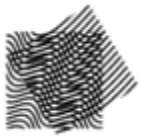
KATHOLIEKE UNIVERSITEIT LEUVEN

Security Aspects of Authenticated Encryption

(in light of the CAESAR competition)

Elena Andreeva
COSIC, KU Leuven, Belgium



Cryptoday 2014

Technion, Haifa, Israel
30/12/2014

Outline

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

AE Security Goal

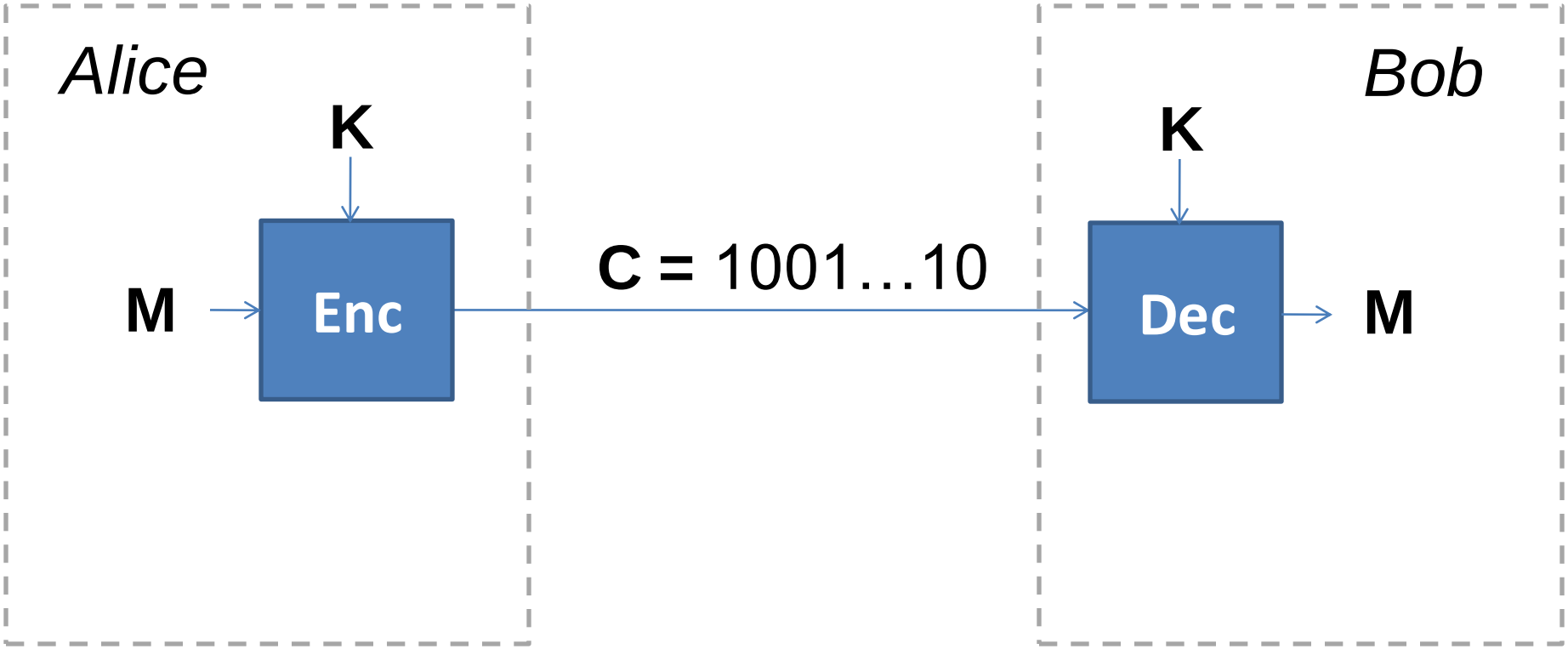
Confidentiality

+

Authenticity

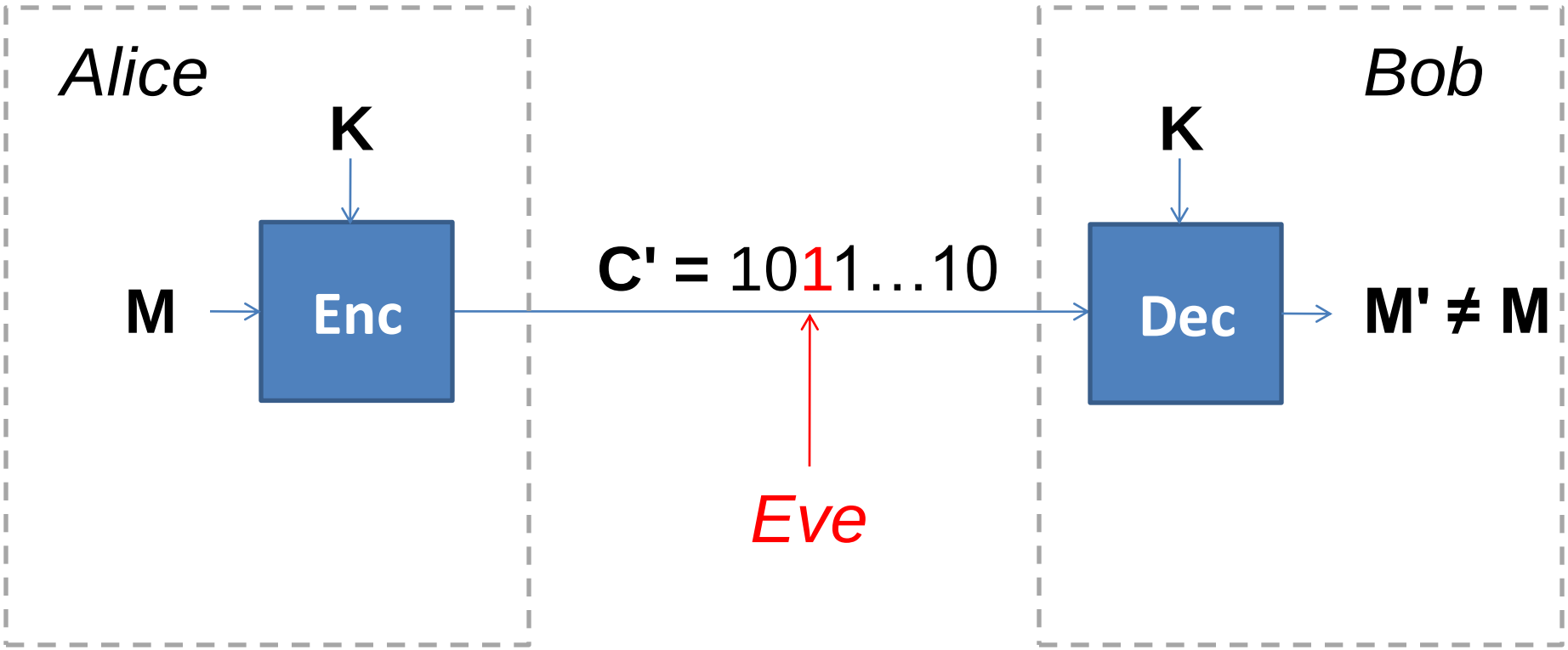
Confidentiality

Encryption Scheme



Confidentiality

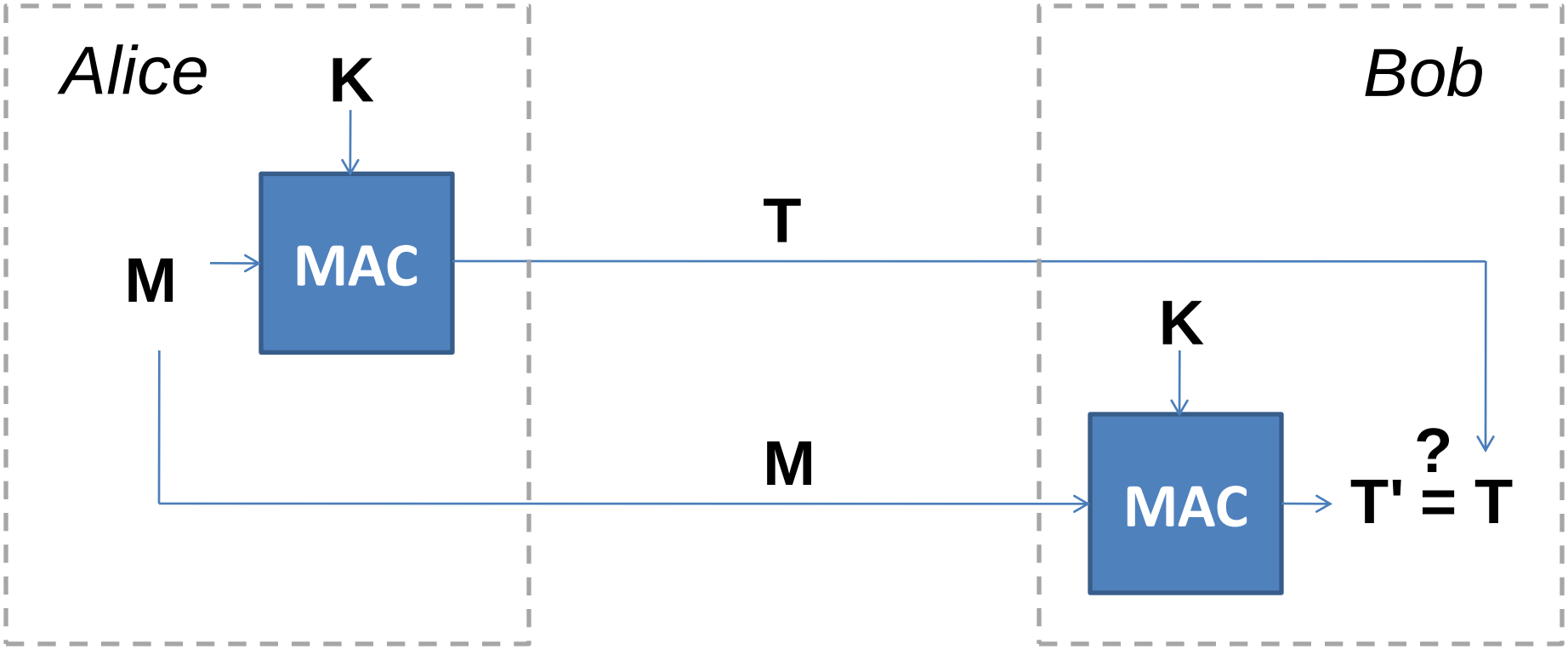
Encryption Scheme



Confidentiality ≠ Authenticity

Authenticity

Message Authentication Code: MAC



Main Question

How to combine Encryption and MAC in a secure way?

