K(M, T)$ (deterministic)

Correctness: $Verify_K(M, MAC_K(M)) = 1$

- Unforgeability (weak M' ≠ M; strong M',T' ≠ M,T)



Generic Composition [BN'00]

- $IND-CPA **Enc** + Unforgeable **MAC**

AE secure: Enc then MAC

- Off the shelf schemes

Enc (CBC, CTR,...) **+ MAC** (CBC-MAC,HMAC,PMAC...)

Caveat: Careful with interpretations!

A. Enc often with badly or **externally** generated random IV

B. IV should not be communicated out of band

A: Random IV Encryption

- **Enc** = (Kg, Enc, Dec)

Key generation: $K \leftarrow_\$ Kg$

Encryption: $IV, C \leftarrow Enc^{IV}_K(M)$ (deterministic)

Decryption: $M \leftarrow Dec_K(IV, C)$ (deterministic)

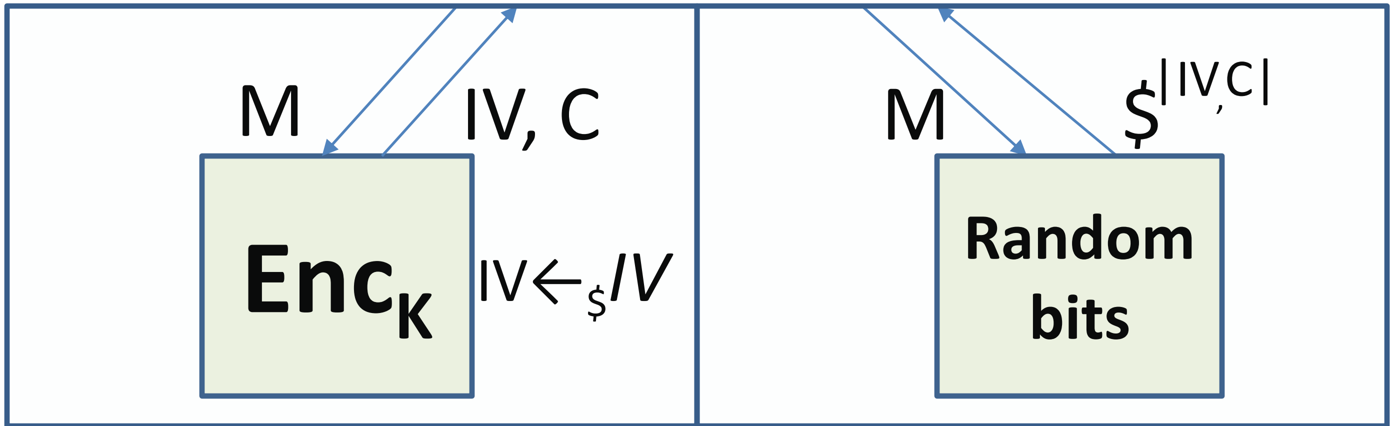
Correctness: $Dec_K(Enc^{IV}_K(M)) = M$

Fix A: Environment not Enc selects IV

B: IV still in-band

- Indistinguishability

$IND-CPA



Nonce IV

- N: nonce IV
- Not required to be random
- Unique non-repeating value
- Can be communicated out of band
- Theoretically: a way to work with an IV (randomness/state) out of Enc algorithm
- Practically: ease of use

Nonce-based Encryption Scheme

- **Enc =** (Kg, Enc, Dec)

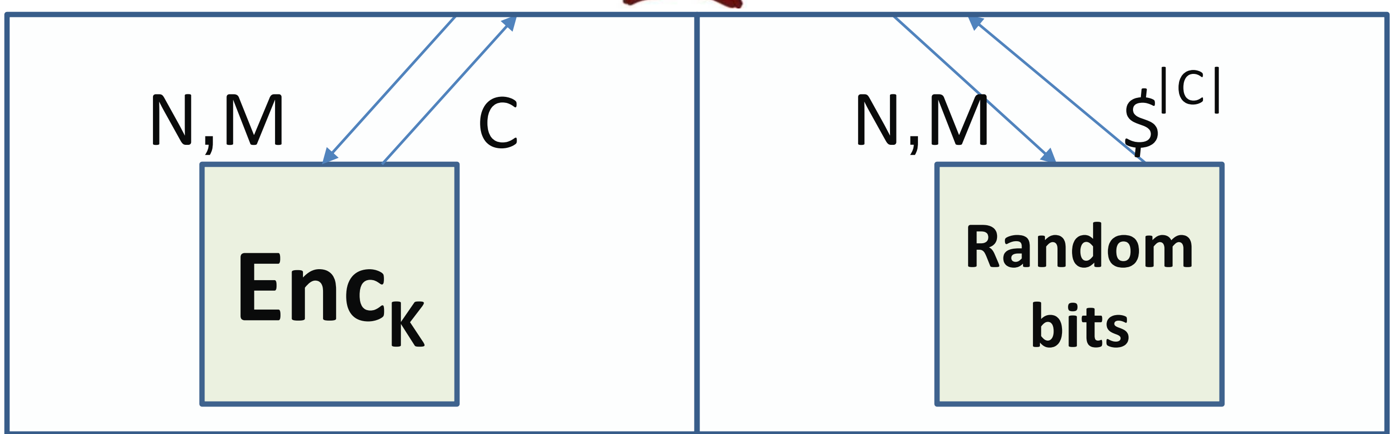
  Key generation: $K \leftarrow_{\$} Kg$
  Encryption: $C \leftarrow Enc_K(N, M)$ (deterministic)
  Decryption: $M \leftarrow Dec_K(N, C)$ (deterministic)

  Correctness: $Dec_K(N, Enc_K(M)) = M$

Fix A: Adversary can select N
Fix B: out-of-band

- Indistinguishability (nonce respecting adversary)

