COBRA: A Parallelizable Authenticated Online Cipher without Block Cipher Inverse[1]

Atul Luykx

COSIC
KU Leuven and iMinds

March 3, 2014

[1] Joint work with E. Andreeva, B. Mennink, and K. Yasuda.

Overview

COBRA

1. Misuse resistance
2. Online
3. GCM-like efficiency
4. No block cipher inverse
5. Security reduction to block cipher

Background: Misuse Resistance

Nonces cannot always be guaranteed unique:

1. Flawed implementations
2. Reset during backup
3. State of virtual machine copied

Background: Misuse Resistance

Nonces cannot always be guaranteed unique:

1. Flawed implementations
2. Reset during backup
3. State of virtual machine copied

SIV ('06, Rogaway and Shrimpton), BTM ('09, Iwata and Yasuda), HBS ('09, Iwata and Yasuda)

Background: Misuse Resistance

Nonces cannot always be guaranteed unique:

1. Flawed implementations
2. Reset during backup
3. State of virtual machine copied

SIV ('06, Rogaway and Shrimpton), BTM ('09, Iwata and Yasuda), HBS ('09, Iwata and Yasuda)

1. High latency (receive full message before first output)
2. Storage issues (large internal state)

Background: Misuse Resistance

Nonces cannot always be guaranteed unique:

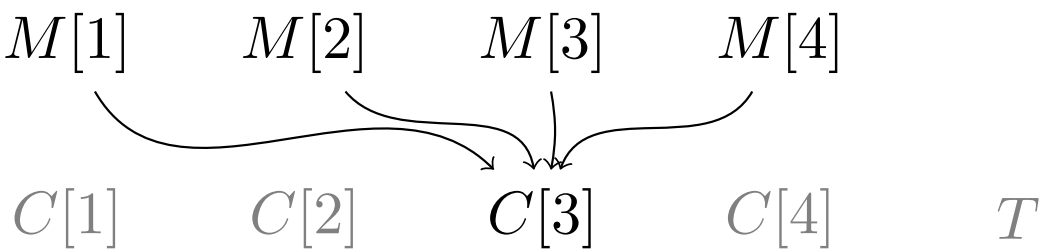
1. Flawed implementations
2. Reset during backup
3. State of virtual machine copied

SIV ('06, Rogaway and Shrimpton), BTM ('09, Iwata and Yasuda), HBS ('09, Iwata and Yasuda)

1. High latency (receive full message before first output)
2. Storage issues (large internal state)

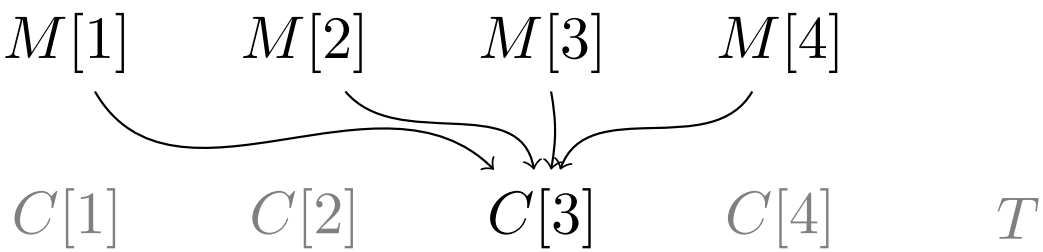
$\Rightarrow$ We want *online* schemes

Background: *Online* Scheme

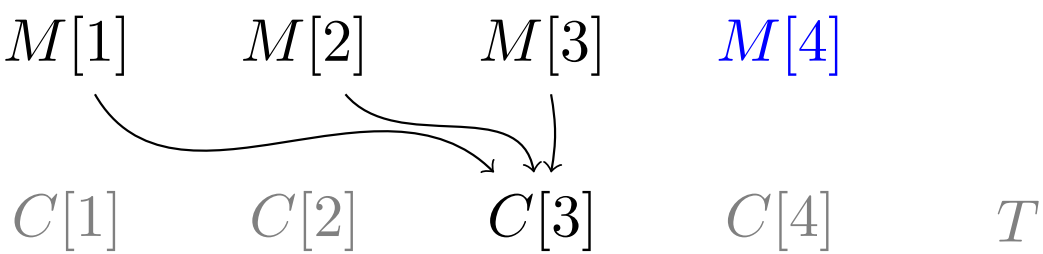


Dependency in SIV, HBS, BTM.

Background: *Online* Scheme

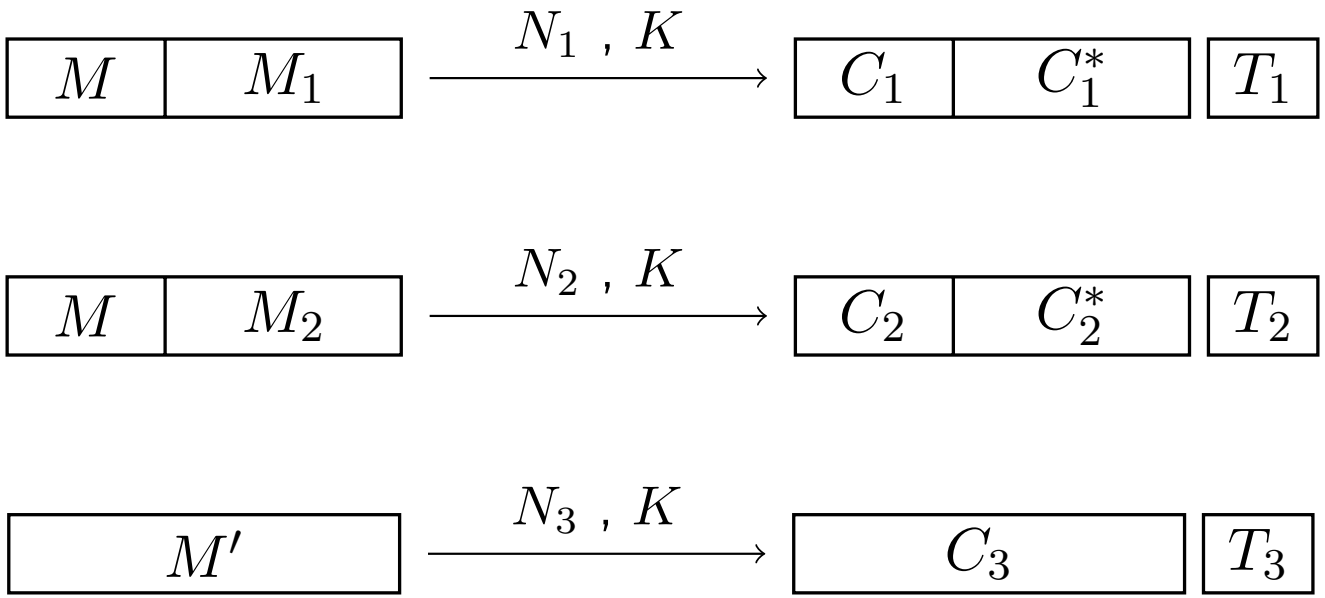


Dependency in SIV, HBS, BTM.

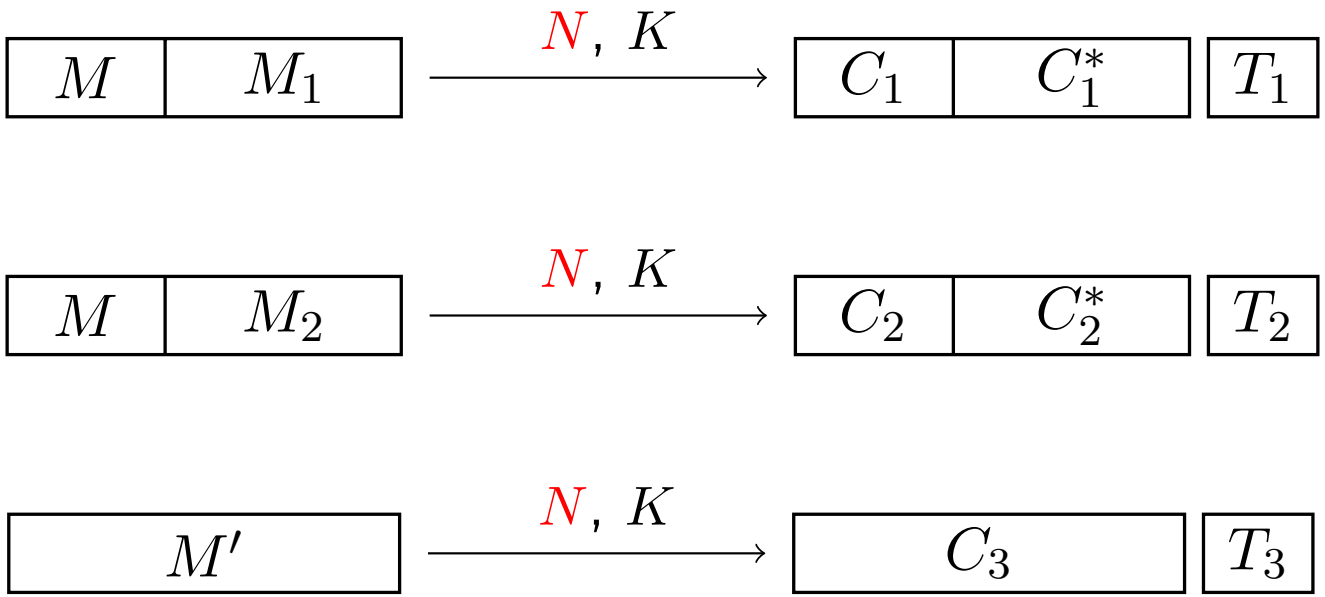


Dependency in an *online* AE scheme.