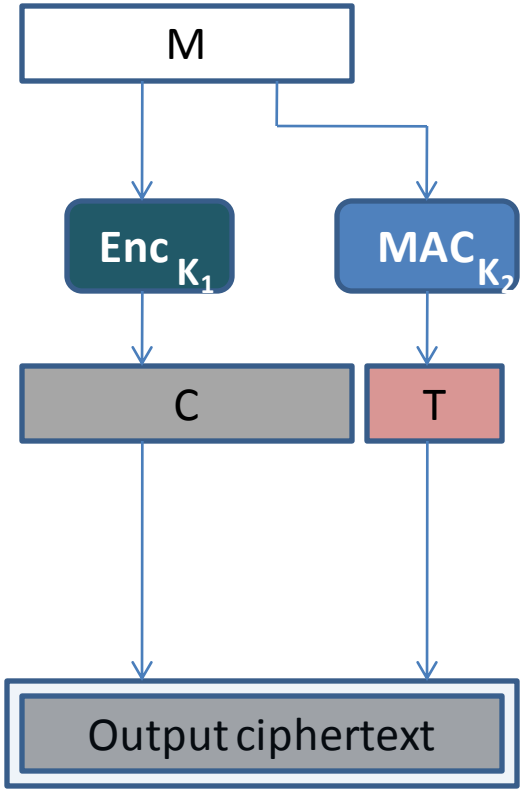
Confidentiality

+

Authenticity

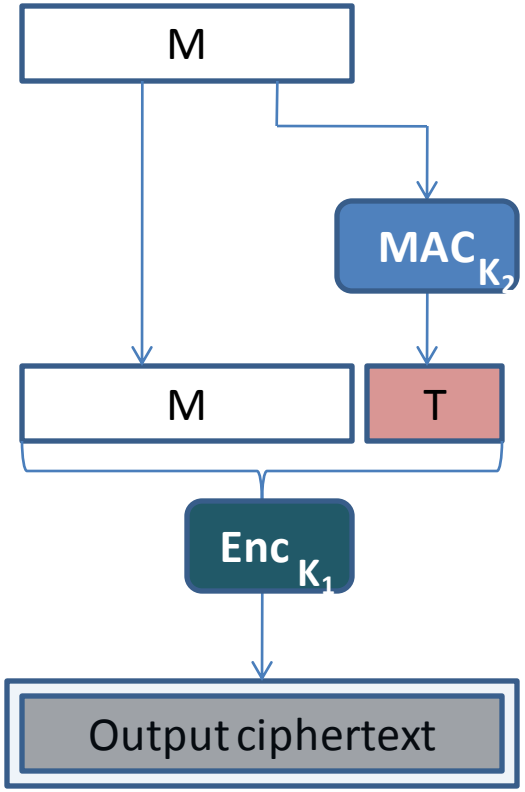
Generic Composition [BN'00]

1. Encrypt and MAC



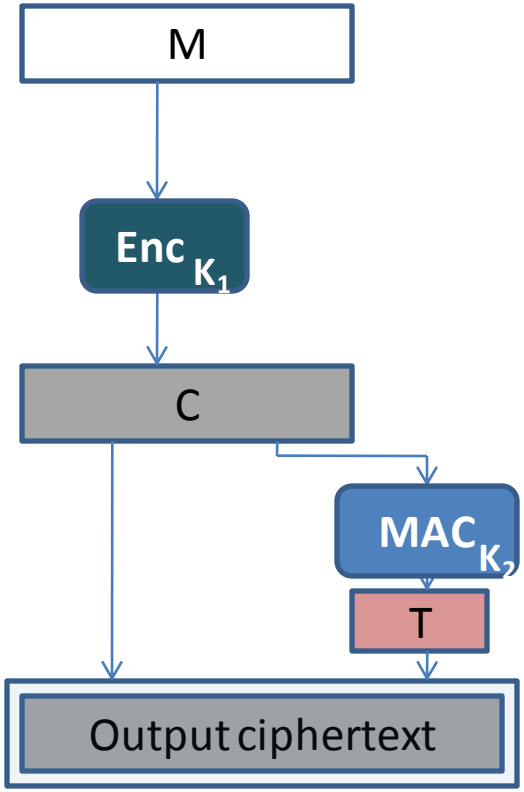
insecure

2. MAC then Encrypt



insecure

3. Encrypt then MAC



secure

Caveat: Careful with interpretations!

Conventional Encryption

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

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

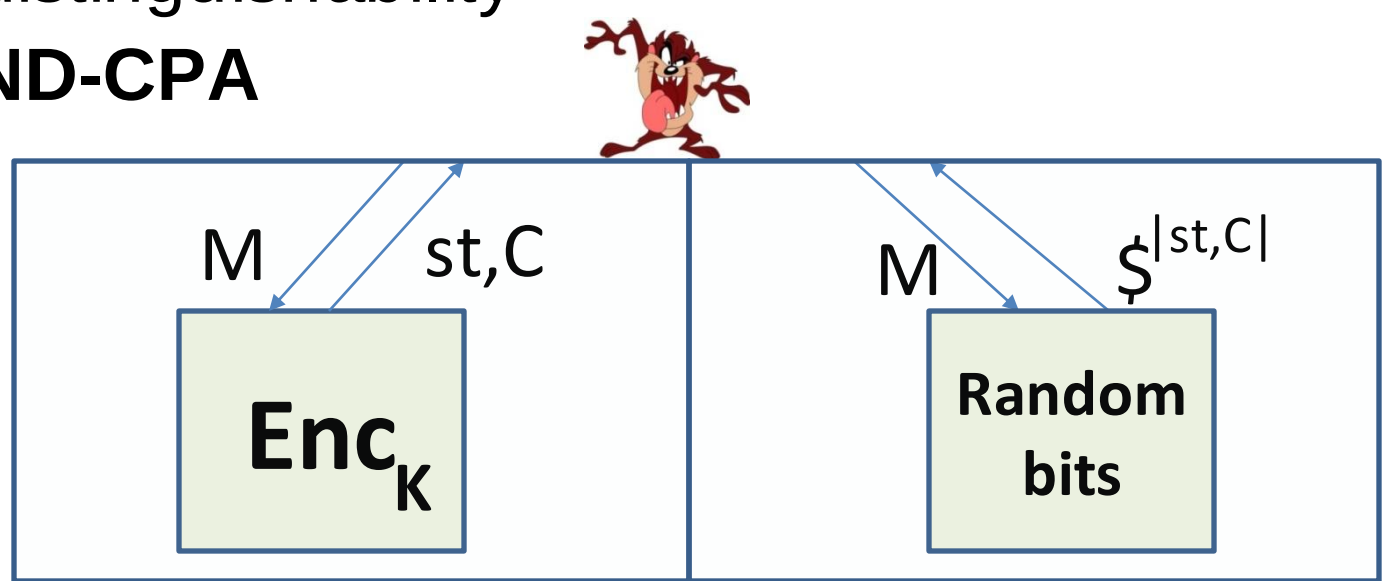
  Encryption: $(st, C) \leftarrow_{\$} Enc^{st}_K(M)$ (randomized or stateful)

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

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

- Indistinguishability

  $IND-CPA



MAC

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

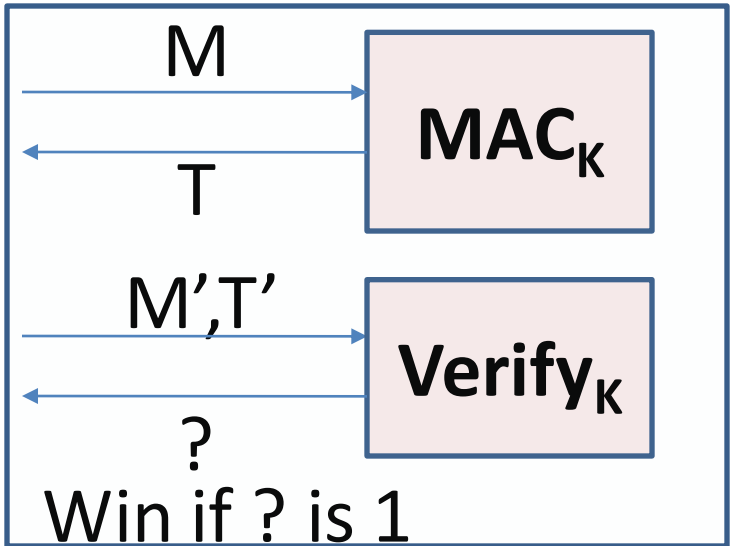
  Key generation: $K \leftarrow_{\$} Kg$

  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 $M' \neq M$; strong $M',T' \neq M,T$)



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 st or IV

B. st or IV is communicated out-of-band

A: Random IV Encryption

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

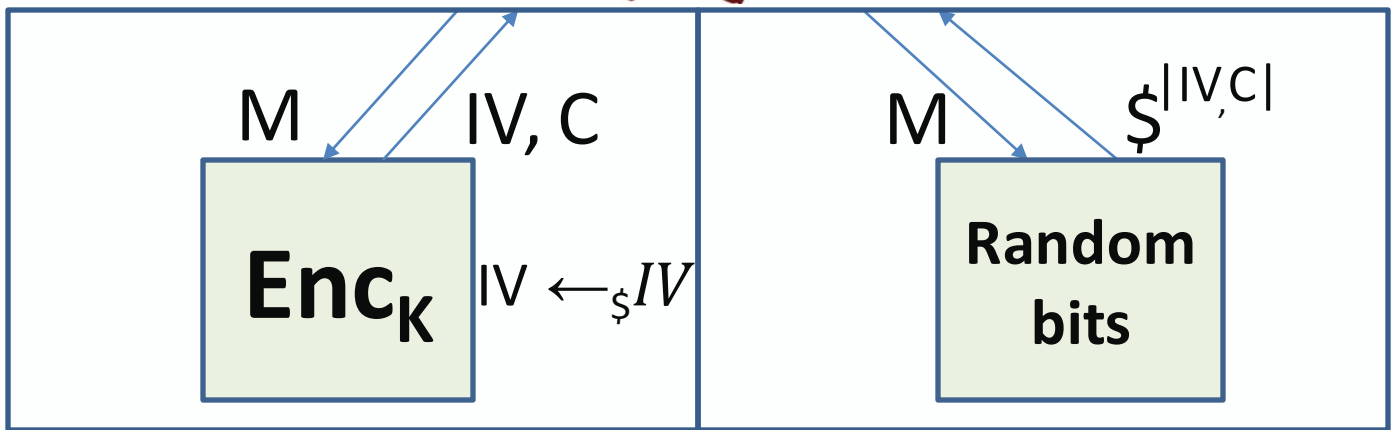
Fix A: Environment not Enc selects IV
B: IV still in-band

Key generation: $K \leftarrow_{\$} Kg$
Encryption: $IV, C \leftarrow Enc^{IV}_K(M)$ (deterministic)
Decryption: $M \leftarrow Dec_K(IV, C)$ (deterministic)