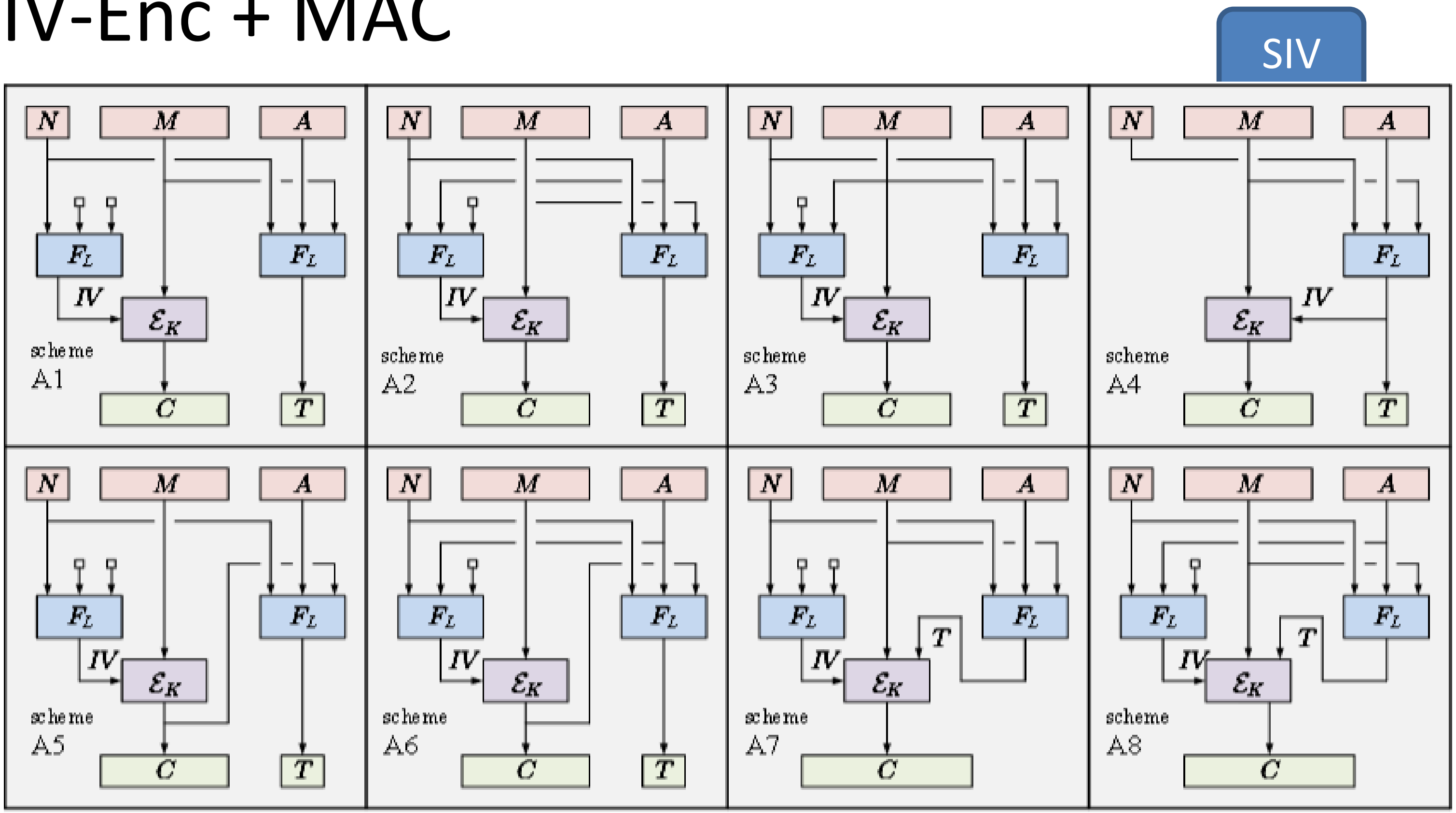
  \$IND-CPA



Generic Composition Reconsidered [NRS'14]

- **Build nonce-based AE from**

1. IV-Enc + MAC

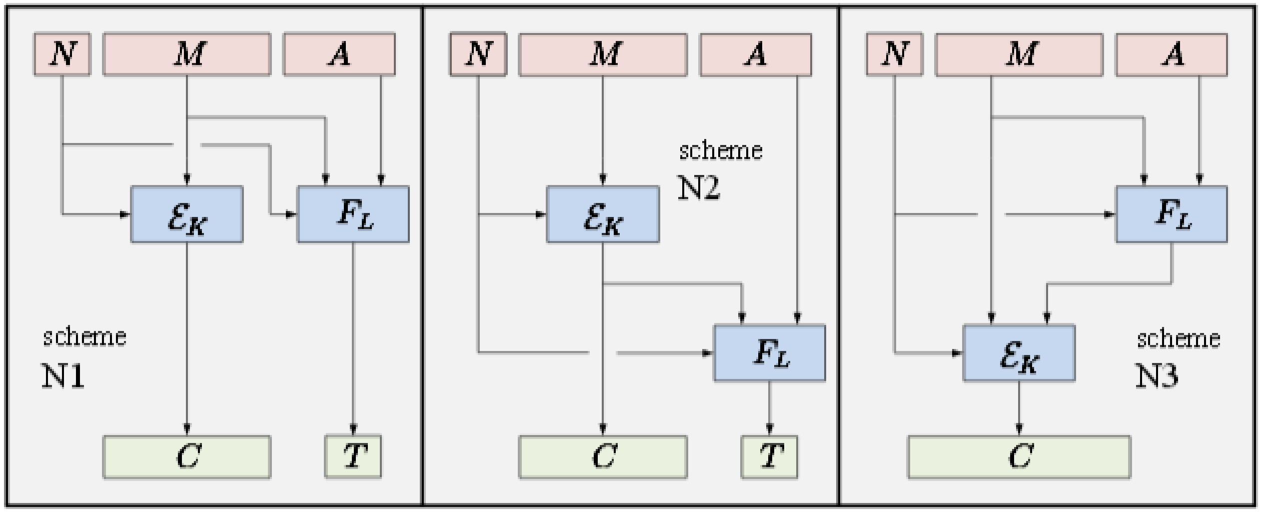


Efficiency issues: 2 passes over the data

Generic Composition Reconsidered [NRS'14]

- **Build nonce-based AE from**

2. N-Enc + MAC



- **Generic composition disadvantages**
  - Efficiency issues: 2 passes over the data
  - Prone to misuse with conventional Enc schemes

Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - Nonce-based AE
  - Nonce misuse resistant AE
- Further challenges

Dedicated AE: State of the Art

Prior to CAESAR

Building Block	Nonce dependent AE security	Nonce independent AE security
Block cipher	IAPM*'00, OCB*'01, XECB*'01, CCM'03, GCM'04, OTR*'14, CLOC'14	SIV'06, BTM'09, McOE-G'11, POET'14 COPA'13
Permutation	SpongeWrap'11 Ketje&Keyak'14 NORX'14	APE'14

* hold a patent

Nonce-based AE

- $\mathbf{AE}$ **=** (Kg, E, D)