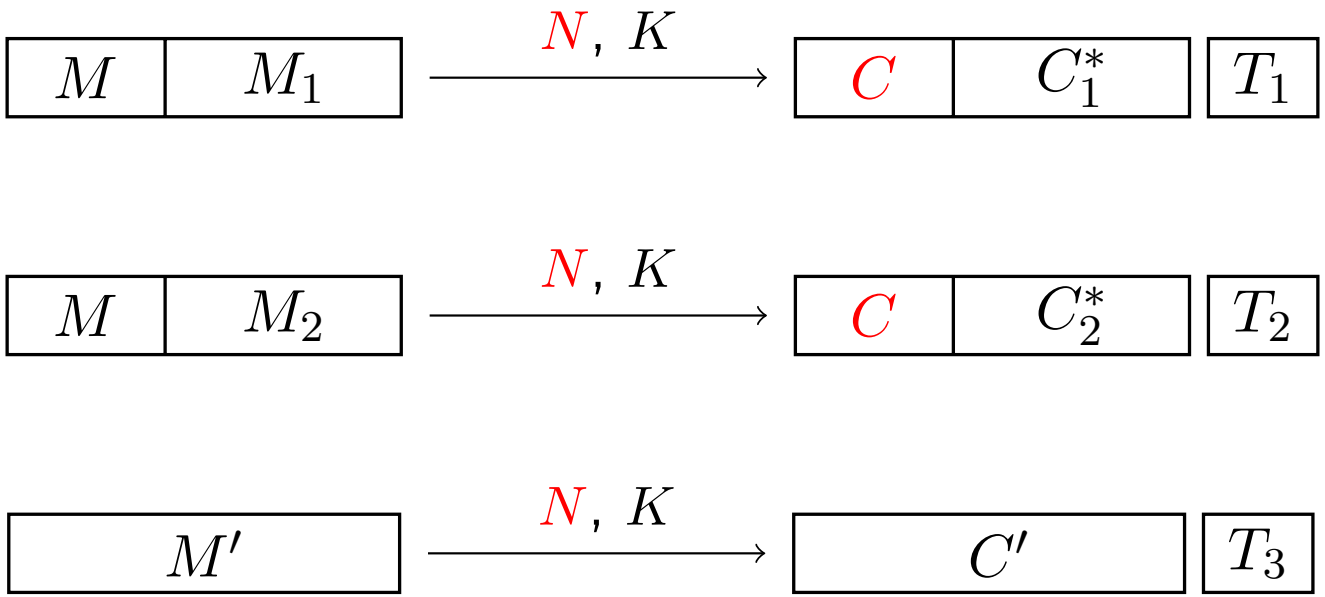
Background: *Online* Nonce Misuse



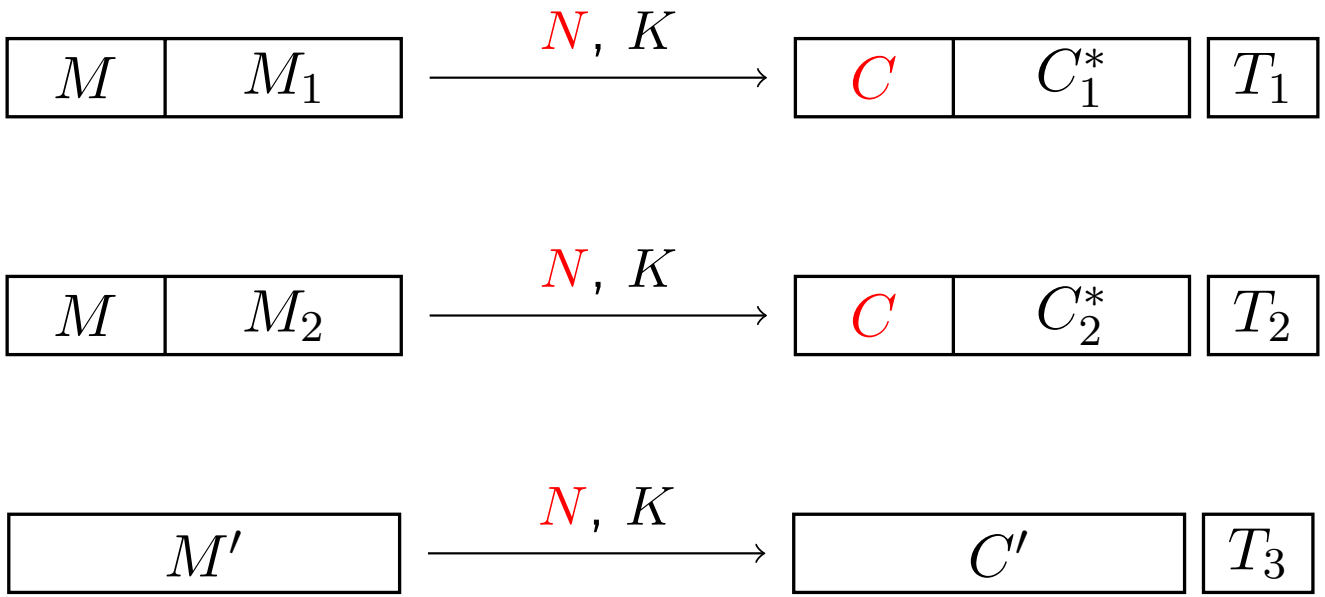
Background: *Online* Nonce Misuse



Background: *Online* Nonce Misuse

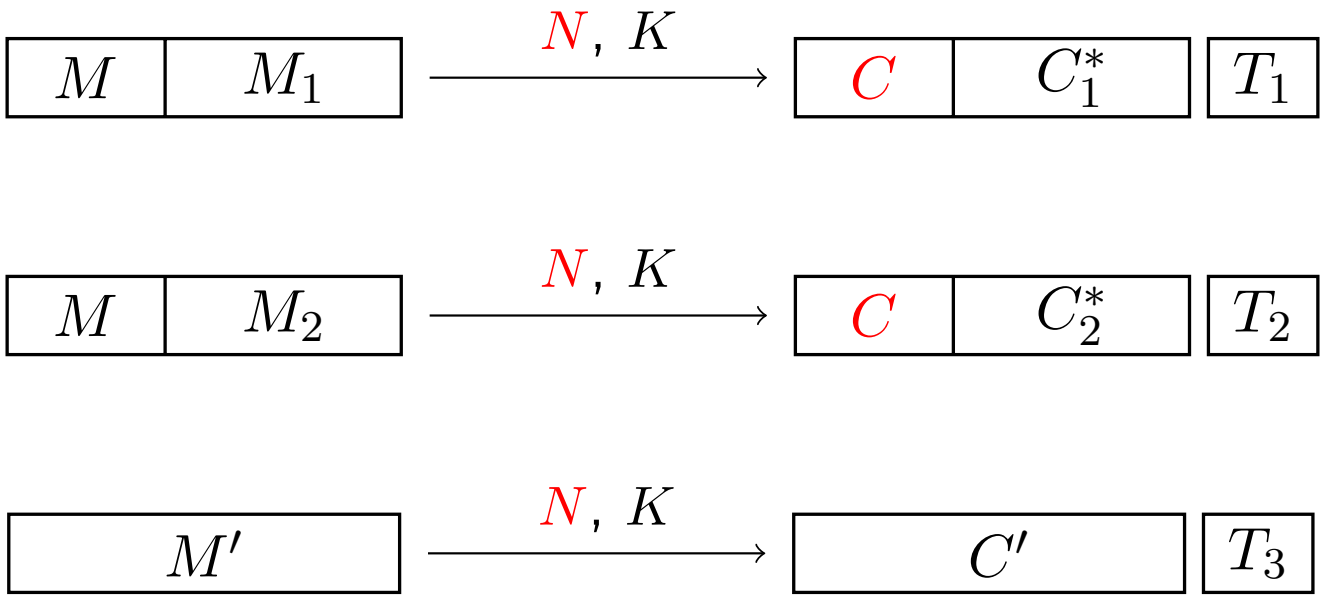


Background: *Online* Nonce Misuse



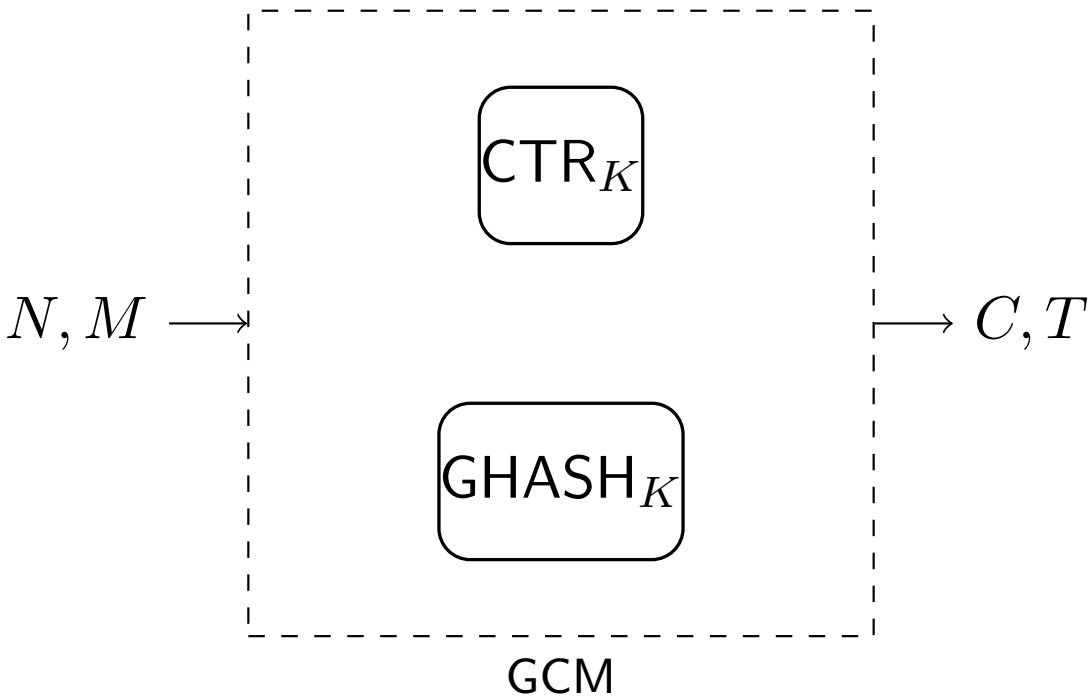
1. Equality of prefixes of messages determined