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

- 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

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

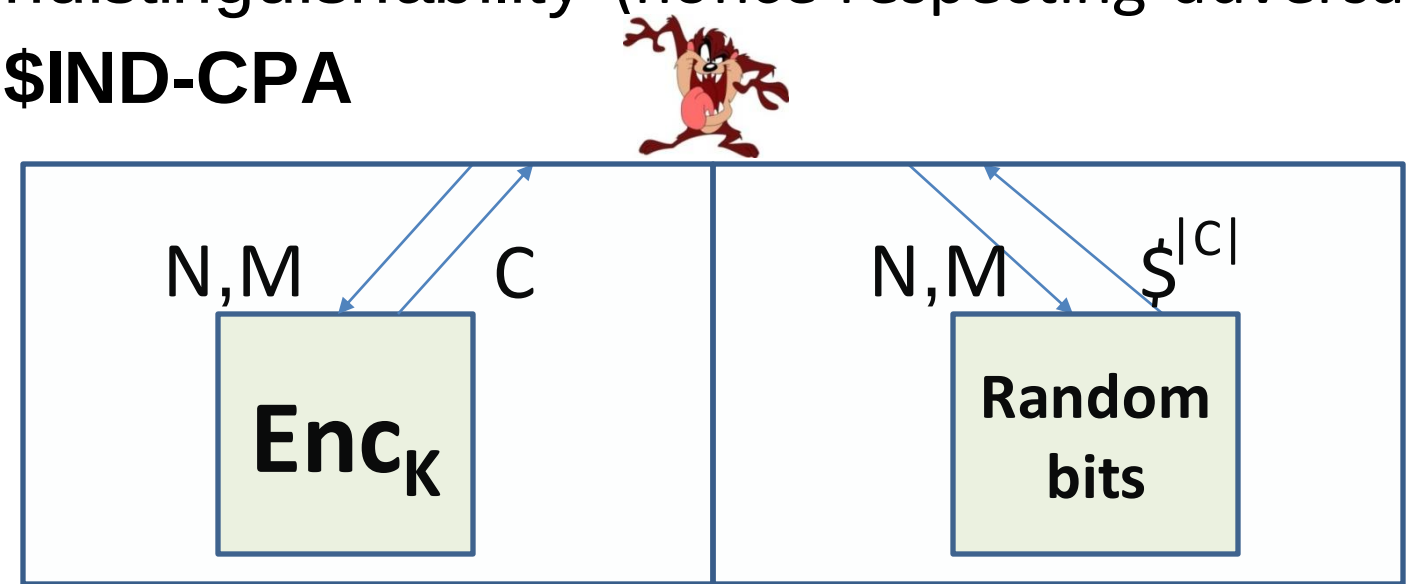
- **Enc =** (Kg, Enc, Dec)

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

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

- Indistinguishability (nonce respecting adversary)

  $IND-CPA

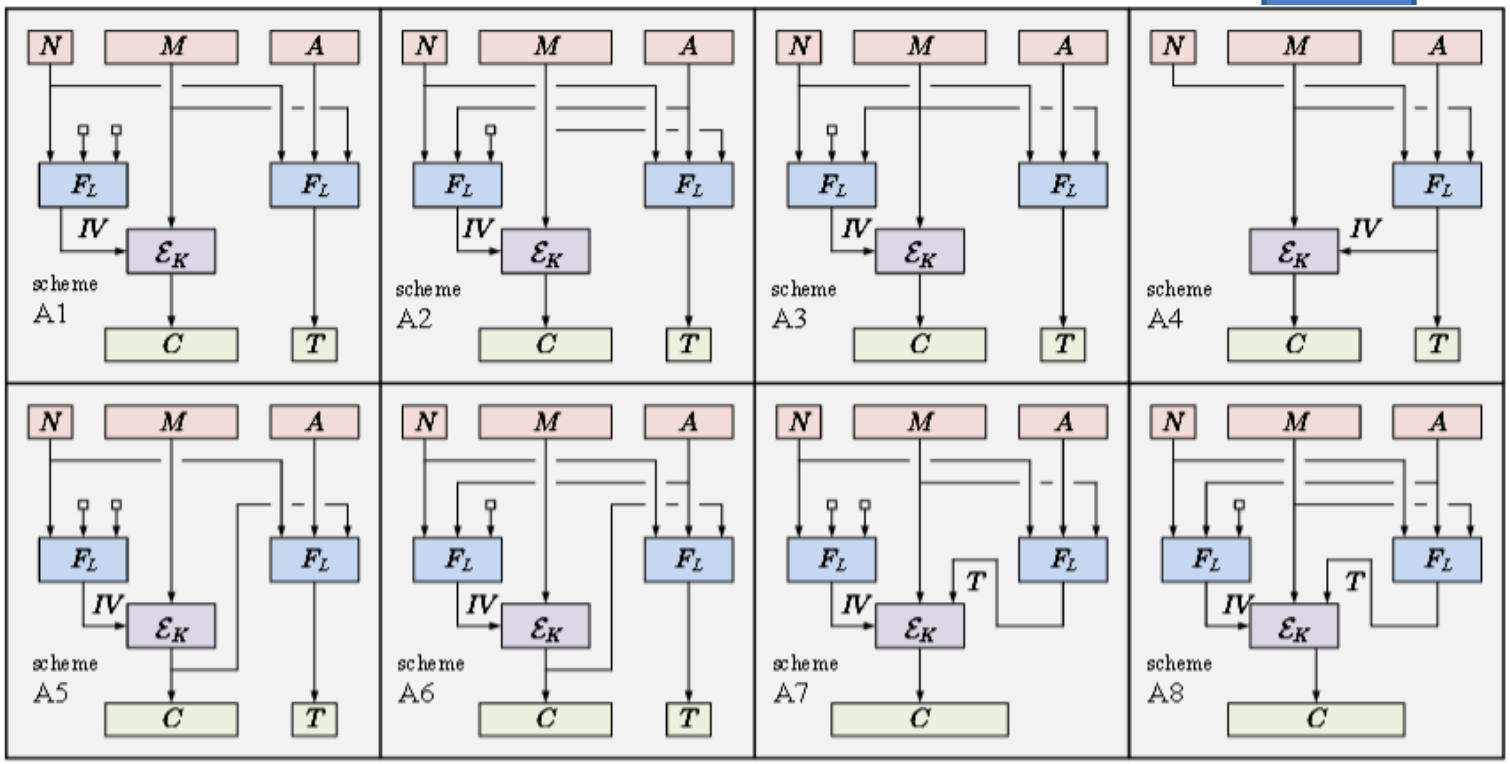


Generic Composition Reconsidered [NRS'14]

- **Build nonce-based AE from**

1. IV-Enc + MAC

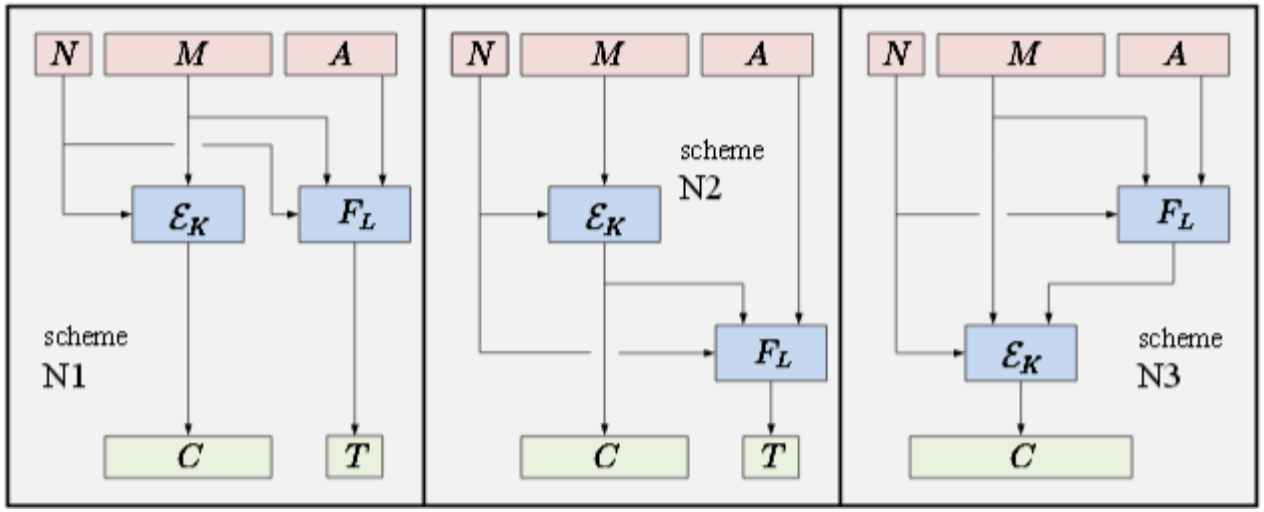
SIV



Generic Composition Reconsidered [NRS'14]

- **Build nonce-based AE from**

2. N-Enc + MAC



- **Generic composition disadvantages**

Efficiency issues: 2 passes over the data

Use of 2 keys

Prone to misuse with conventional Enc schemes

Other Ways to Build AE Schemes?

1. Generic **AE** composition

   + off the shelf primitives

   - 2 passes

   - 2 keys

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

Dedicated AE

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	Sponge Wrap'11 Ketje&Keyak'14 NORX'14	APE'14

* hold a patent

AE Syntax

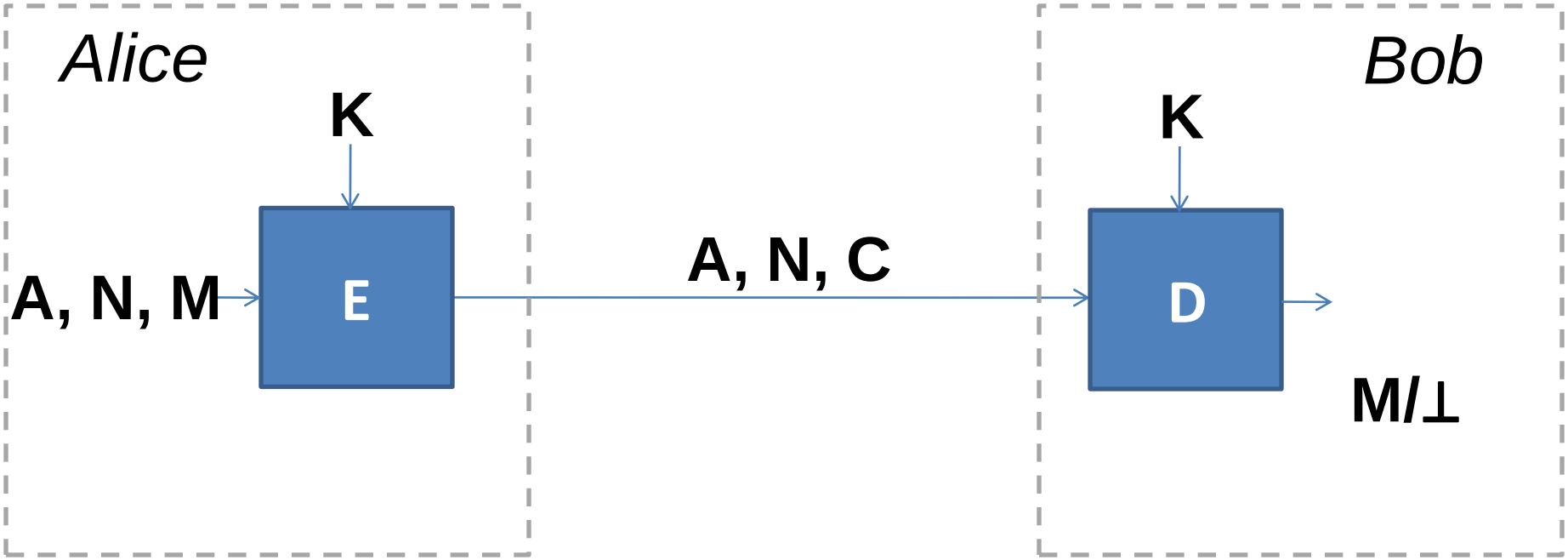
- **AE** = (Kg, E, D)