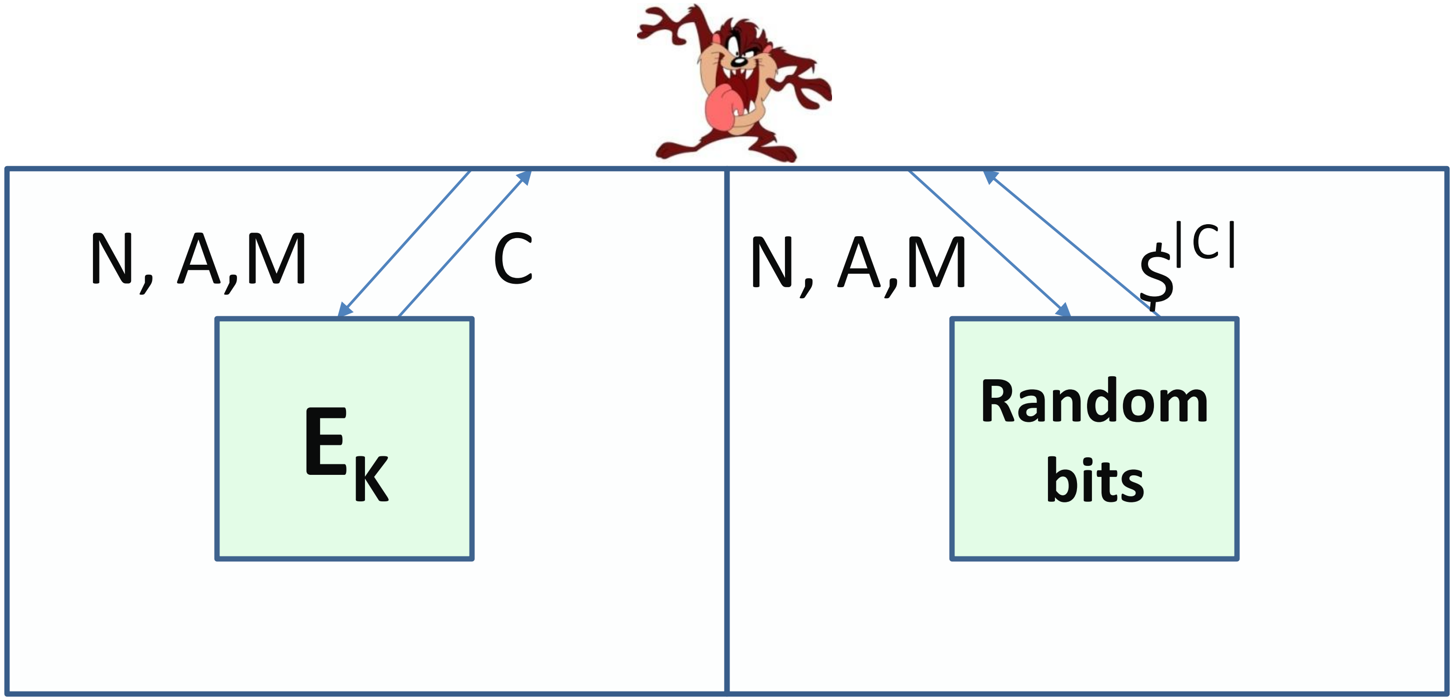
Key generation: $K \leftarrow_{\$} Kg$
Encryption: $C \leftarrow E_K(A, N, M)$ (deterministic)
Decryption: $M/\perp \leftarrow D_K(A, N, C)$ (deterministic)