Background: *Online* Nonce Misuse

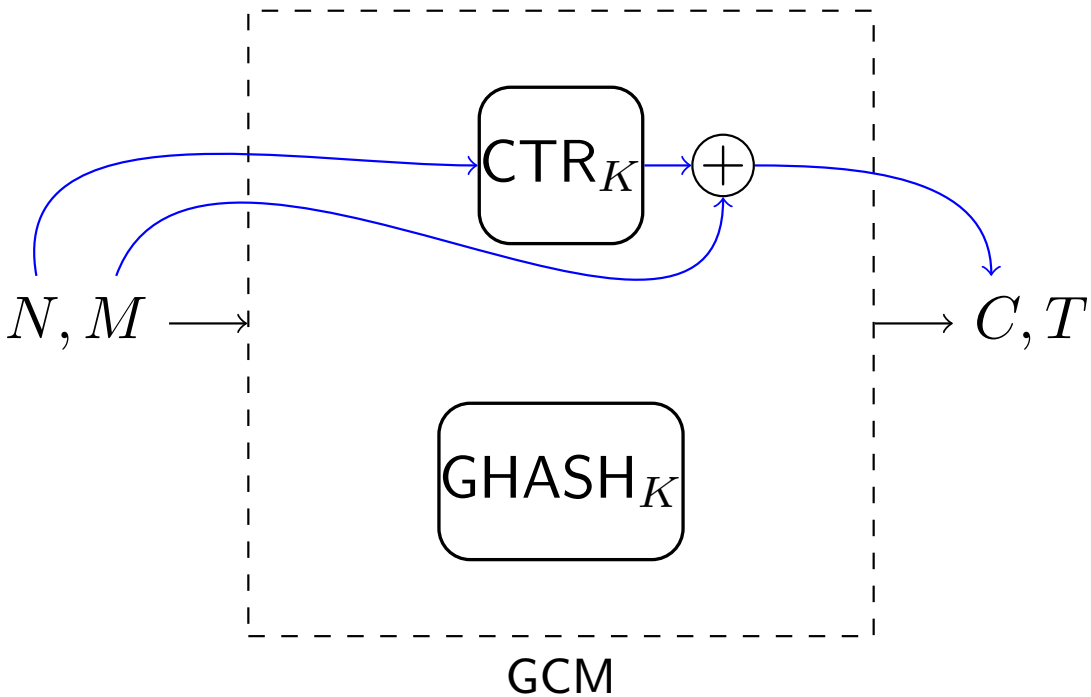


1. Equality of prefixes of messages determined
2. No relationship past common prefix

Background: GCM not Misuse Resistant



Background: GCM not Misuse Resistant



Overview

COBRA:

1. Misuse resistance
2. Online
3. GCM-like efficiency
4. No block cipher inverse
5. Security reduction to block cipher

Overview

COBRA:

1. Misuse resistance
2. Online
3. GCM-like efficiency
4. No block cipher inverse
5. Security reduction to block cipher

Motivation: Overview of Some Online Schemes

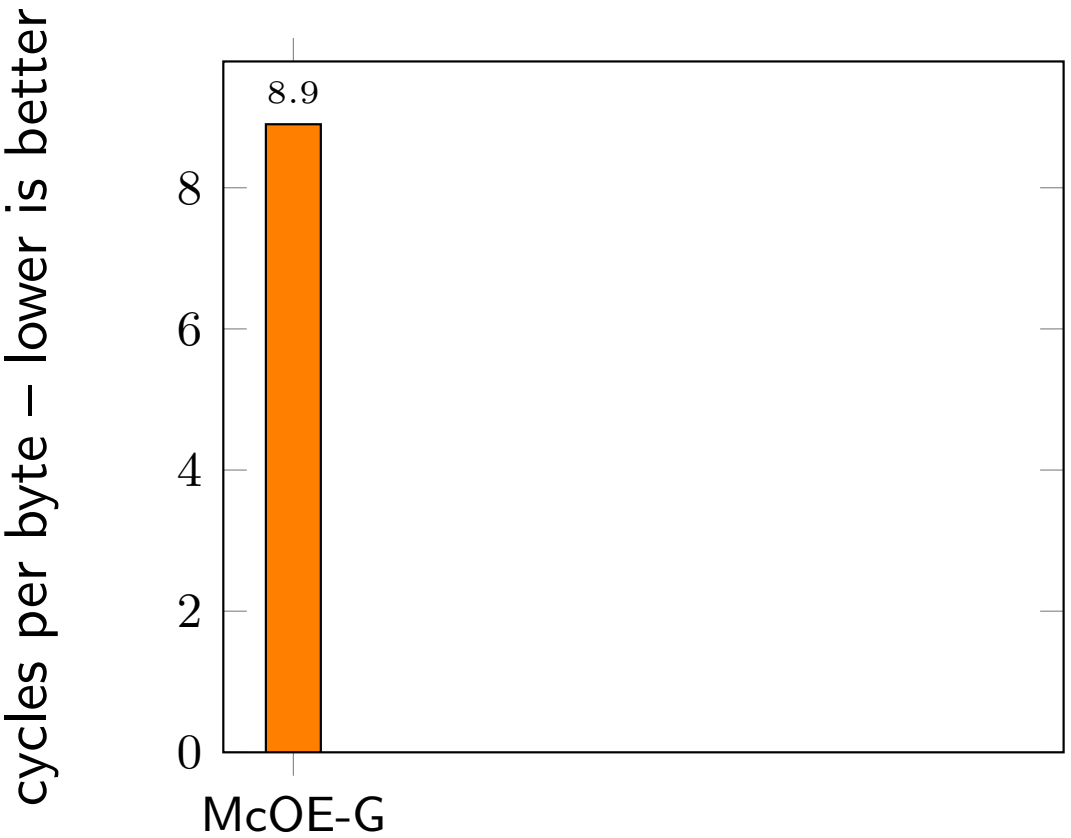


Figure : Sandy Bridge with AES-NI[2]

[2]References: Gueron DIAC 2013 and Andreeva et al. Asiacrypt 2013.

Motivation: Overview of Some Online Schemes

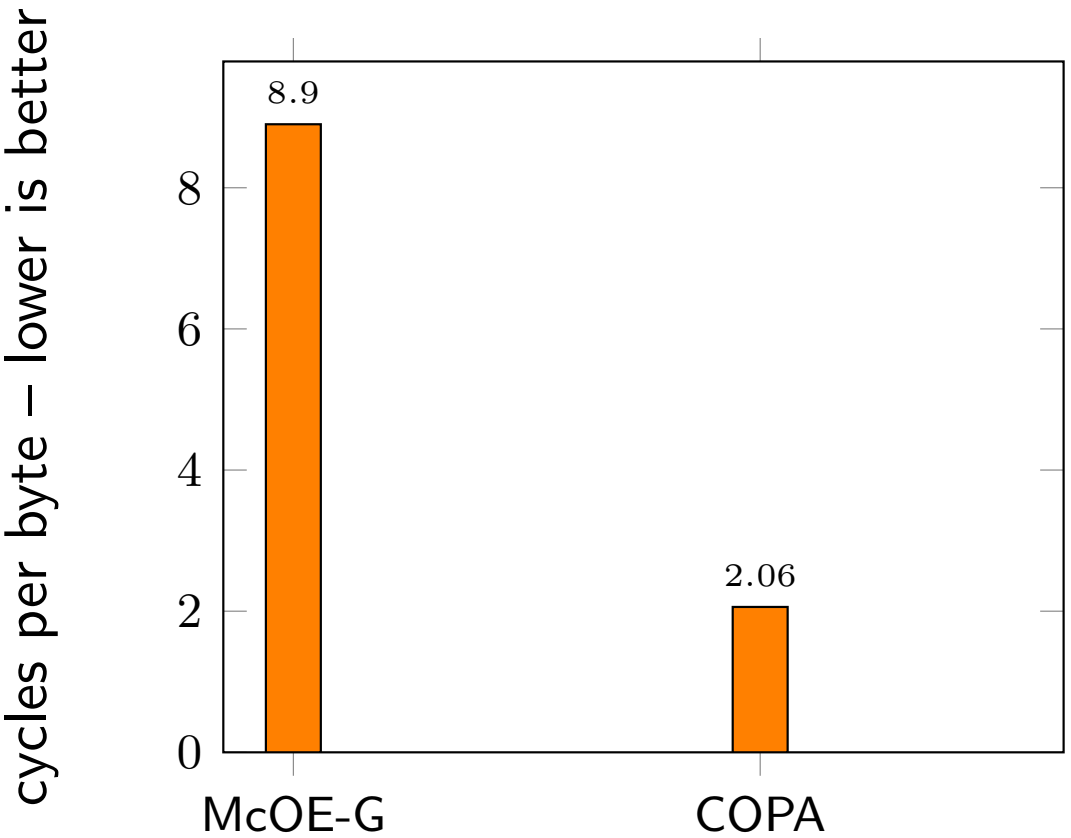


Figure : Sandy Bridge with AES-NI[2]

[2]References: Gueron DIAC 2013 and Andreeva et al. Asiacrypt 2013.

Motivation: Overview of Some Online Schemes

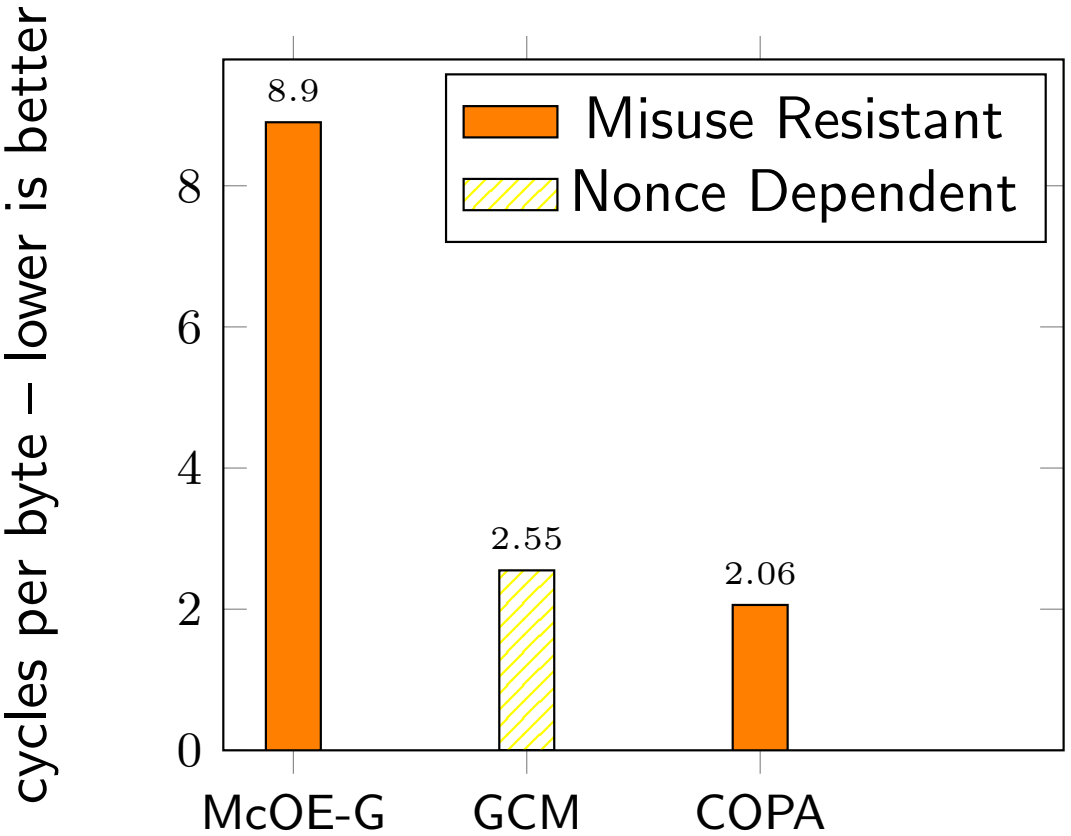


Figure : Sandy Bridge with AES-NI[2]

[2]References: Gueron DIAC 2013 and Andreeva et al. Asiacrypt 2013.