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

Encryption: $C \leftarrow E_K(A, N, M)$ (deterministic)

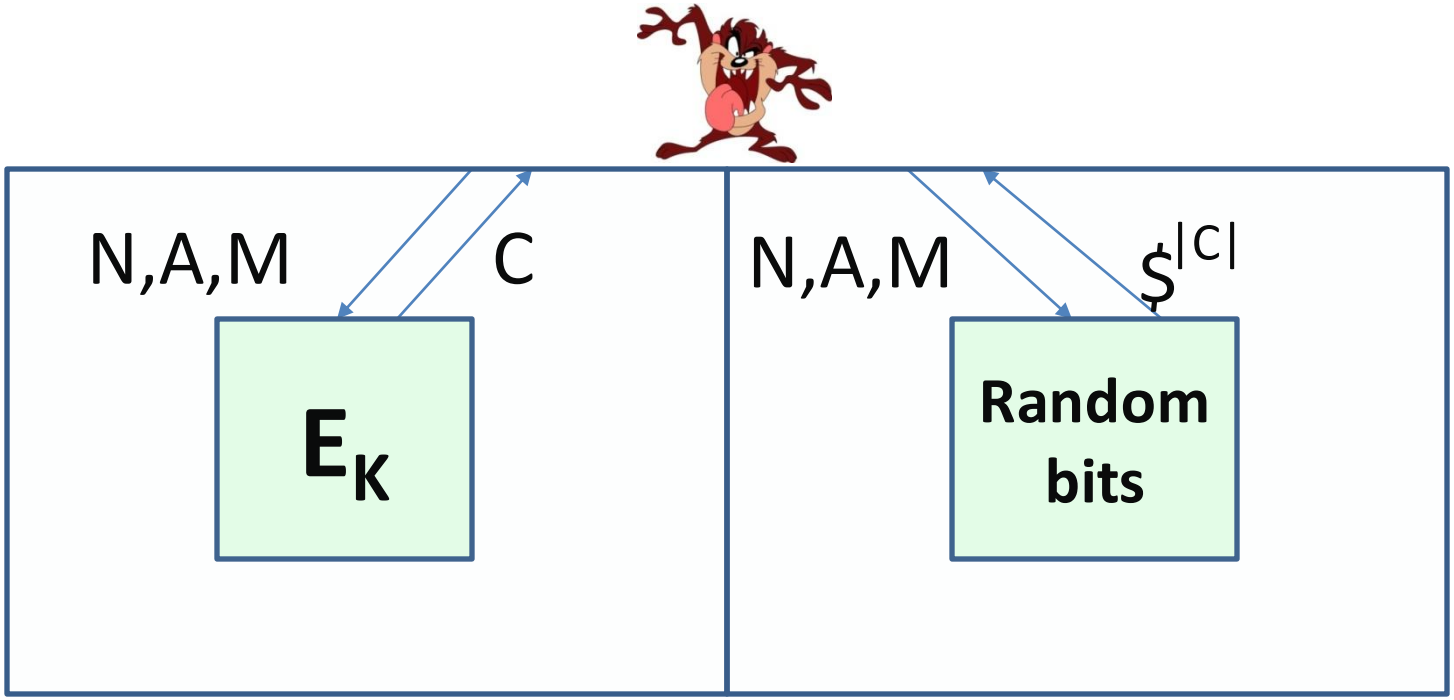
Decryption: $M/\perp \leftarrow D_K(A, N, C)$ (deterministic)

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



AE Confidentiality

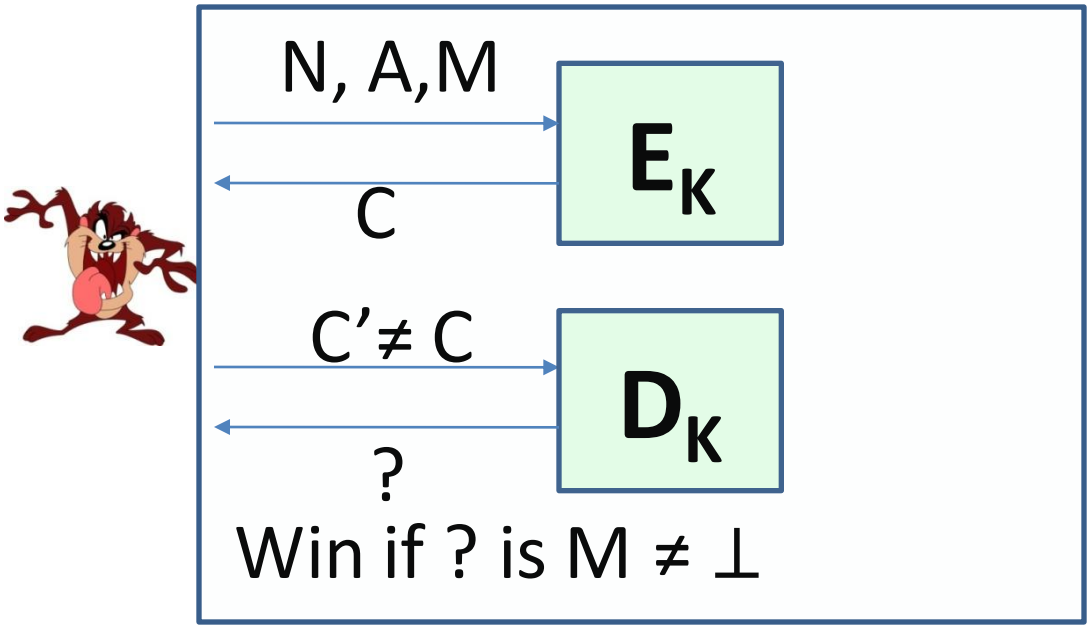
- **$IND-CPA**



Adversary is nonce respecting

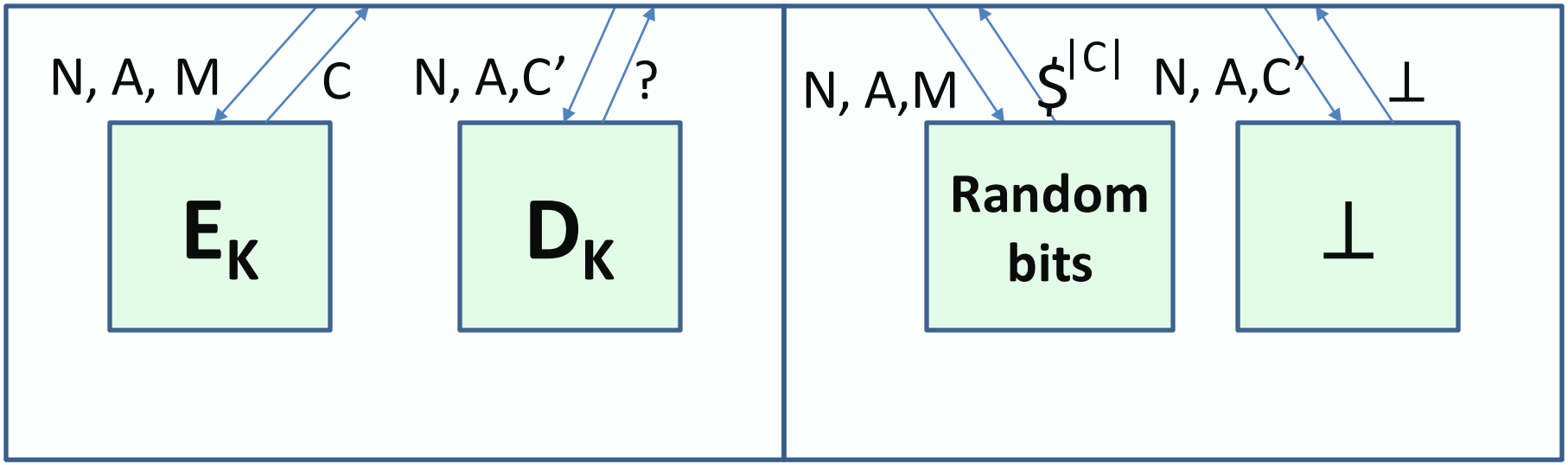
AE Integrity

- **INT-CTXT**



Adversary maybe nonce respecting

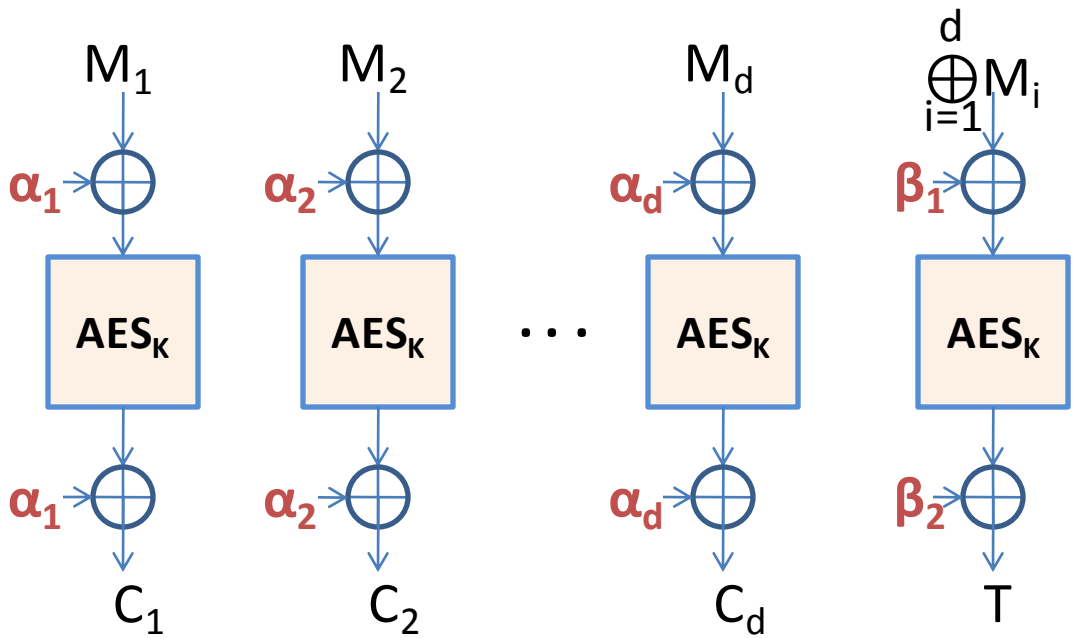
Nonce-based AE Security



Adversary is nonce respecting

Example AE with Block Cipher

OCB [RBBK'01]