Correctness: $D_K(A, N, E_K(A, N, M)) = M$

- AE confidentiality + AE integrity = AE security

AE Confidentiality

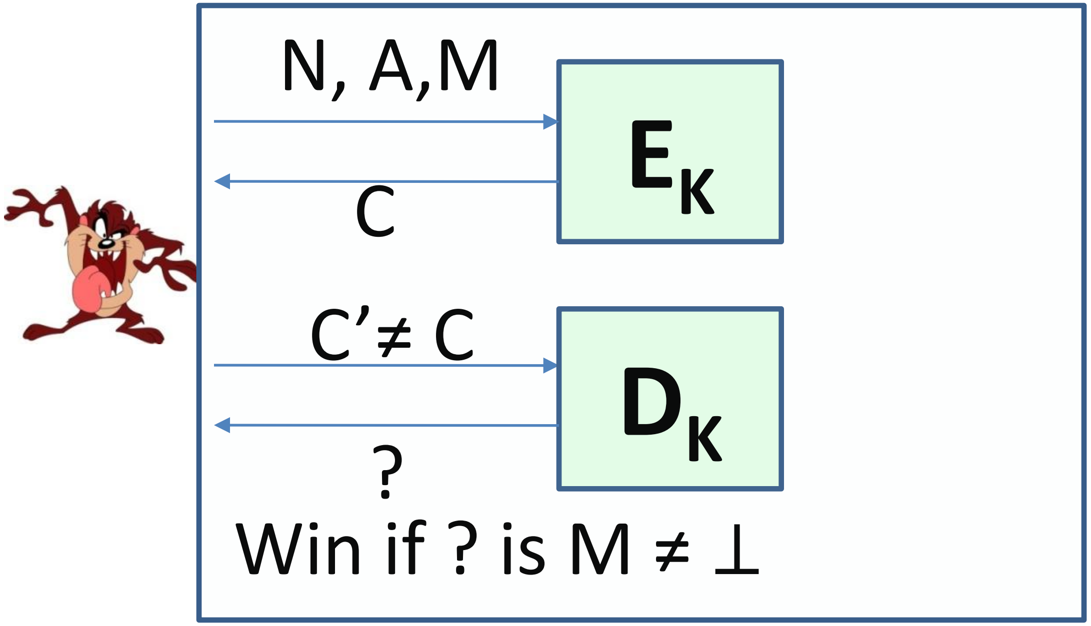
- **$IND-CPA**



Adversary is nonce respecting

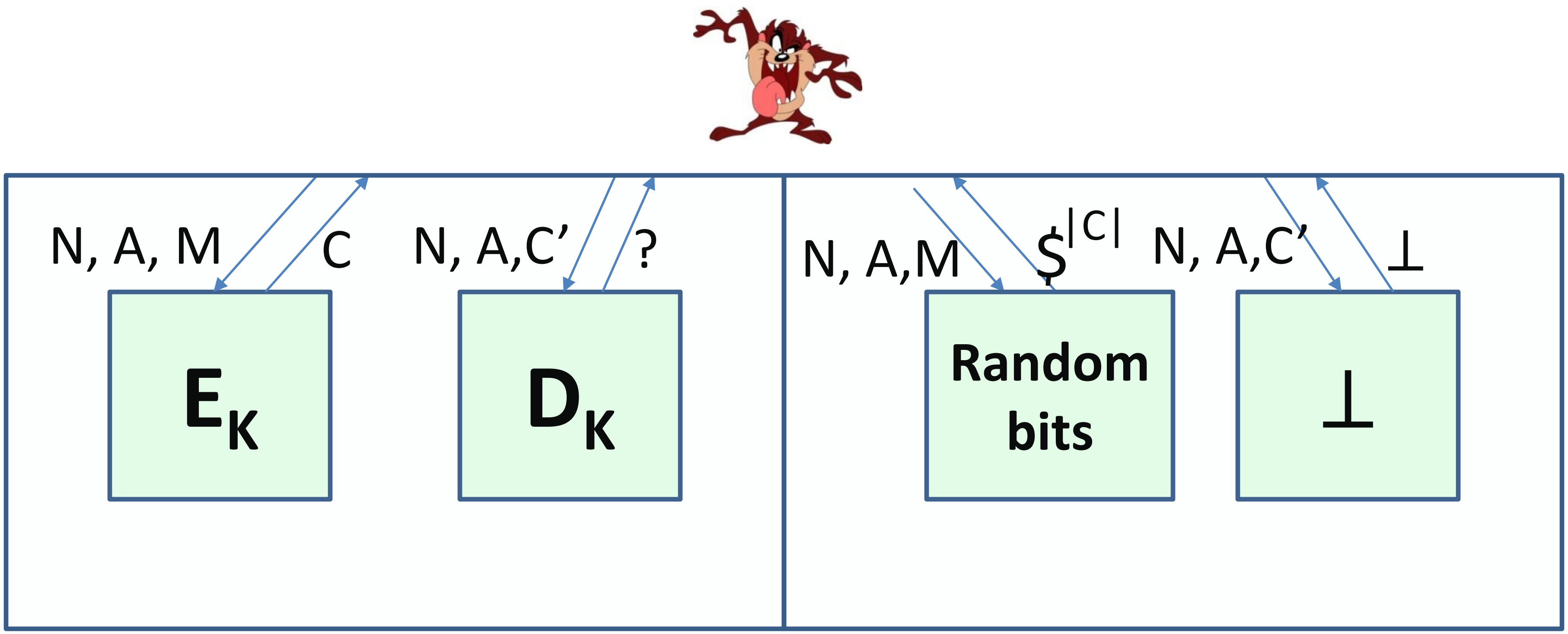
AE Integrity

- **INT-CTXT**



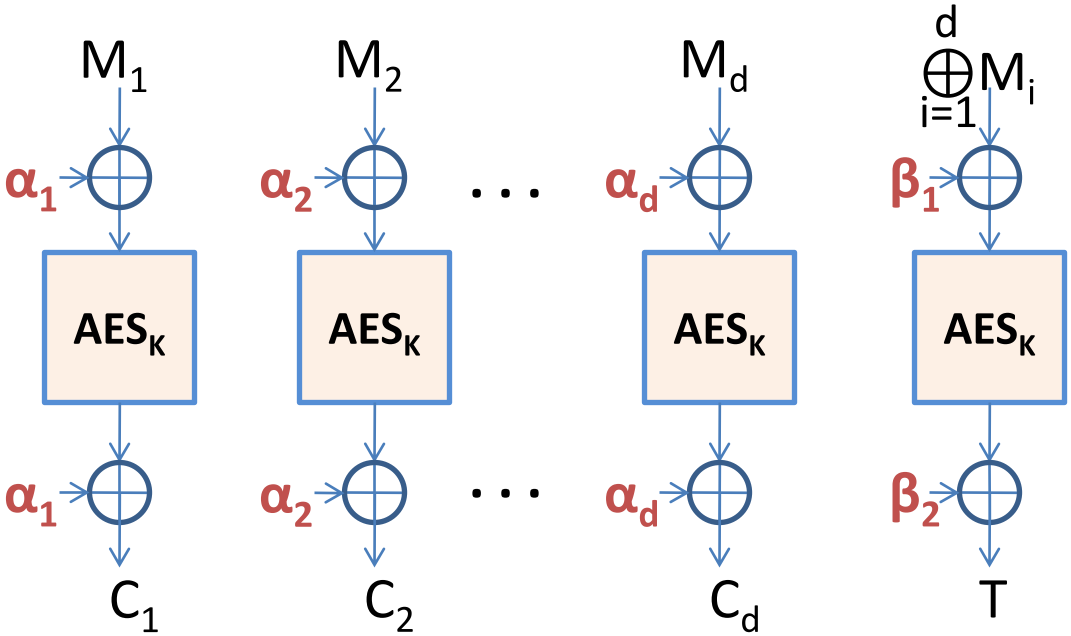
Adversary maybe nonce respecting

Nonce-based AE Security



Adversary is nonce respecting

Example: OCB [RBBK'01]



$\alpha_i = f_i(K,N)$

$\beta_i = g_i(K,N)$

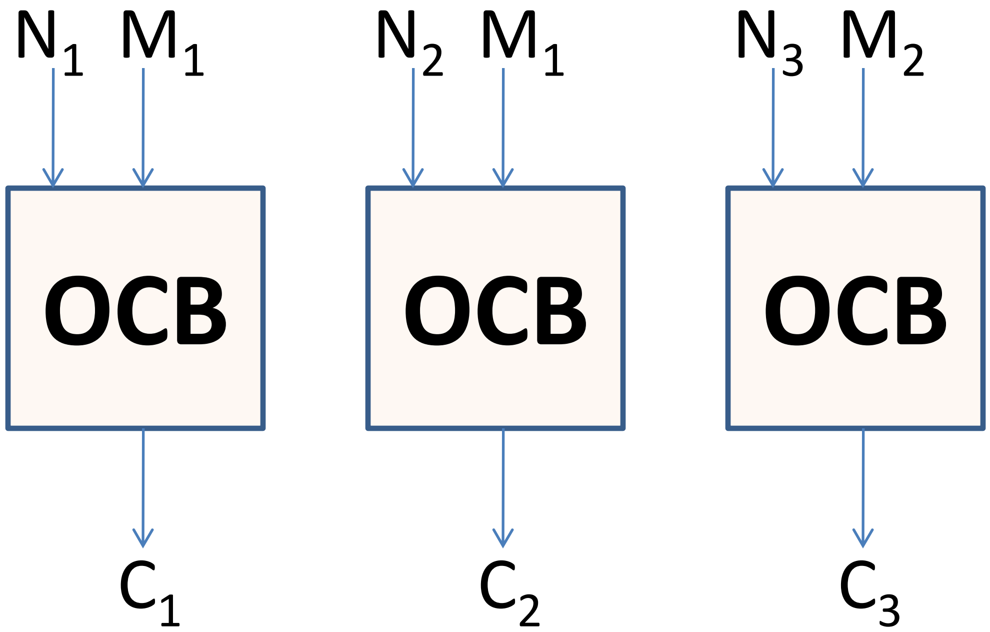
Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - Nonce-based AE
  - Nonce misuse resistant AE
- Further challenges