Motivation: Overview of Some Online Schemes

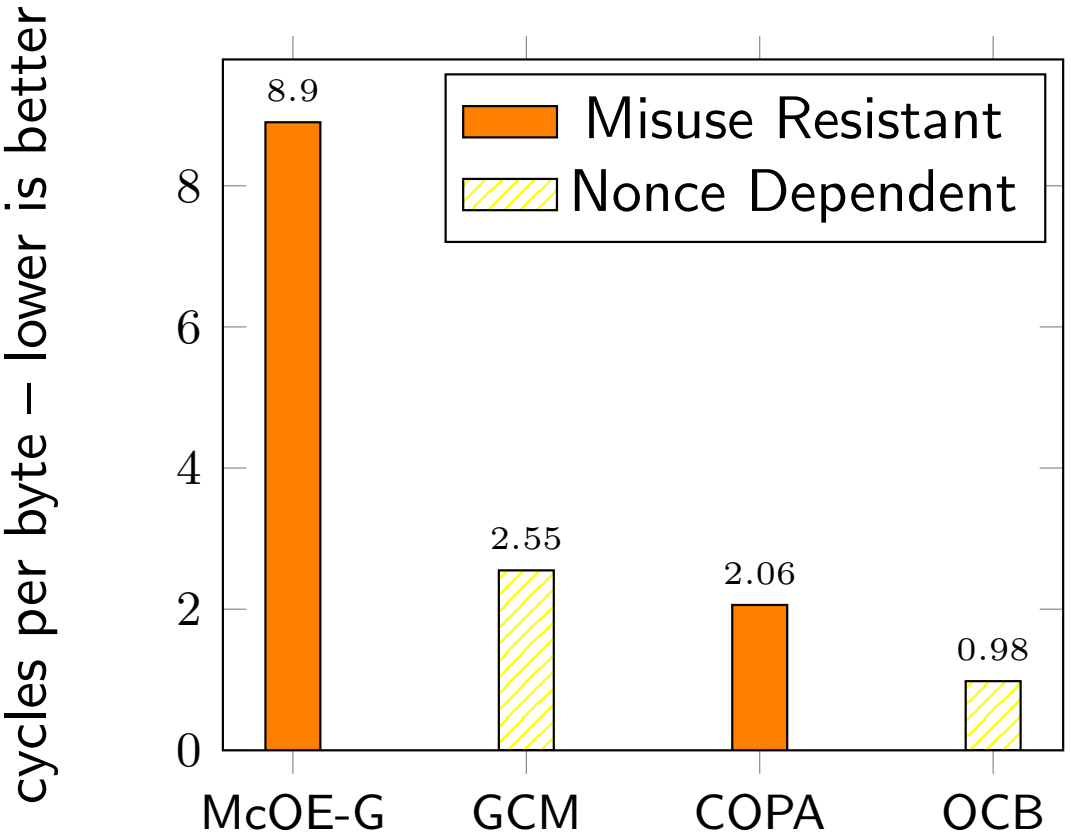


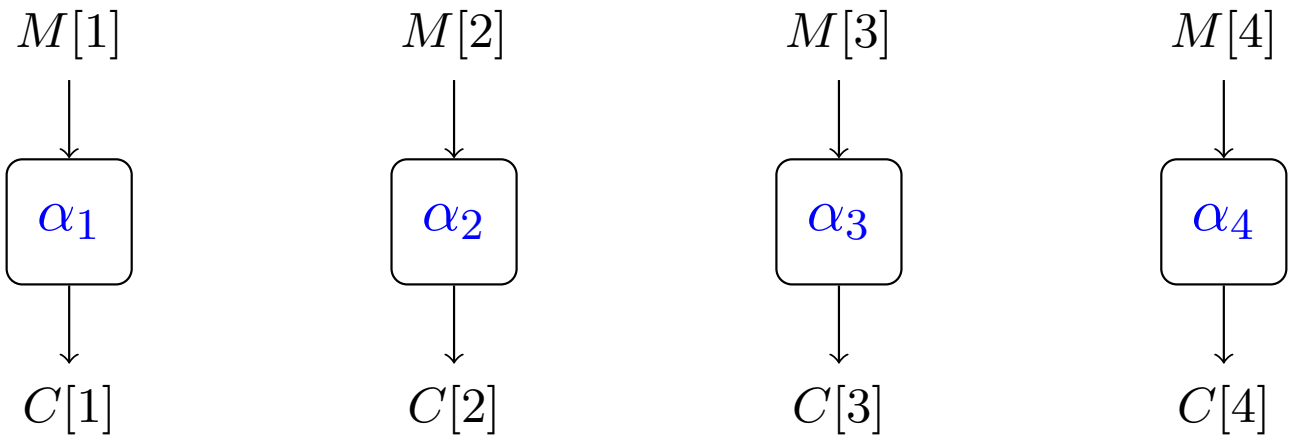
Figure : Sandy Bridge with AES-NI[2]

[2]References: Gueron DIAC 2013 and Andreeva et al. Asiacrypt 2013.

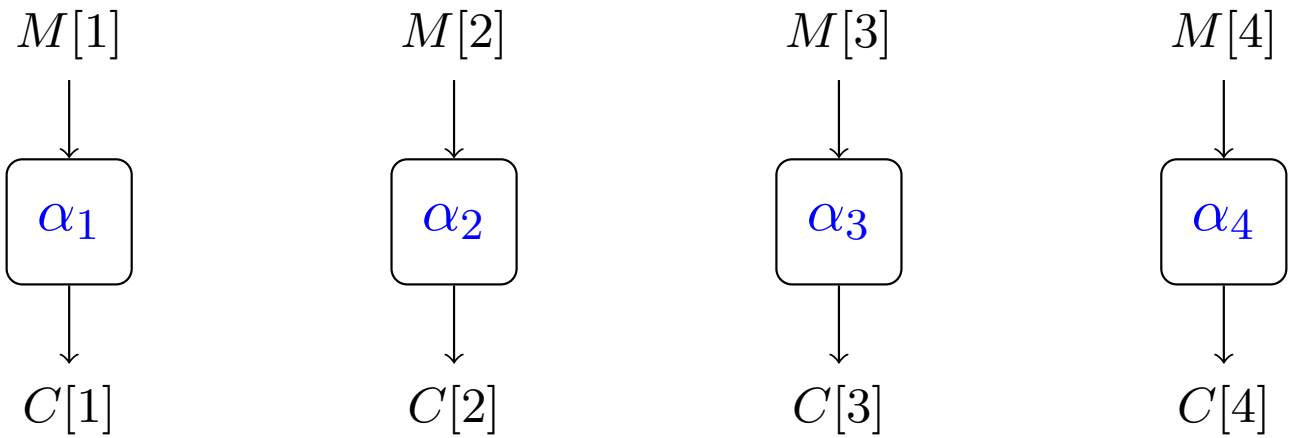
Motivation

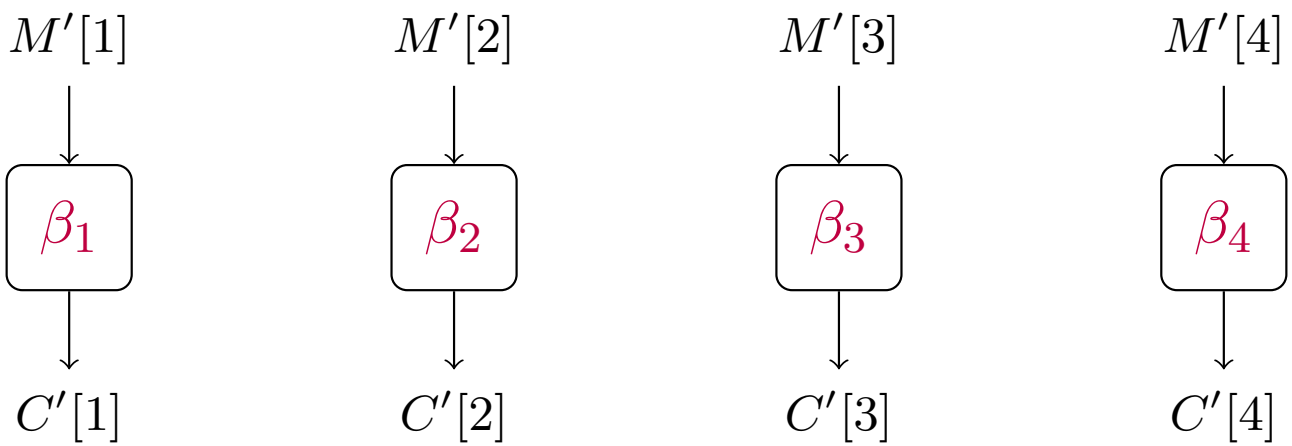
Can we close the gap in efficiency between nonce dependent and misuse resistant schemes?

Motivation: Misuse Resistance From OCB?