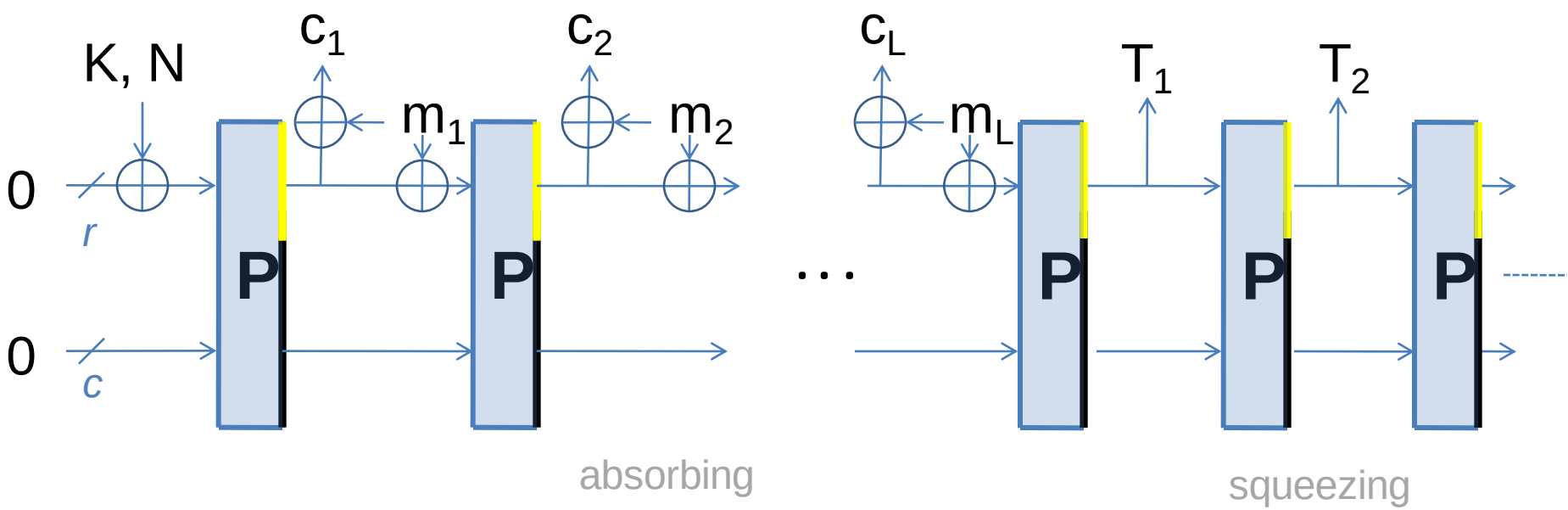
$\alpha_i = f_i(K,N)$

$\beta_i = g_i(K,N)$

If BC (AES) is SPRP, OCB is AE secure up to $2^{n/2}$ queries for non repeating N

Example AE with Permutation

Sponge Wrap [BDPV'11]



If P is an ideal permutation, Sponge Wrap is AE secure up to $\min\{2^k, 2^{c/2}\}$ queries for non repeating N

- bound follows Sponge hash indifferentiability proof
- but possibly conservative for secret K and N not repeating

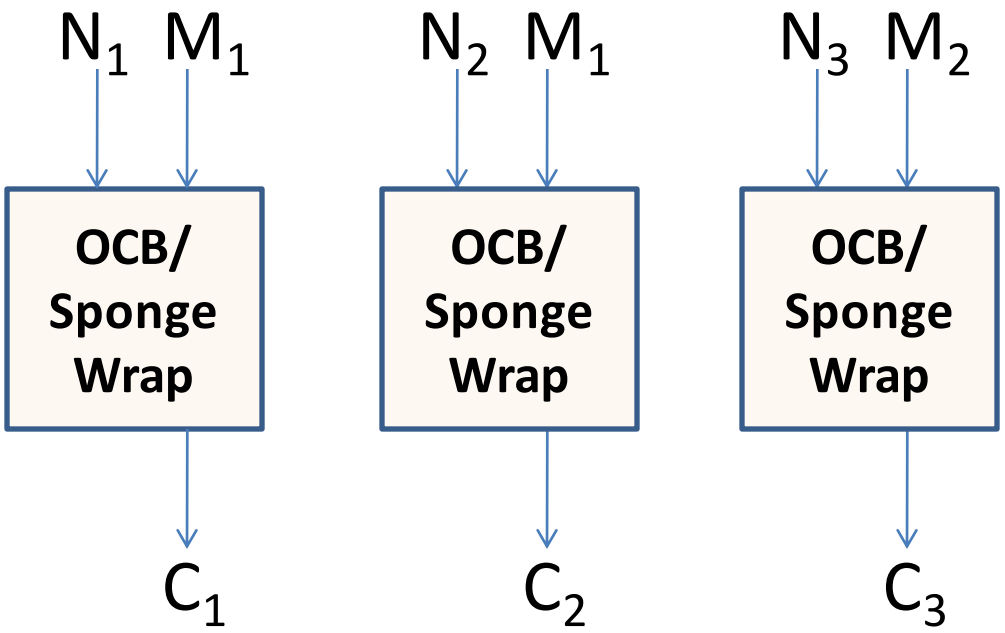
Outline

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

Nonce Misuse Resistant AE

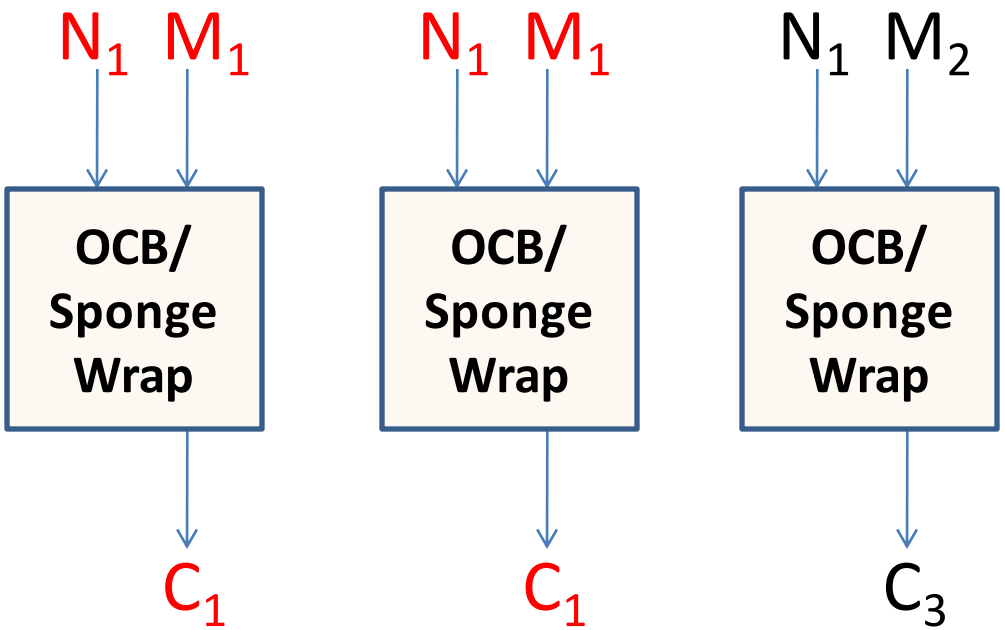
Not all security should be lost if N misused!

Distinct Nonces



Nonce Misuse
Ciphertext Repetitions

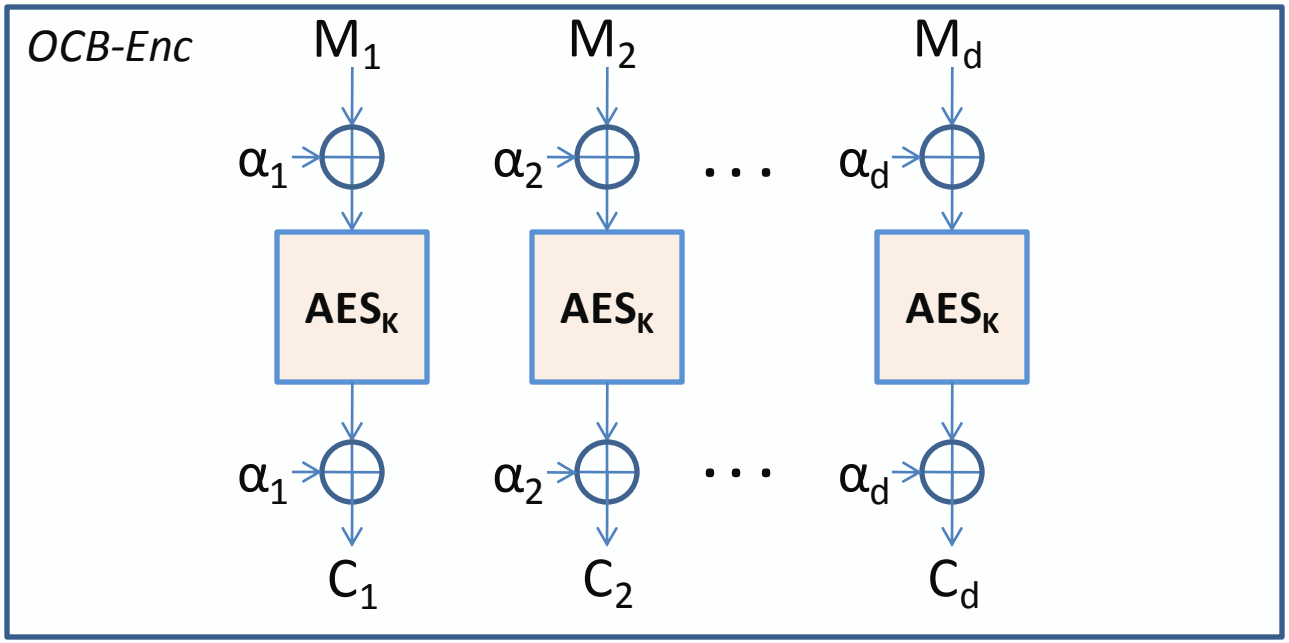
What security can be lost?