Nonce Misuse Resistant AE

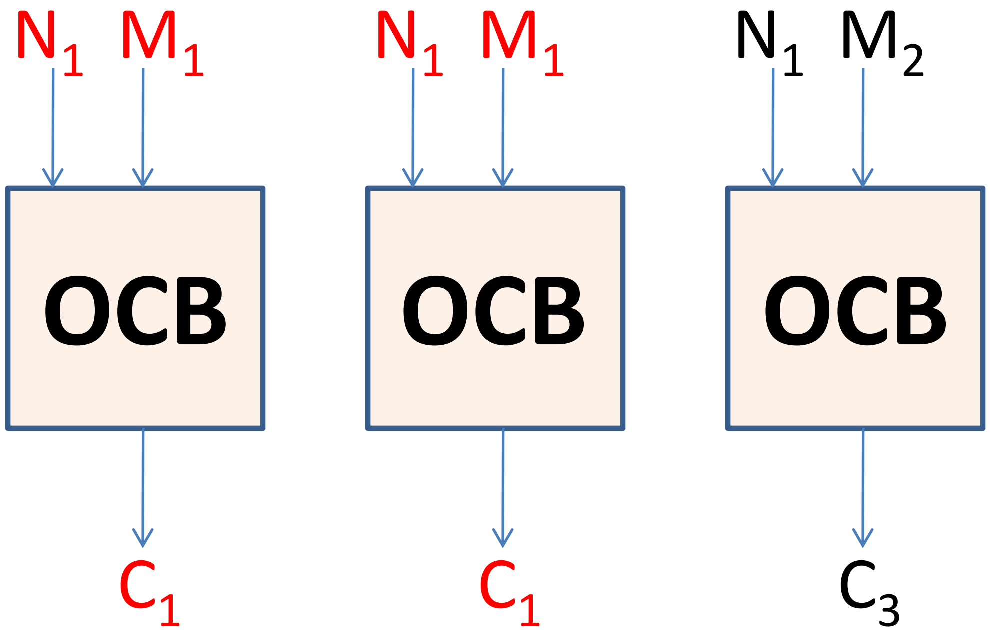
Not all security should be lost if N misused!

Distinct Nonces



Nonce Misuse OCB
Ciphertext Repetitions

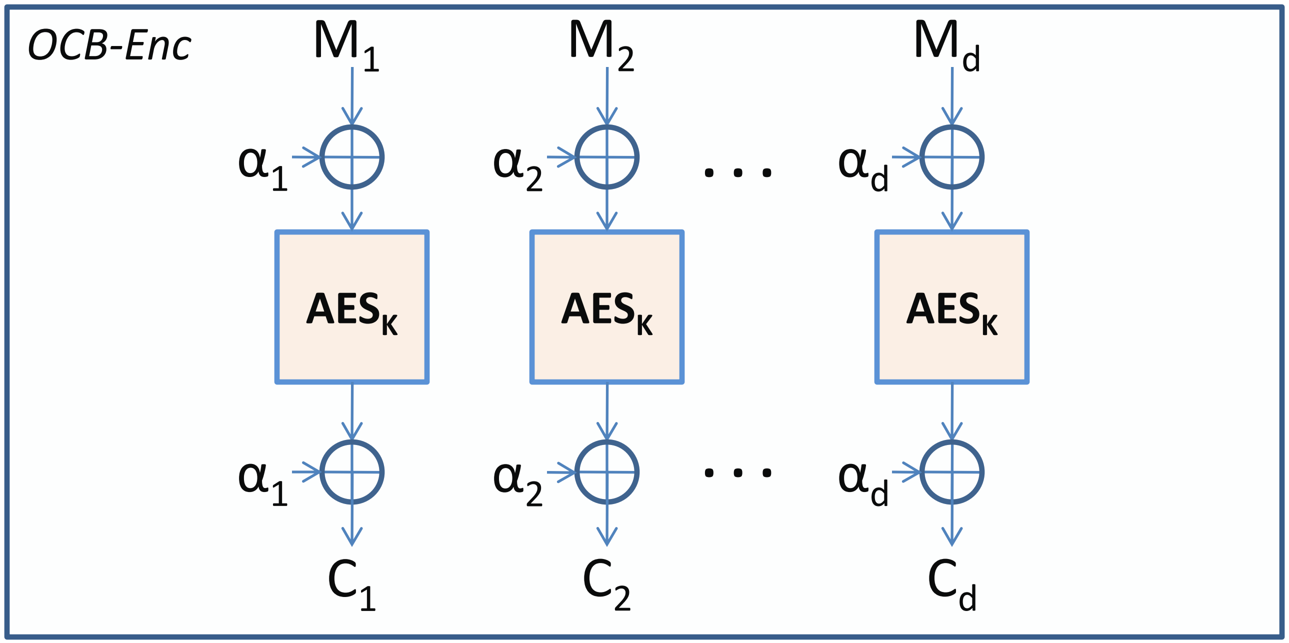
What security can be lost?