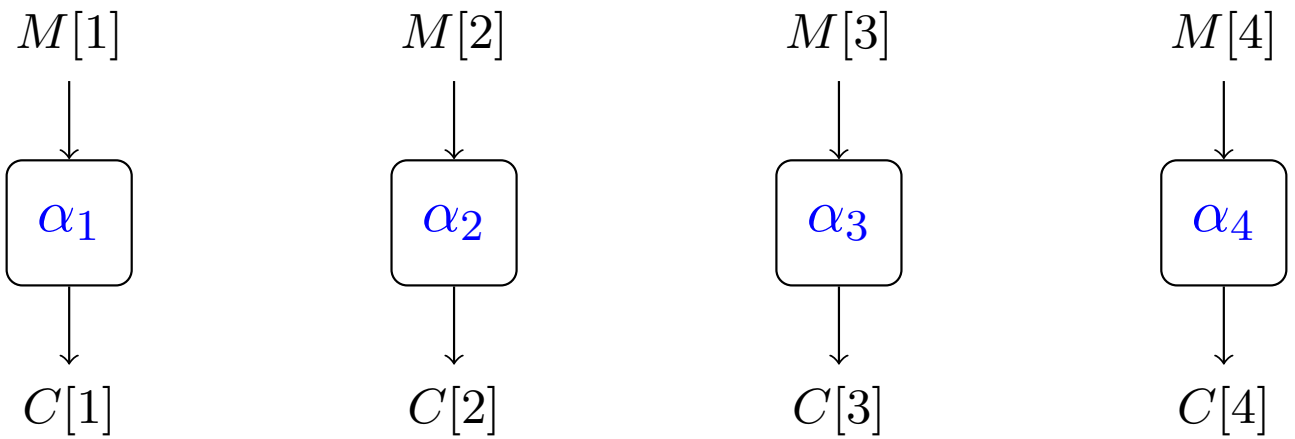


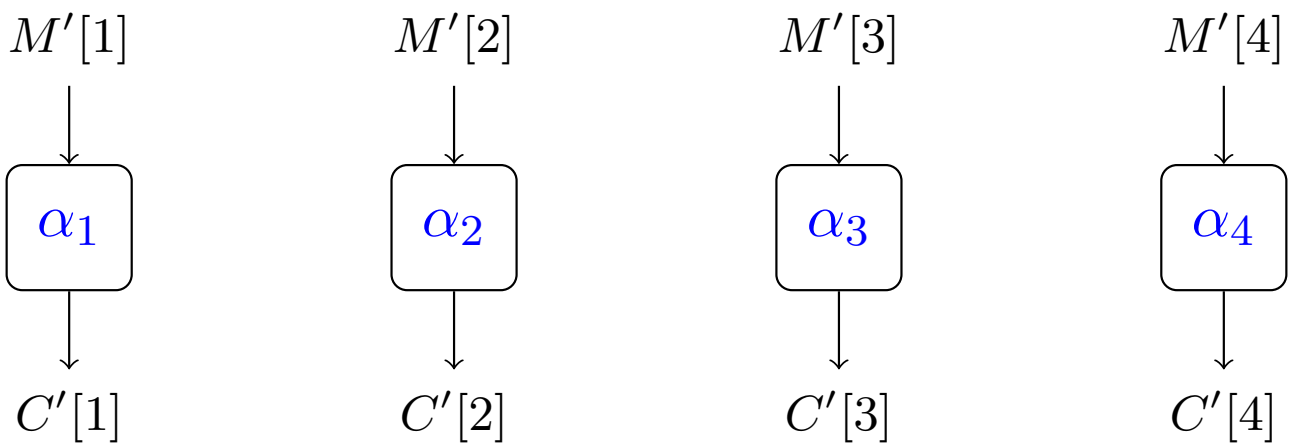
Motivation: Misuse Resistance From OCB?



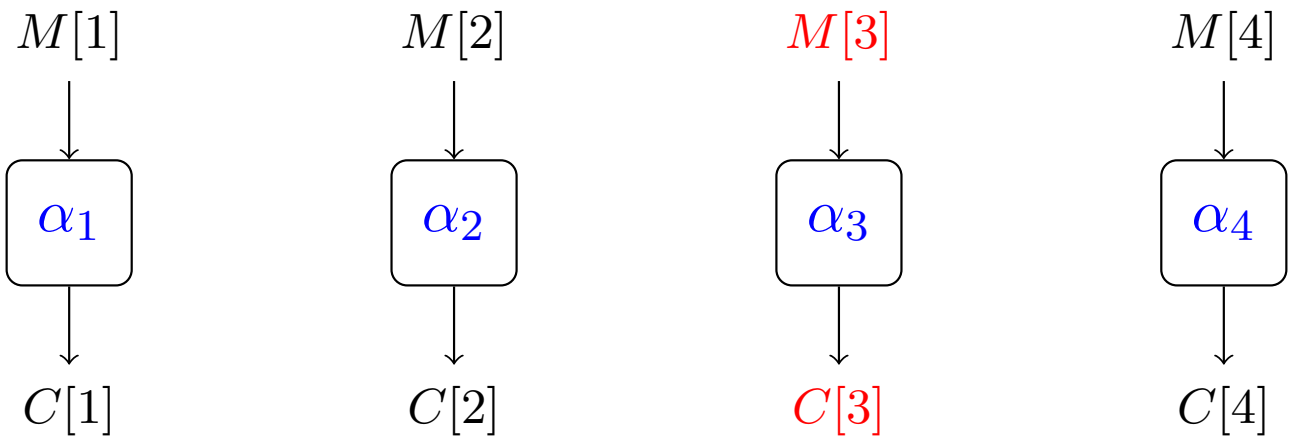


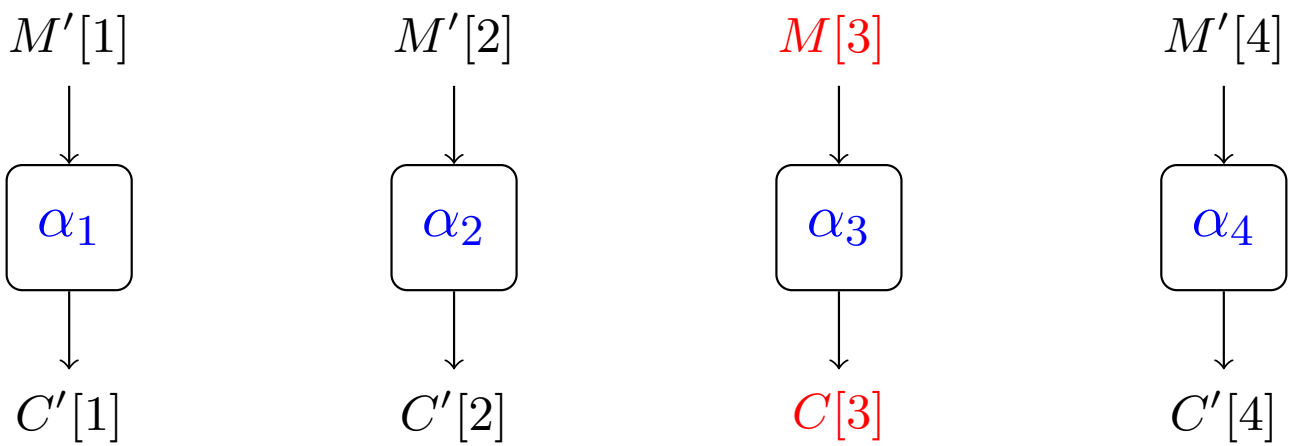
Motivation: Misuse Resistance From OCB?



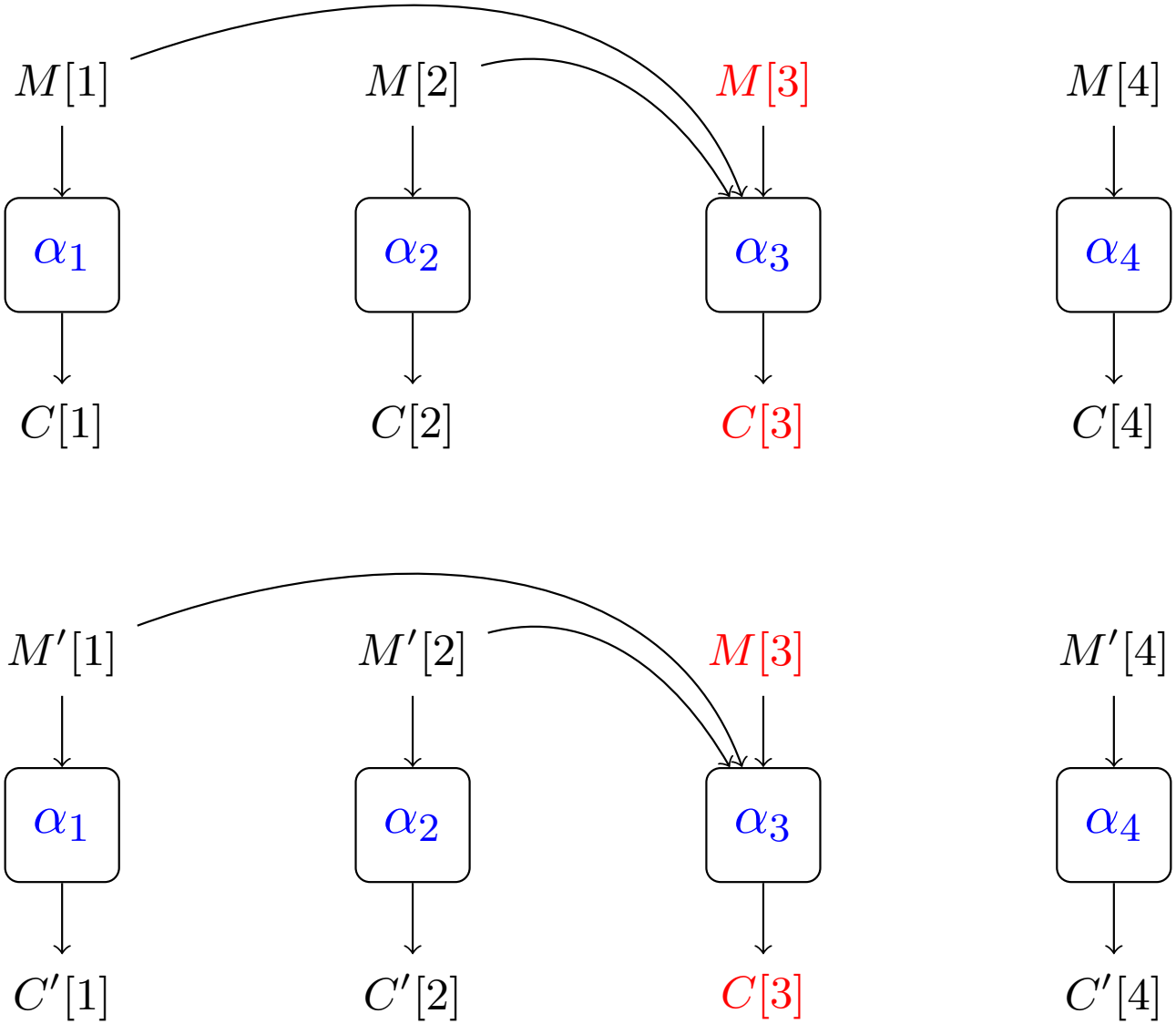


Motivation: Misuse Resistance From OCB?