- Valid for **ALL** nonce respecting AE schemes

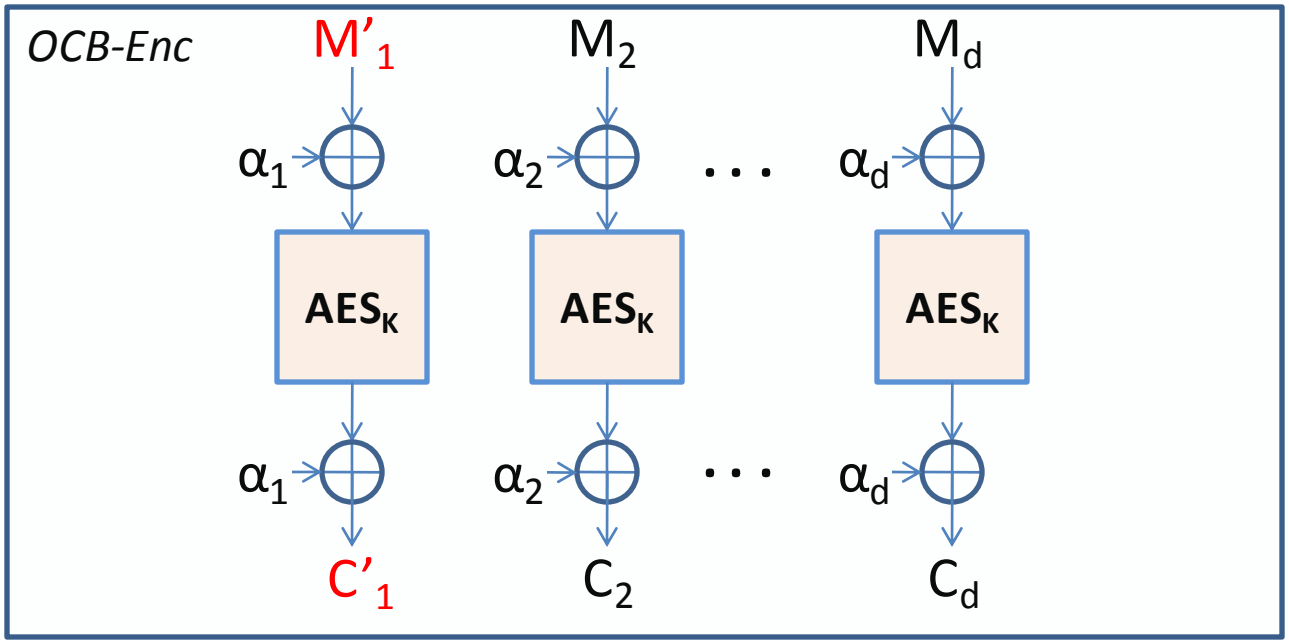
Nonce Misuse OCB
Ciphertext Block Repetitions

What else can be lost?



Nonce Misuse OCB
Ciphertext Block Repetitions

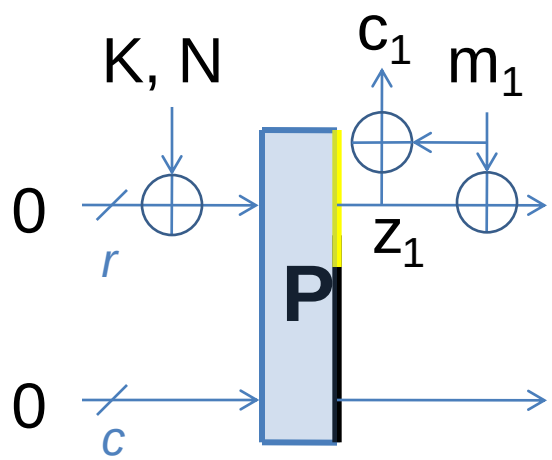
What else can be lost? (OCB looses confidentiality)

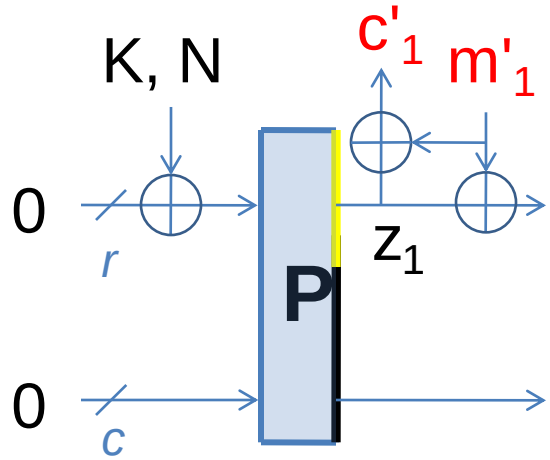


- If blocks in C repeat (over distinct OCB calls) then blocks in M repeat (OCB, IAPM, XCBC, ...)

Nonce Misuse Sponge Wrap

What else can be lost? (Sponge Wrap looses confidentiality)





$$c_1 \oplus c'_1 = m_1 \oplus m'_1$$

What to Do against Nonce Misuse?

Not all security should be lost if N misused!

1. **Security up to repetitions**

ciphertext leaks only presence of repeating Ms

MAX: SIV, BTM, HBS but two passes over the data

2. **Security up to longest common prefix**

ciphertext leaks only presence of common M prefixes

LCP: McOE-G, COPA, APE, POET

LCP + X: SpongeWrap

Nonce Misuse Resistance via Online Ciphers

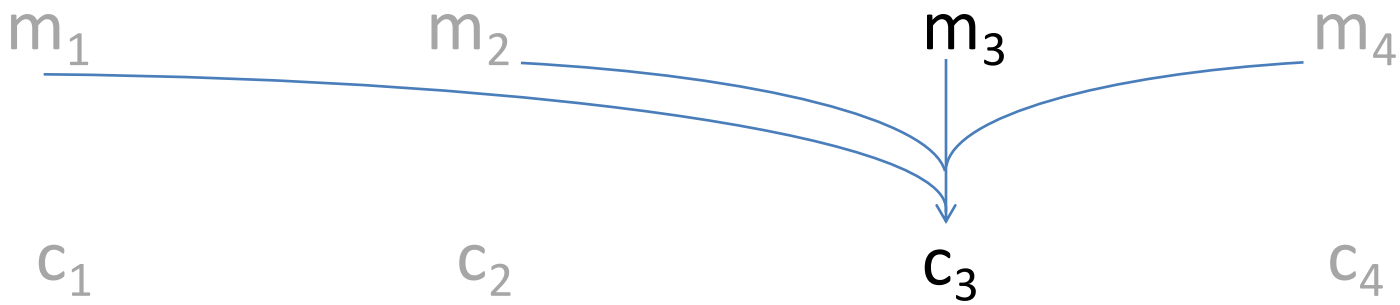
1. Online cipher + authentication [BBKN'01, FFLW'12]

nonce misuse resistant *nmr* AE scheme

secure up to common prefix repetitions

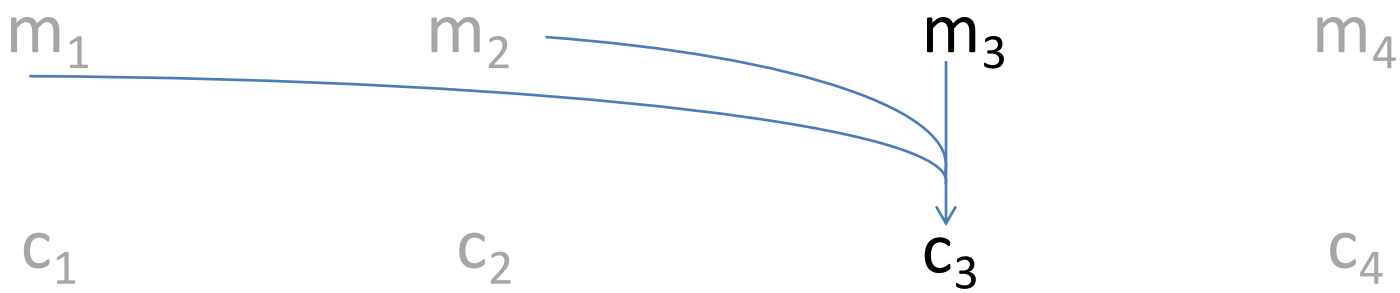
Regular vs Online Ciphers

- Normally in a cipher



- Online cipher

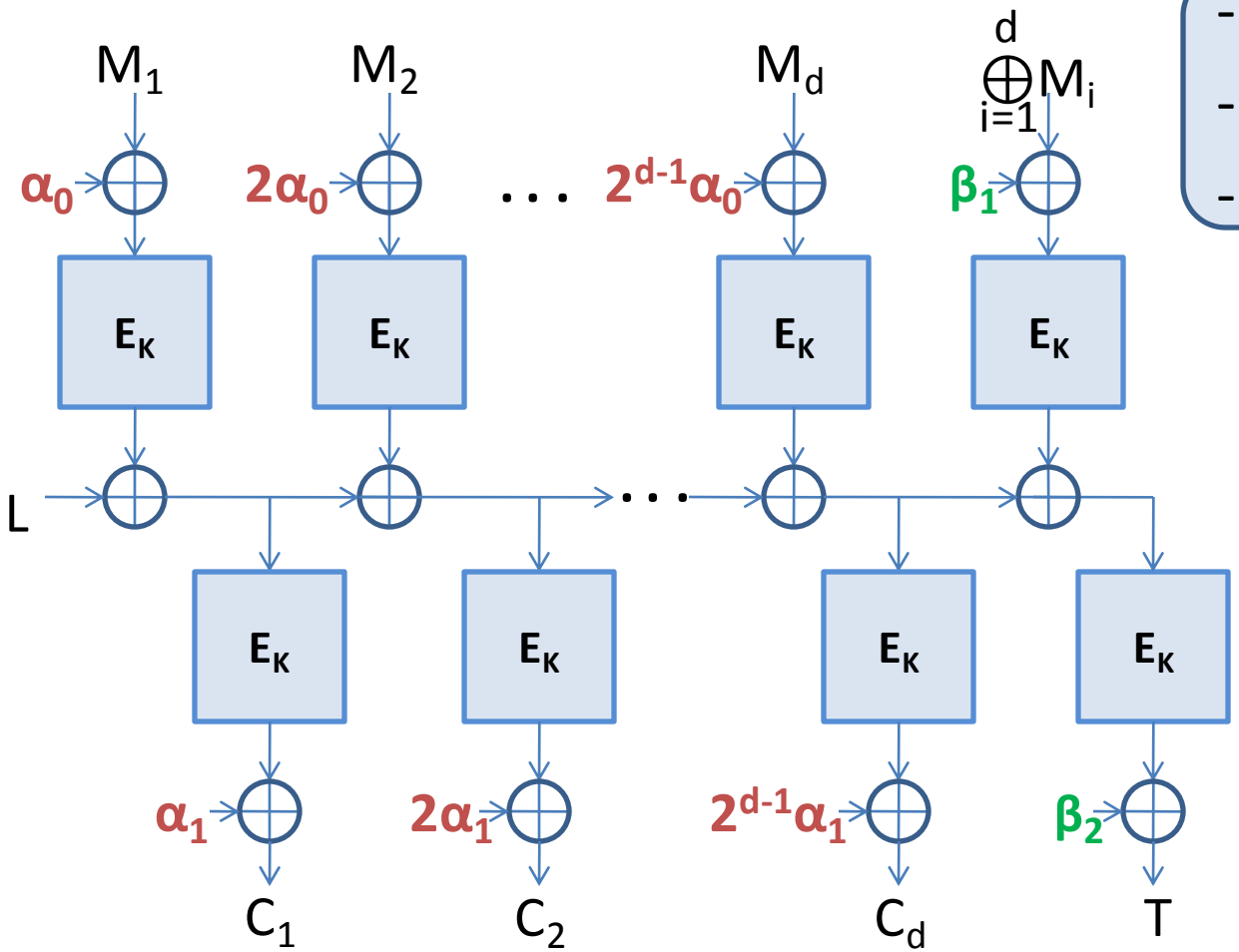
- more efficient
- different security (IND from random online permutation)