- Valid for all nonce respecting AE schemes

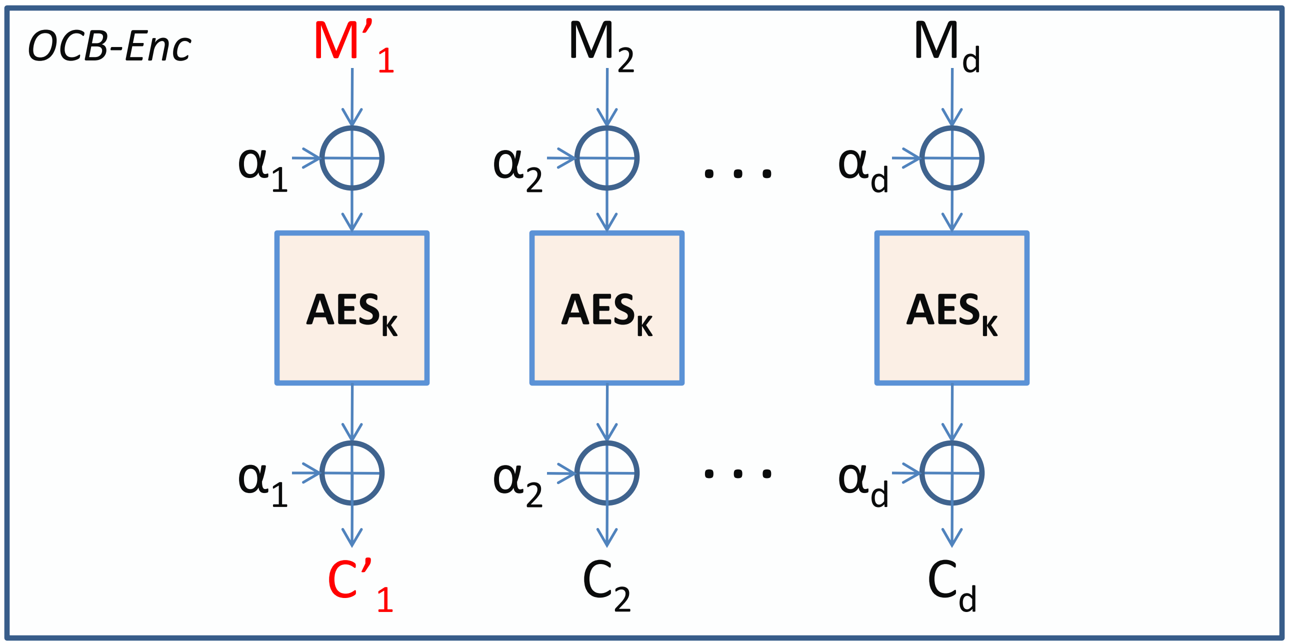
Nonce Misuse OCB
Ciphertext Block Repetitions

What else can be lost?



Nonce Misuse OCB
Ciphertext Block Repetitions

What else can be lost? (OCB looses confidentiality)



- If C blocks repeat (over distinct OCB calls) then M blocks repeat (OCB, IAPM, XCBC, ...)

What to Do against Nonce Misuse?

Not all security should be lost if N misused!

1. **Security up to common prefixes**

ciphertext leaks only presence of common M prefixes
McOE-G, COPA, APE, COBRA, POET

2. **Security up to repetitions**

ciphertext leaks only presence of repeating Ms
SIV, BTM, HBS but two passes over the data

Nonce Misuse Resistance via Online Ciphers

- Online cipher + authentication [BBKN‘01, FFLW’12]