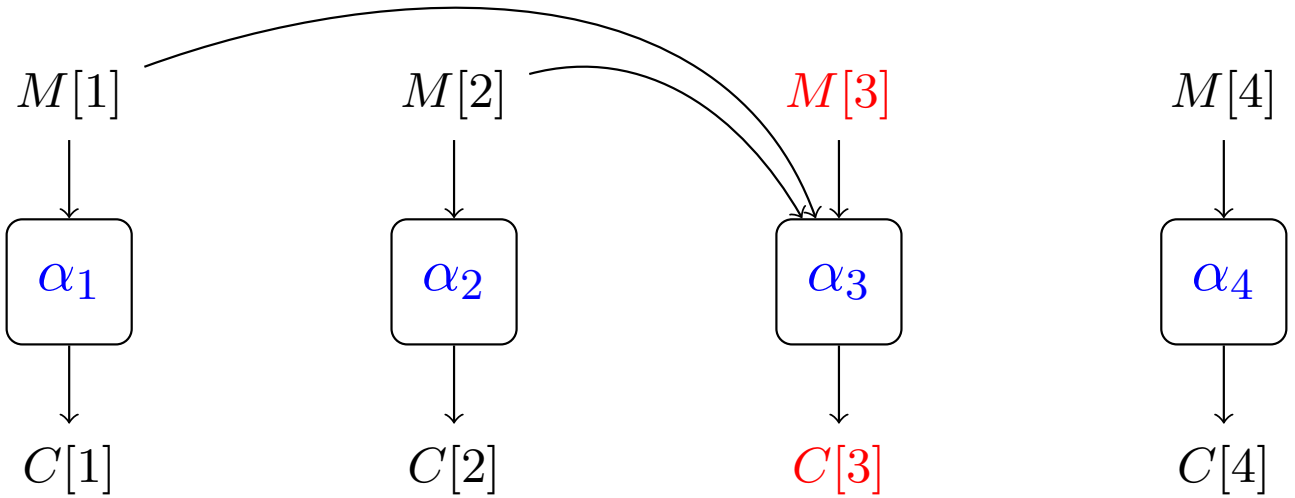




Motivation: Misuse Resistance From OCB?



Motivation: Misuse Resistance From OCB?



1. Dependency upon previous message blocks
2. Function using only key
3. No collisions between different messages

$\Rightarrow$ Universal hash

Motivation: Nonce Dependent Versus Misuse Resistant

Difference in efficiency:
at least efficiency of universal hash

Motivation: Universal Hash in AE

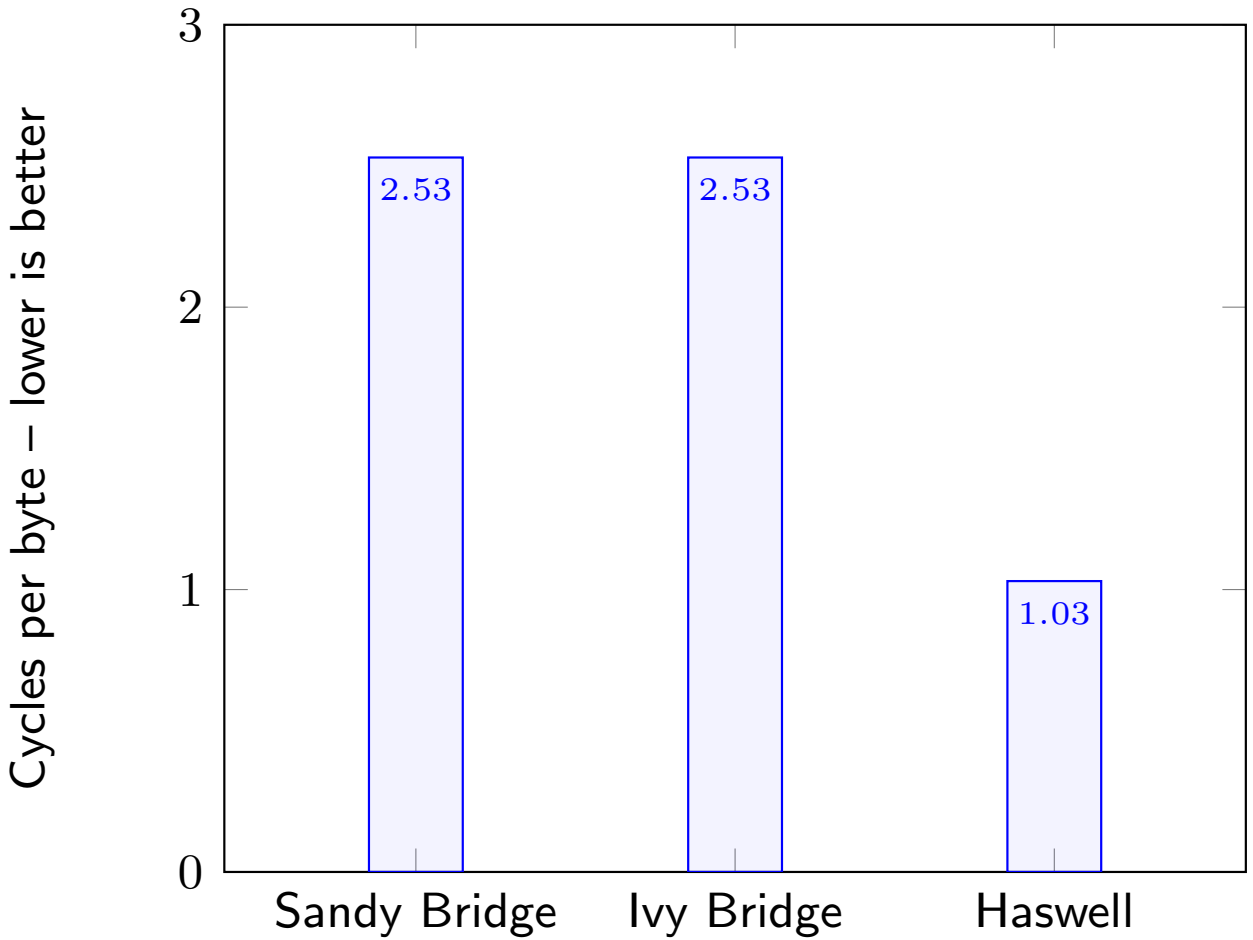


Figure : GCM with AES-NI. Results Gueron DIAC 2013.

Motivation: Universal Hash in AE

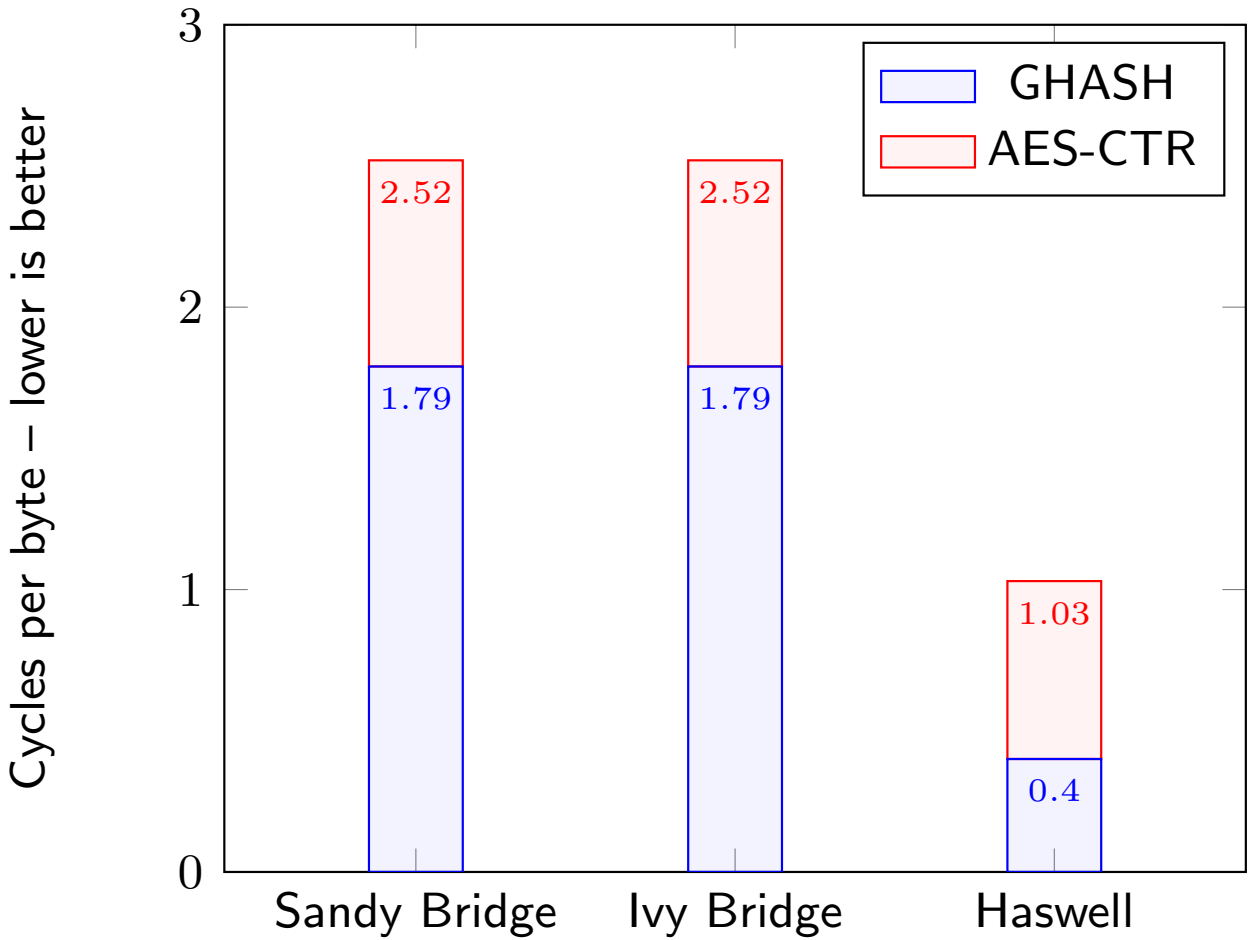


Figure : GCM with AES-NI. Results Gueron DIAC 2013.