COPA [ABLMY'13]

Nonce Misuse Resistant AE

- nmr
- online
- parallelizable

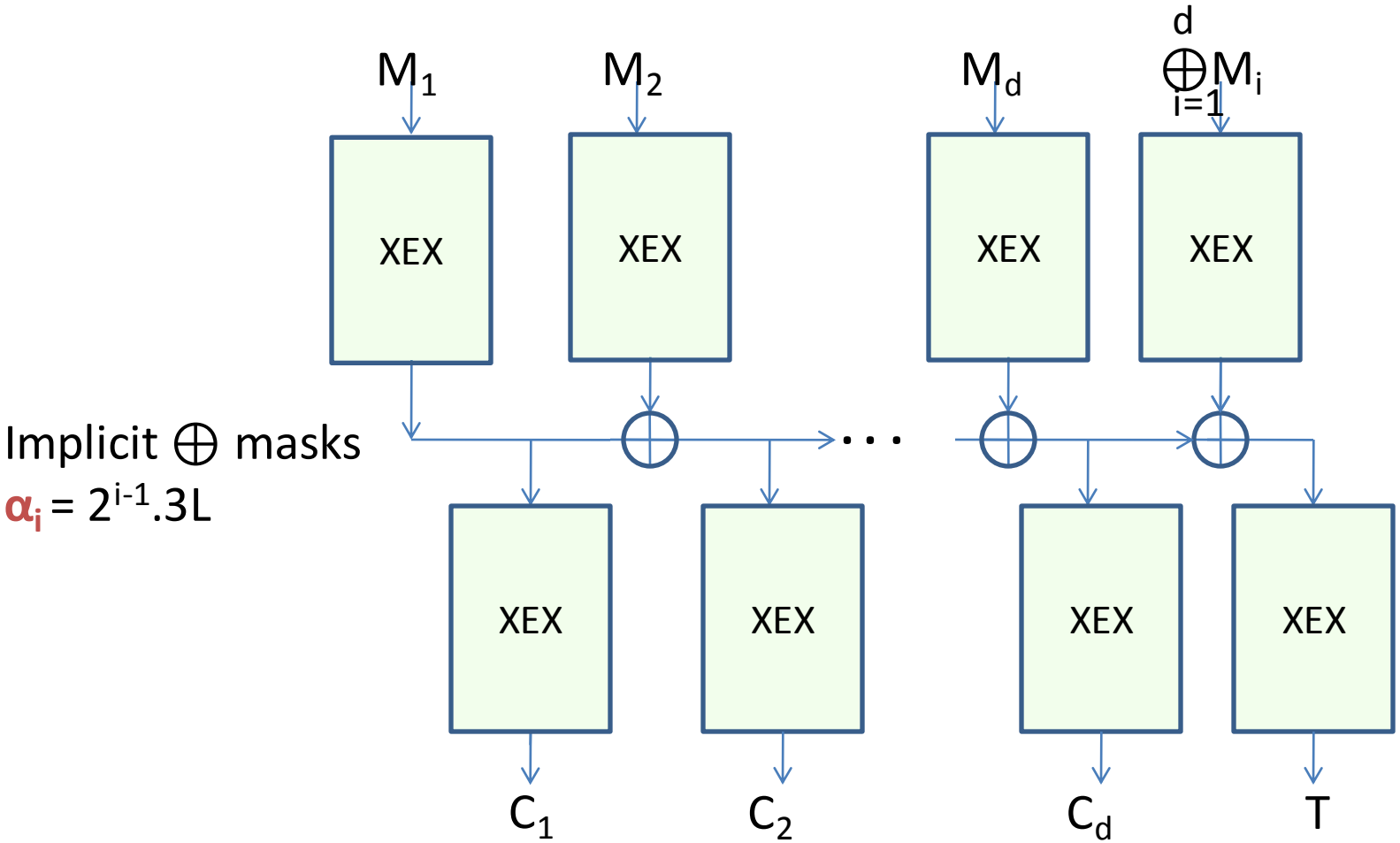


$L = E_K(0)$

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

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

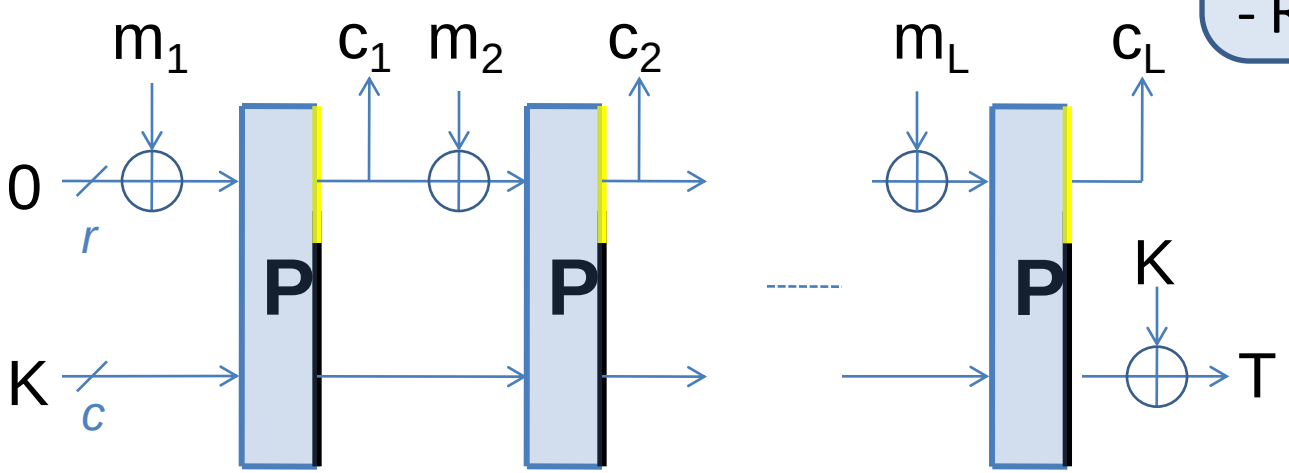
COPA
Security Proof



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

APE [ABLMNY'14]
Nonce Misuse Resistant AE

- nmr
- online
- RUP secure



If P is ideal permutation, APE is AE secure up to $2^{c/2}$ queries

Outline

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

Further Security Pitfalls in AE

What if attacker gets C decryptions before verification completed?

RUP: Release of unverified plaintext [ABLMNY'14]

- Scenarios
  - insecure memory
  - small buffer
  - 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)