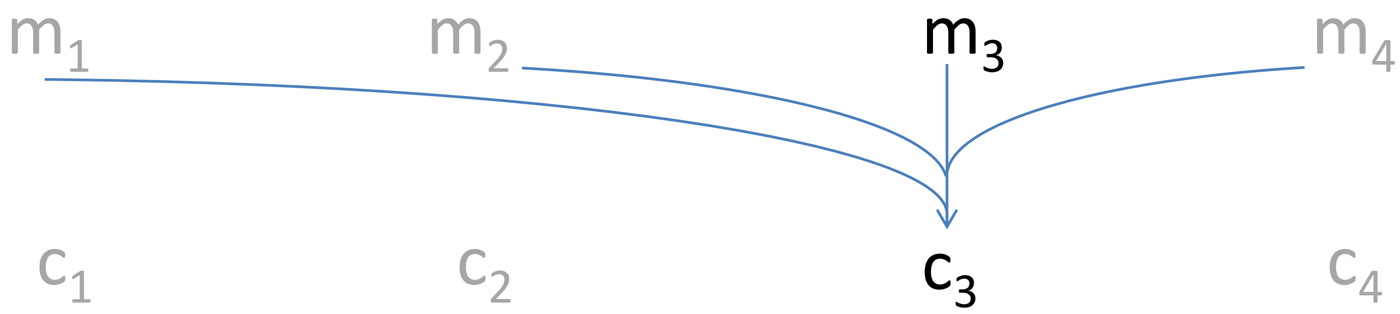
↓

nonce misuse resistant *nmr* AE scheme

secure up to common prefix repetitions

Regular vs Online Ciphers

- Normally in a cipher

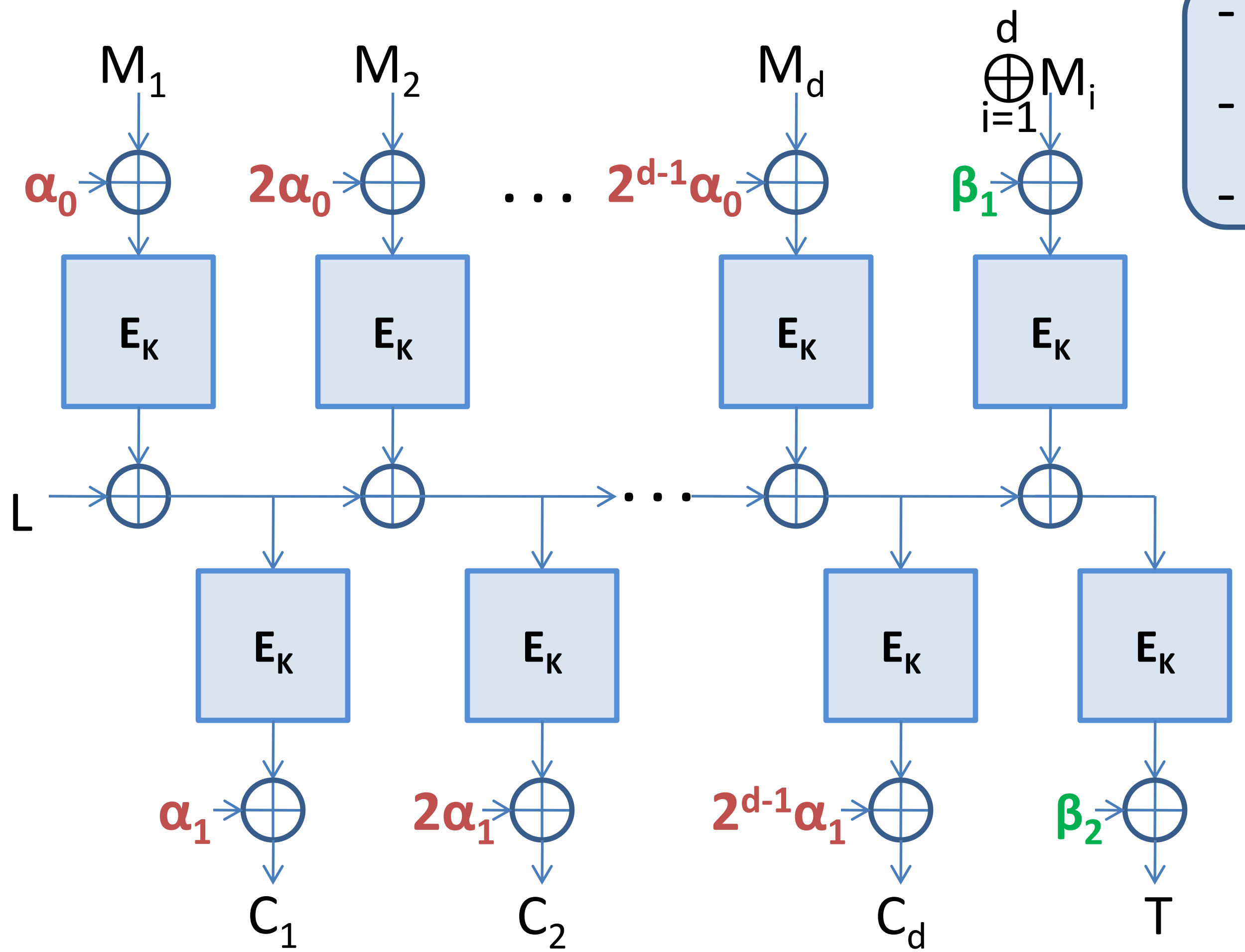


- Online cipher

- more efficient
- different security (IND from random online permutation)

COPA [ABLMY'13]
nmr AE

- nmr
- online
- parallelizable



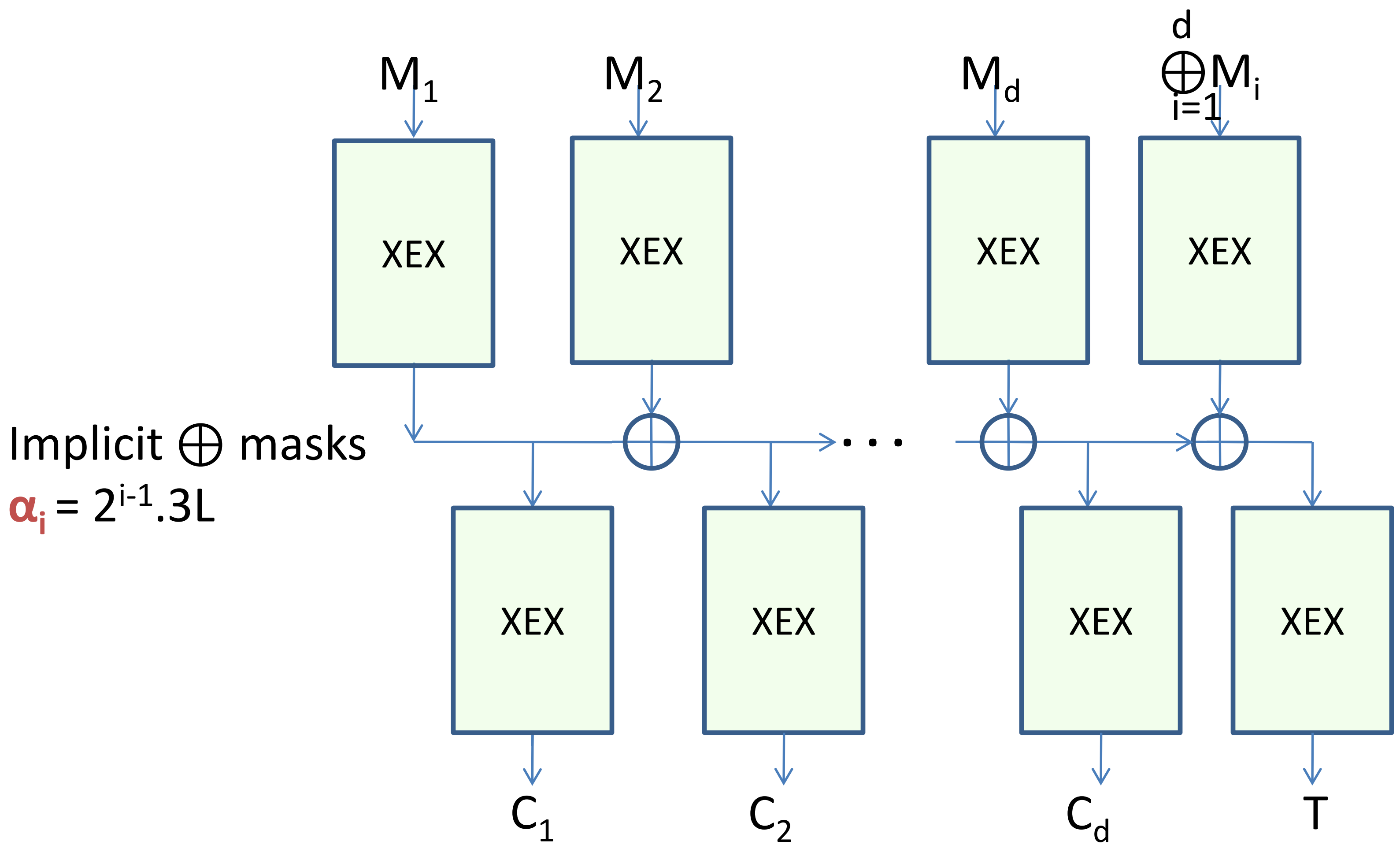
$L = E_K(0)$

$\alpha_0 = 3L$ and $\alpha_1 = 2L$

$\beta_1 = 2^{d-1}.3^2L$ and $\beta_2 = 2^{d-1}.7L$

COPA

Security Proof



If E is SPRP, COPA is AE secure up to $2^{n/2}$ queries

Outline

- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - Nonce-based AE
  - Nonce misuse resistant AE
- Further challenges

Further Security Pitfalls in AE

What if attacker gets C decryptions before verification completed?

RUP: Release of unverified plaintext [ABLMNY'14]

- Scenarios
  - Insufficient memory
  - Real-time requirements
- Not in current AE security models!