Overview

COBRA:

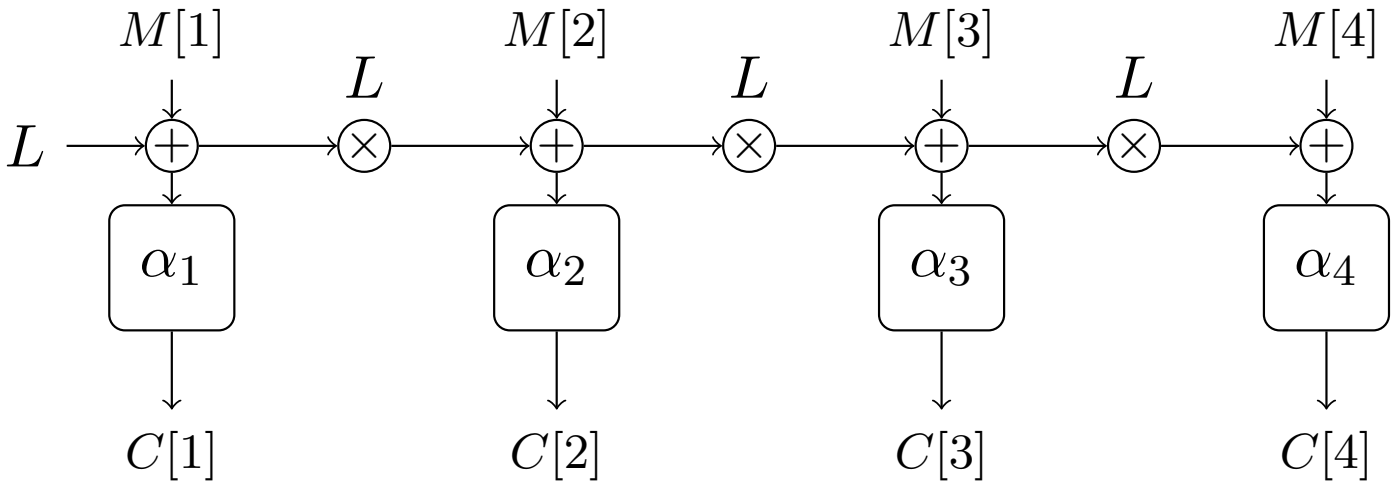
1. Misuse resistance
2. Online
3. GCM-like efficiency
4. No block cipher inverse
5. Security reduction to block cipher

Overview

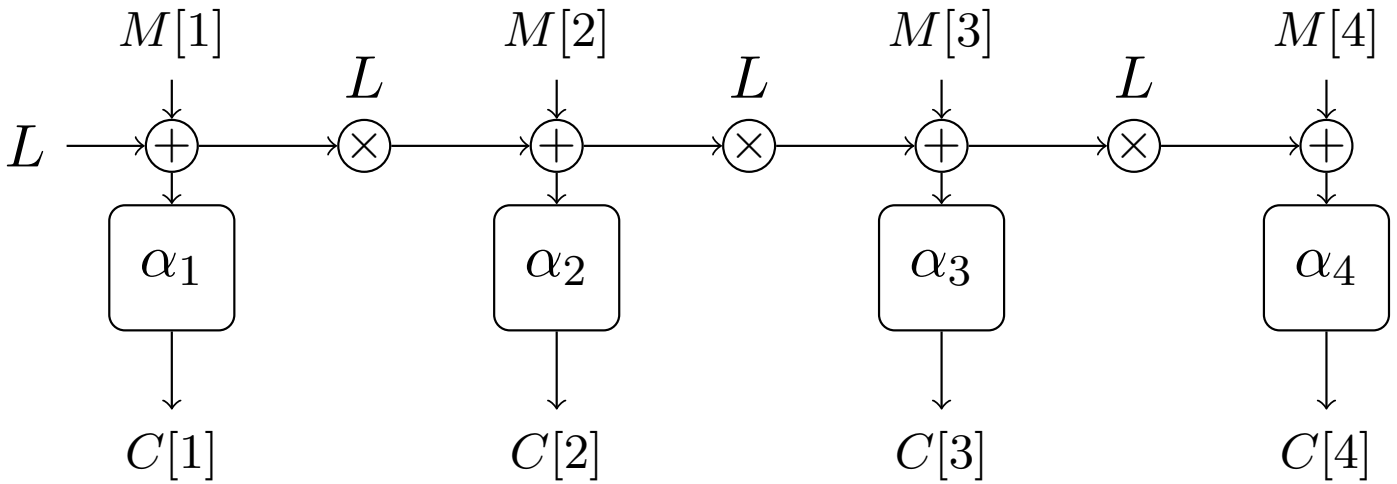
COBRA:

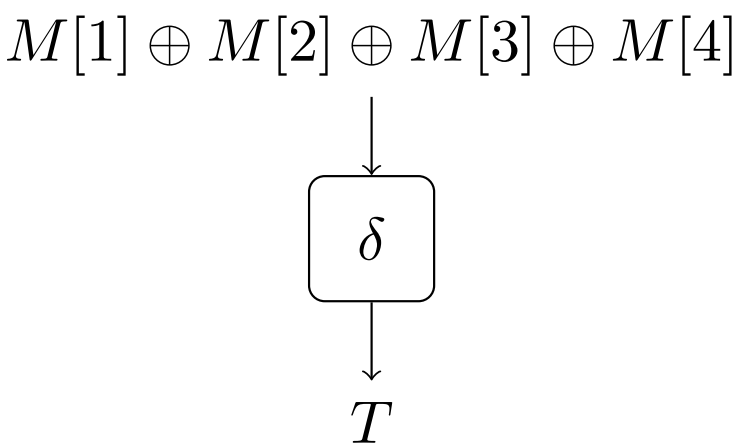
1. Misuse resistance
2. Online
3. GCM-like efficiency
    1. One multiplication per block
    2. One block cipher call per block
    3. Parallelizable
4. No block cipher inverse
5. Security reduction to block cipher

Motivation: How To Add Authenticity?

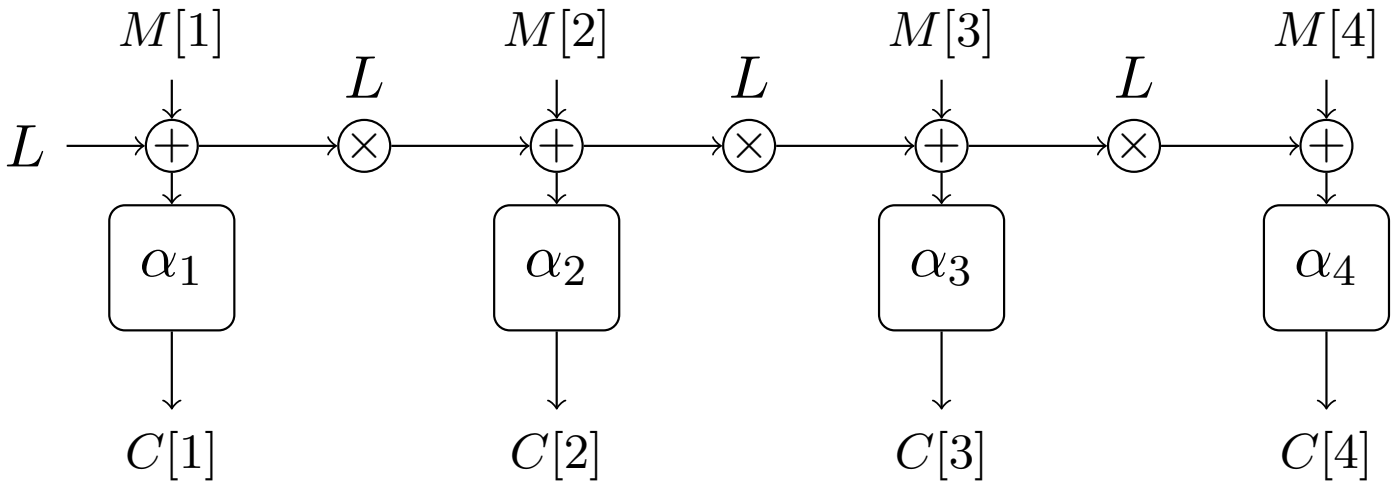


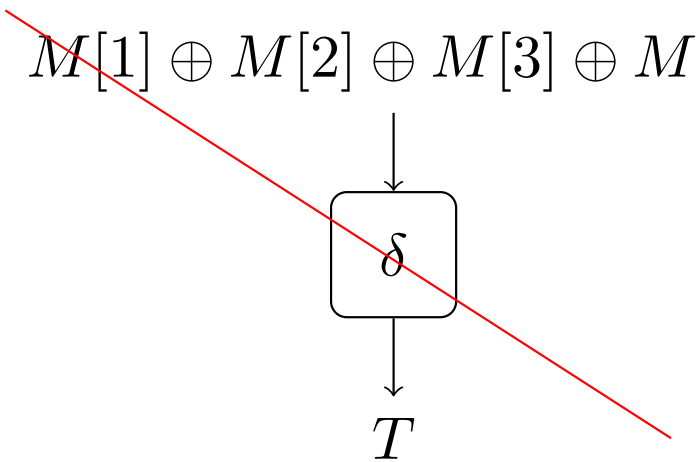
Motivation: How To Add Authenticity?