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

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

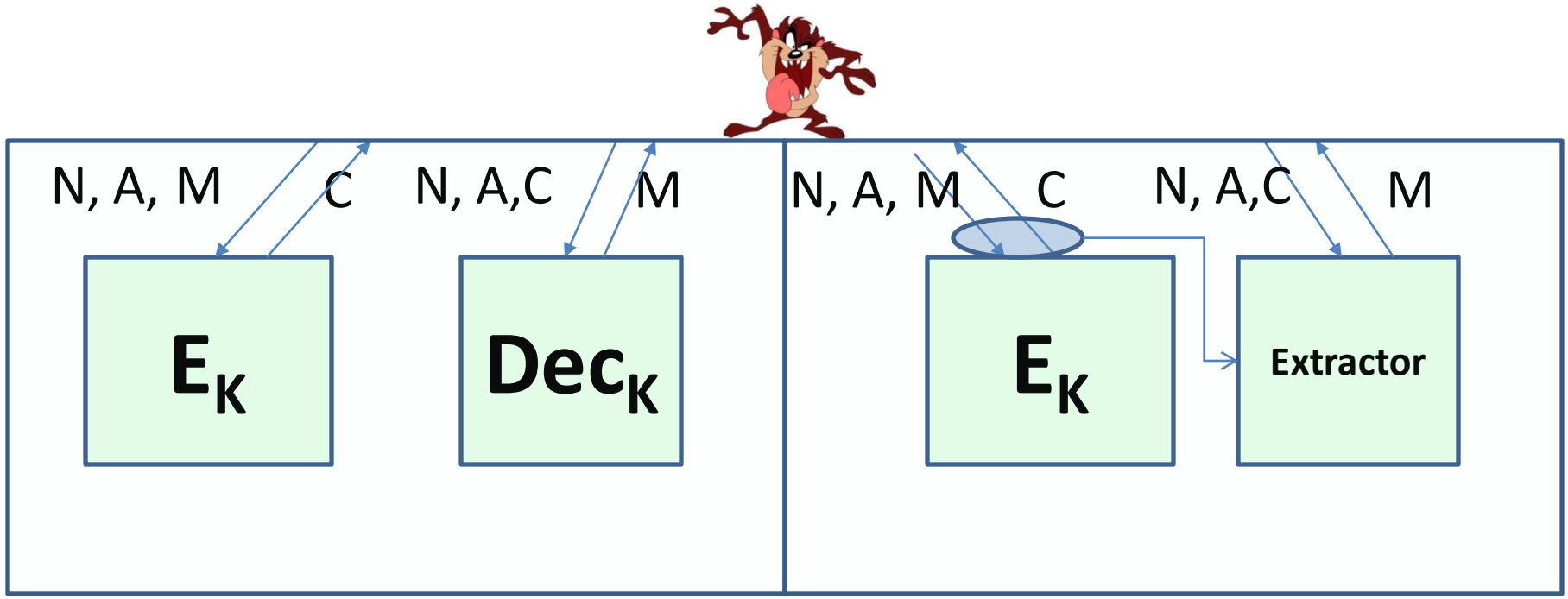
$$1/0 \leftarrow Verify_K(A, N, C, T)$$

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

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

RUP Confidentiality

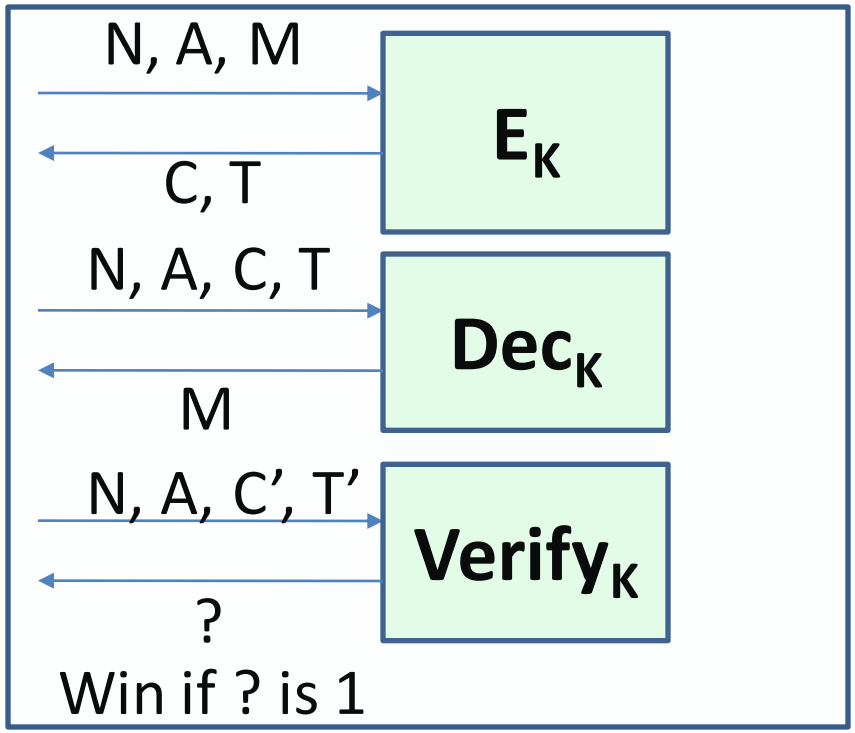
- $IND-CPA + PA1
- Plaintext awareness PA1



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, Sponge Wrap	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?

Outline

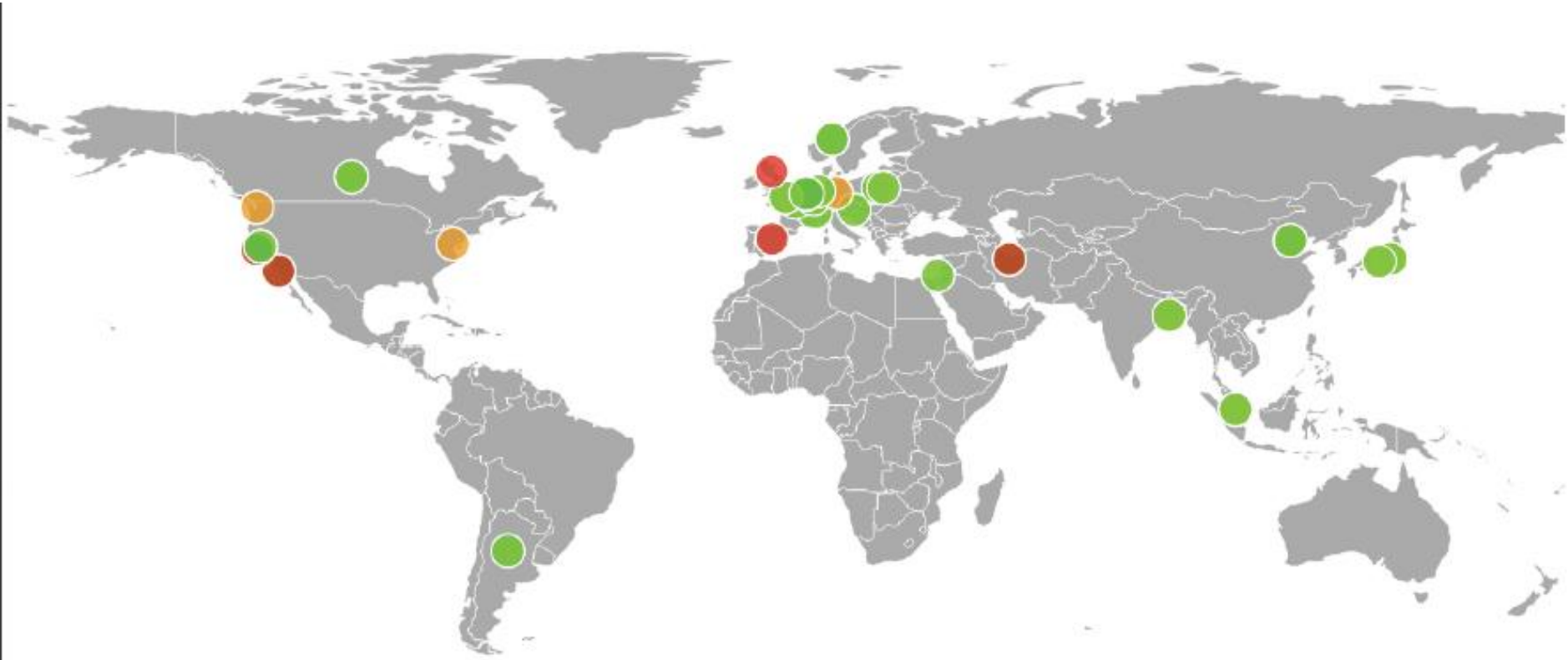
- Authenticated Encryption AE
- Generic AE composition
- Dedicated AE schemes
  - nonce-based AE
  - nonce misuse resistant AE
- Further challenges
- CAESAR AE competition

CAESAR Competition

Competition for Authenticated Encryption: Security, Applicability, and Robustness

- Follows NIST AES, EU NESSIE, EU eStream, and NIST SHA-3 and is co-funded by NIST
- Need for secure and efficient authenticated encryption
- Winner should offer advantages over AES-GCM and be suitable for widespread adoption

CAESAR Submissions



- 57 submissions in march 2014
- 7 withdrawals

CAESAR Timeline

- Jan 2015 – announcement 2nd round candidates
- Dec 2015 – announcement 3rd round candidates
- Dec 2016 – announcement of finalists
- Dec 2017 – announcement of final portfolio

CAESAR Candidate Characteristics

- Online +
- Parallelizable +
- Nonce misuse resistant +
- Release of unverified plaintext RUP +
- Underlying primitive
- Inverse free +
- Efficient +

CAESAR Classification

https://aezoo.compute.dtu.dk

#	AE Scheme	Type (BC or P)	Parallelizable (E/D)	Online (E/D)	NMR Nonce misuse resistance	Inverse free	Status
1	ACORN	Other					
2	++AE	BC	Partly/Partly			No	
3	AEGIS	BC				No	
4	AES-CMCC	BC					
5	AES-COBRA	BC	Partly/Partly	Fully/Fully		Yes	Withdrawn
6	AES-COPA	BC	Partly/Partly	Fully/Fully		No	
7	AES-CPFB	BC	Fully/No	Fully/Fully		Yes	
8	AES-JAMBU	BC	No/No			Yes	
9	AES-OTR	BC	Fully/Fully	Fully/Fully	A+N	Yes	
10	AEZ	BC	Fully/Fully		MAX	No	
11	Artemia	P/Sponge	No/No	Fully/Fully		Yes	
12	Ascon	P/Sponge	No/No	Fully/Fully		Yes	
13	AVALANCHE	BC	Fully/Fully	Fully/Fully			
14	Calico						
15	CBA	BC	Fully/Fully	Fully/Fully			
16	CBEAM						Withdrawn
17	CLOC	BC	No/No	Fully/Fully			

CAESAR Classification

https://aezoo.compute.dtu.dk

#	AE Scheme	Type (BC or P)	Parallelizable (E/D)	Online (E/D)	NMR Nonce misuse resistance	Inverse free	Status
18	Deoxys						
19	ELmD	BC	Partly/Partly	Fully/Fully		No	
20	Enchilada	BC	Fully/Fully	Fully/Fully	None	Yes	
21	FASER						Withdrawn
22	HKC						Withdrawn
23	HS1-SIV	Other	Fully/Fully	No/No	MAX	Yes	
24	ICEPOLE	P/Sponge	Fully/Fully	Fully/Fully	LCP+X	Yes	
25	iFeed[AES]	BC	Fully/No	Fully/Fully	LCP+X	Yes	
26	Joltik	BC	Fully/Fully, Partly/Partly	Fully/Fully, Fully/Fully	None, LCP	No, No	
27	Julius	BC	Fully/Fully	No/No	MAX	Yes, No	
28	Ketje	P/Sponge	No/No				
29	Keyak						
30	KIASU	BC	Fully/Fully, Partly/Partly	Fully/Fully, Fully/Fully	None, LCP	No, No	
31	LAC	BC	No/No	Fully/Fully	None	No	
32	Marble	BC	Partly/Partly	Fully/Fully	A+N/MAX	No	

CAESAR Classification

https://aezoo.compute.dtu.dk

#	AE Scheme	Type (BC or P)	Parallelizable (E/D)	Online (E/D)	NMR Nonce misuse resistance	Inverse free	Status
33	McMambo	LRX	No/No	Fully/Fully		No	Withdrawn
34	Minalpher						
35	MORUS	Other	No/No	Fully/Fully	A+N/LCP+X	N/A	
36	NORX	P/Sponge	Fully/Fully	Fully/Fully	A+N/LCP+X	Yes	
37	OCB	BC	Fully/Fully	Fully/Fully	None	No	
38	OMD						
39	PAEQ						
40	PAES	AES					Withdrawn
41	PANDA						Withdrawn
42	π-Cipher	P/Sponge	Fully/Fully	Fully/Fully	None	Yes	
43	POET	BC/AES					POET-G withdrawn
44	POLAWIS	Other					
45	PRIMATEs	P/Sponge					
46	Prøst	P	Partly/Partly, Fully/Fully, No/No	Fully/Fully		Yes, No, Yes	
47	Raviyoyla	Other					

CAESAR Classification

https://aezoo.compute.dtu.dk

#	AE Scheme	Type (BC or P)	Parallelizable (E/D)	Online (E/D)	NMR Nonce misuse resistance	Inverse free	Status
48	Sablier	Other					
49	SCREAM	BC	Fully/Fully	Fully/Fully	None	No	
50	SHELL	BC	Partly/Partly	Fully/Fully		No	
51	SILC	BC	No/No	Fully/Fully	A+N	Yes	
52	Silver	BC					
53	STRIBOB	P/Sponge	No/No	Fully/Fully	A+N	Yes	
54	Tiaoxin	BC	No/No	Fully/Fully	None	Yes	
55	TriviA-ck	Other	No/No	No/No	A+N	N/A	
56	Wheesht	Other			None	N/A	
57	YAES	BC	Fully/Fully	Fully/Fully	None	Yes	

Software comparison:

http://www1.spms.ntu.edu.sg/~syllab/speed/

More Features …

- Further features:
  - Incrementality, tag truncation, ciphertext expansion, secret msg number, etc.
  - Side channel resistance
  - Distinctive security properties
  - …
- AE design categories

  (nonce-based vs nonce misuse resistant, software, hardware, etc.)

Thank you!

Elena.Andreeva@esat.kuleuven.be