AE Syntax under RUP

- Separate the AE Decryption D functionality into Dec and Verify (how we design AE schemes)

$$C, T \leftarrow E_K(A, N, M)$$

$$M \leftarrow Dec_K(A, N, C, T)$$

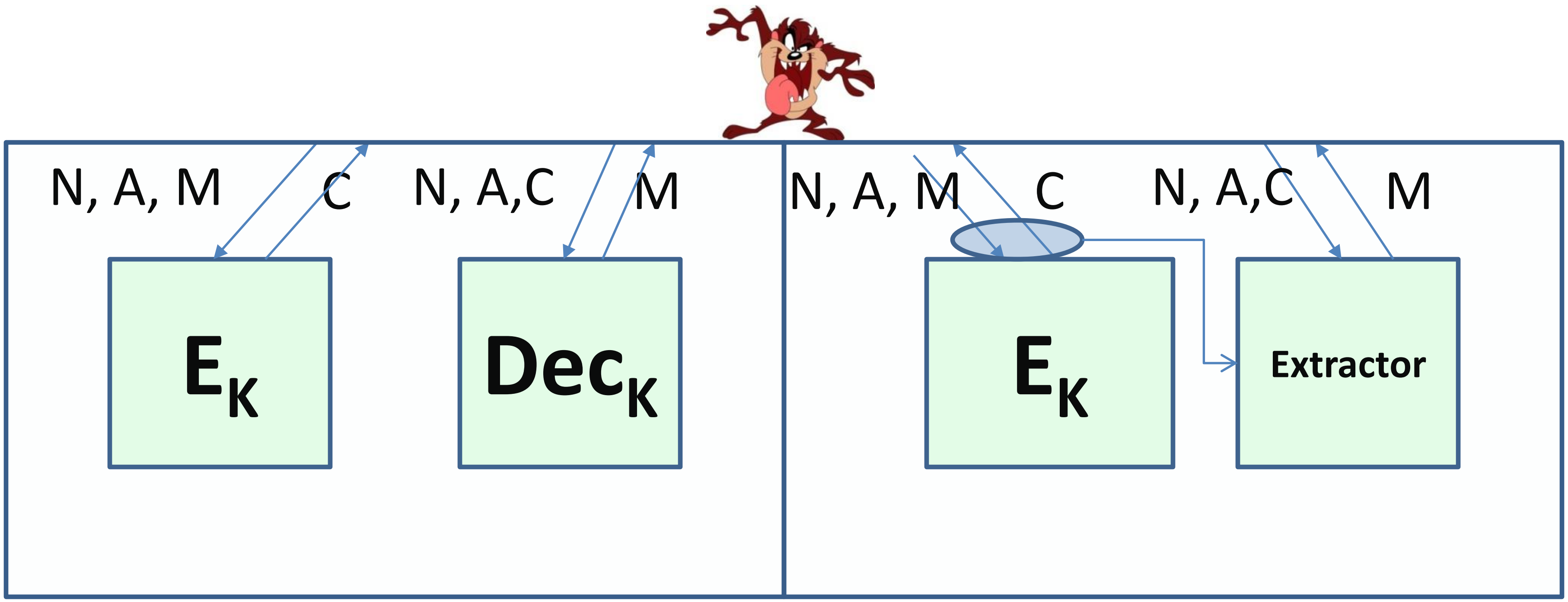
$$1/0 \leftarrow Verify_K(A, N, C, T)$$

Correctness: $Dec_K(A, N, E_K(A, N, M)) = M$

and $Verify_K(A, N, E_K(A, N, M)) = 1$

RUP Confidentiality

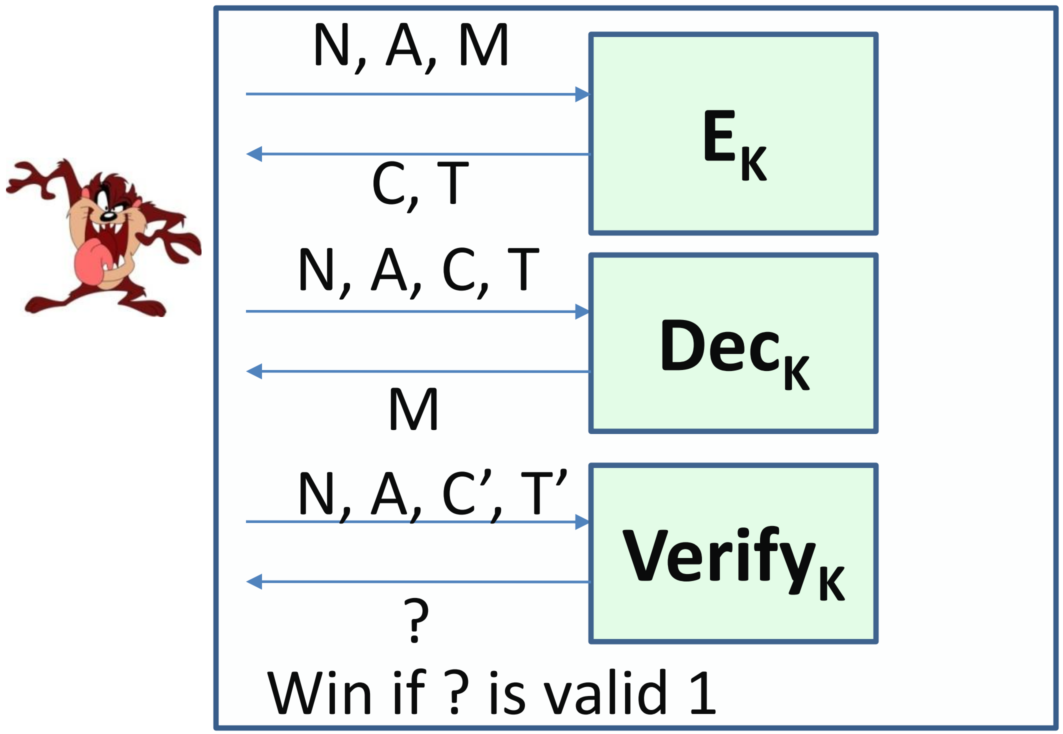
- Confidentiality: $IND-CPA + PA1
- Plaintext awareness PA1



Adversary can choose any nonce

RUP Integrity

- Int-RUP



Adversary can choose any nonce

Security of AE Schemes under RUP

IV Type	Scheme	PA1
Random	CTR, CBC encryption	Yes
Nonce	OCB	No
	GCM, SpongeWrap	No
	CCM	No
Arbitrary	COPA	No
	McOE-G	No
	APE	Yes
	SIV, BTM, HBS	Yes
	Encode-then-Encipher	Yes

Further Challenges

- AE security
  - handling failure events?
  - further generic results?
  - identify relevant AE security risks?

- Security of present solutions?

Thank you!