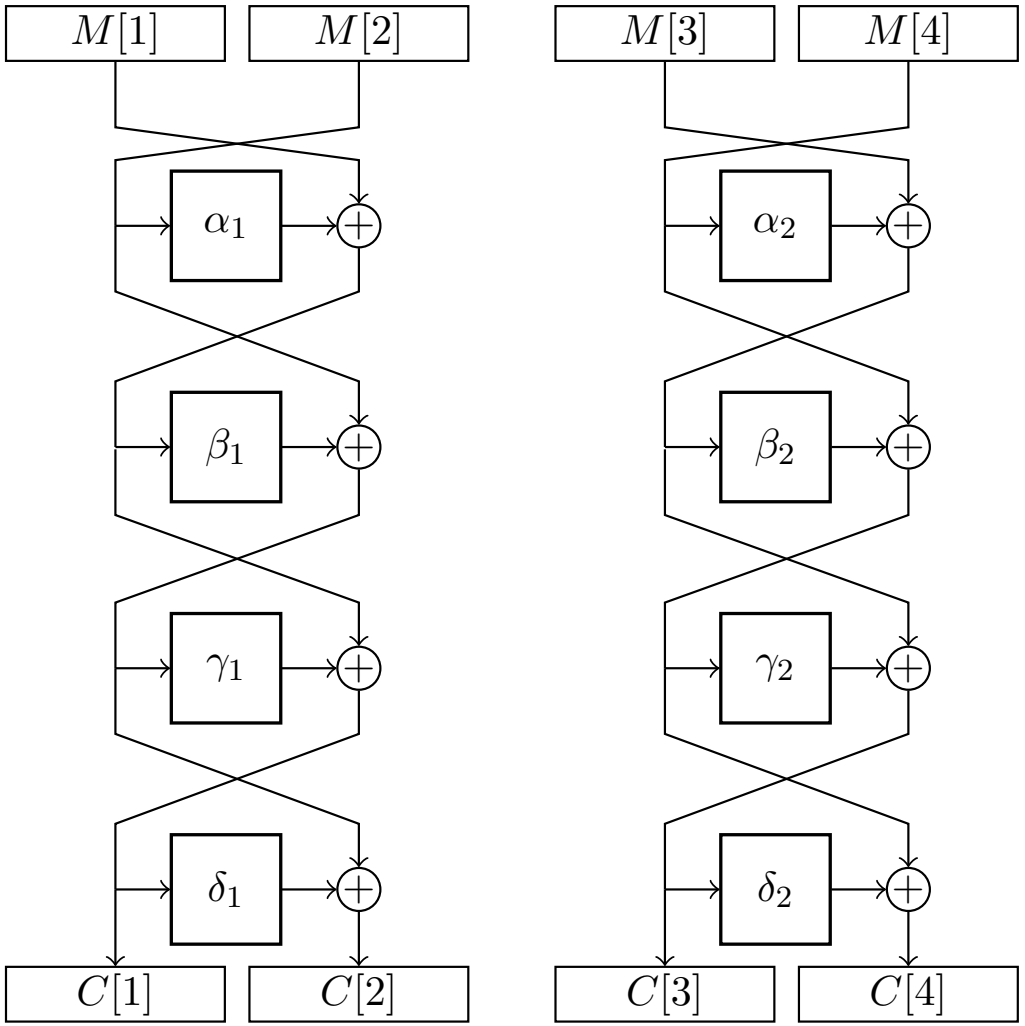


Motivation: How To Add Authenticity?



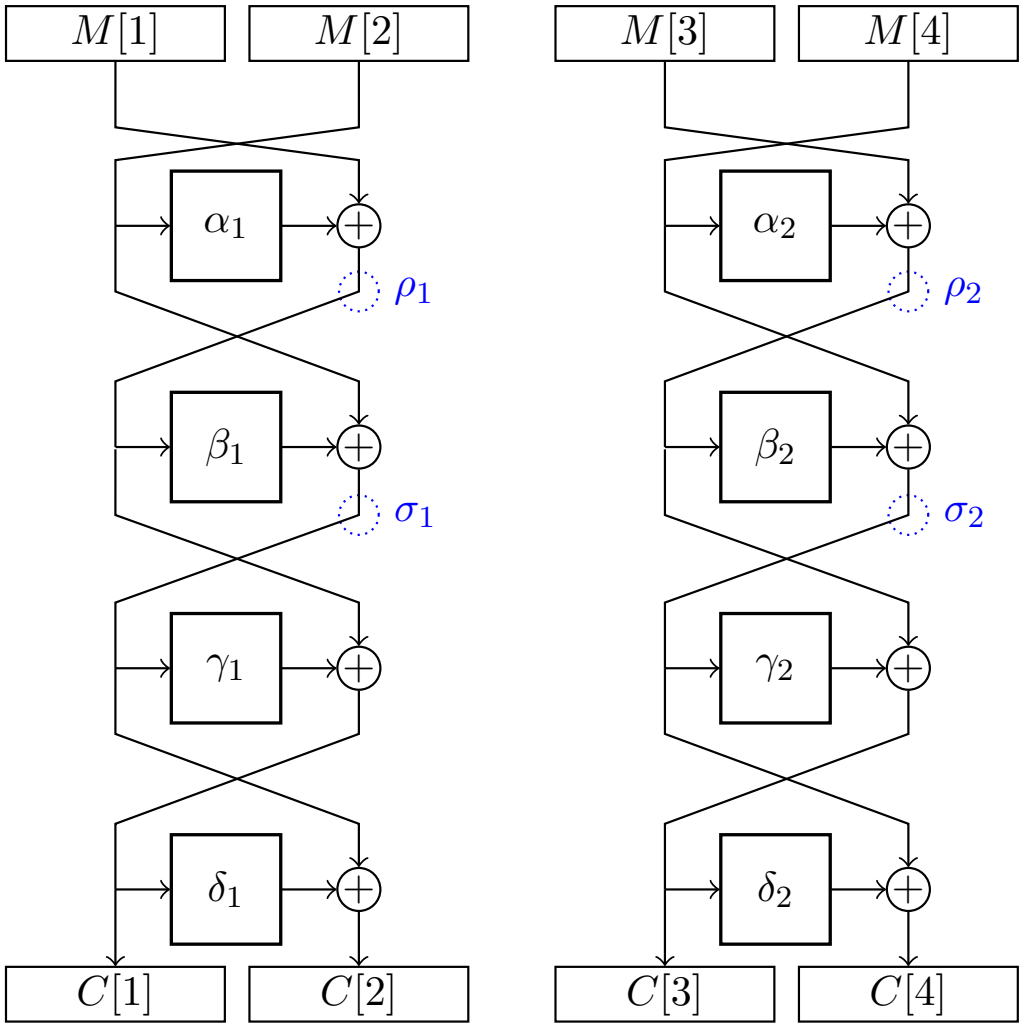


Motivation: ManTiCore, Beaver et al. ACISP '04



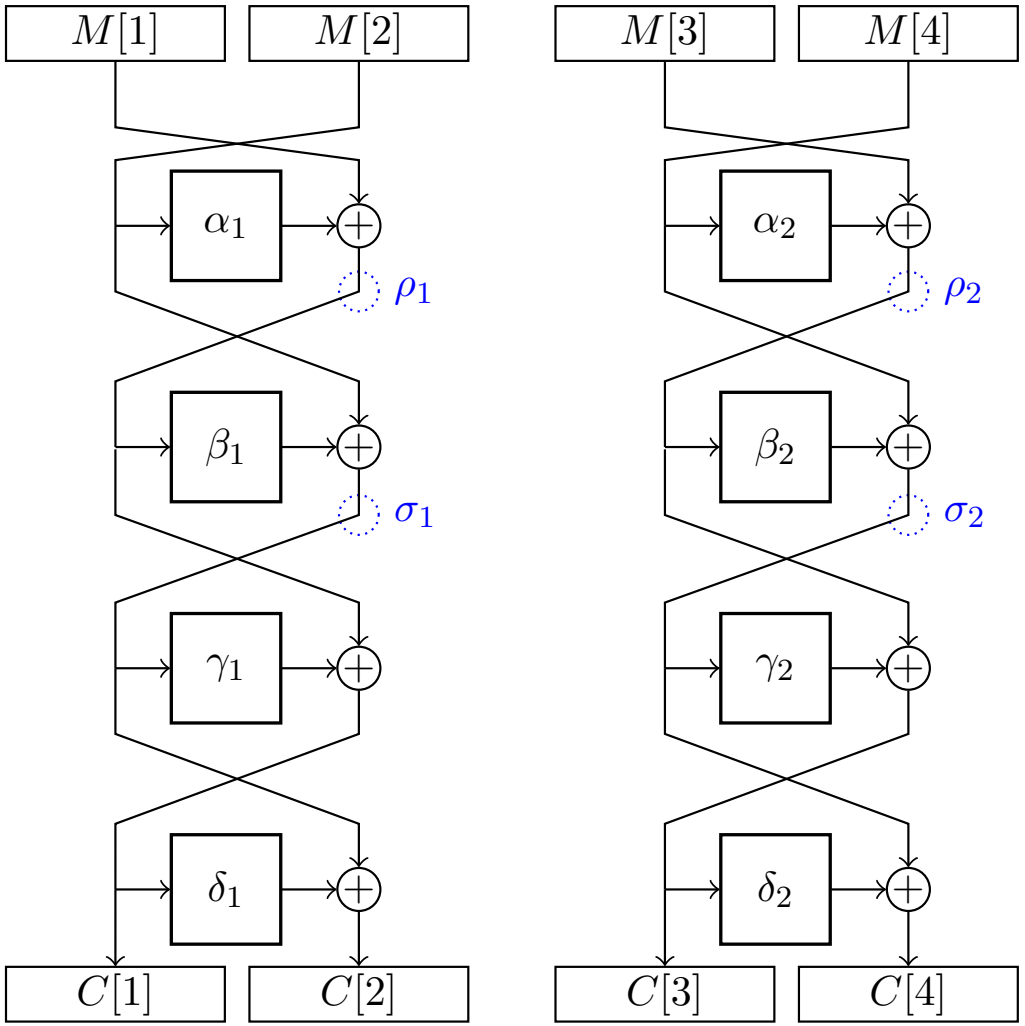
$\alpha_i, \beta_i, \gamma_i, \delta_i$: uniform random functions (URF)

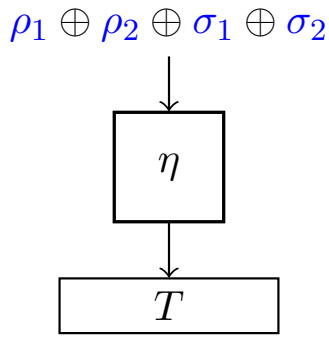
Motivation: ManTiCore, Beaver et al. ACISP '04



$\alpha_i, \beta_i, \gamma_i, \delta_i$: uniform random functions (URF)

Motivation: ManTiCore, Beaver et al. ACISP '04





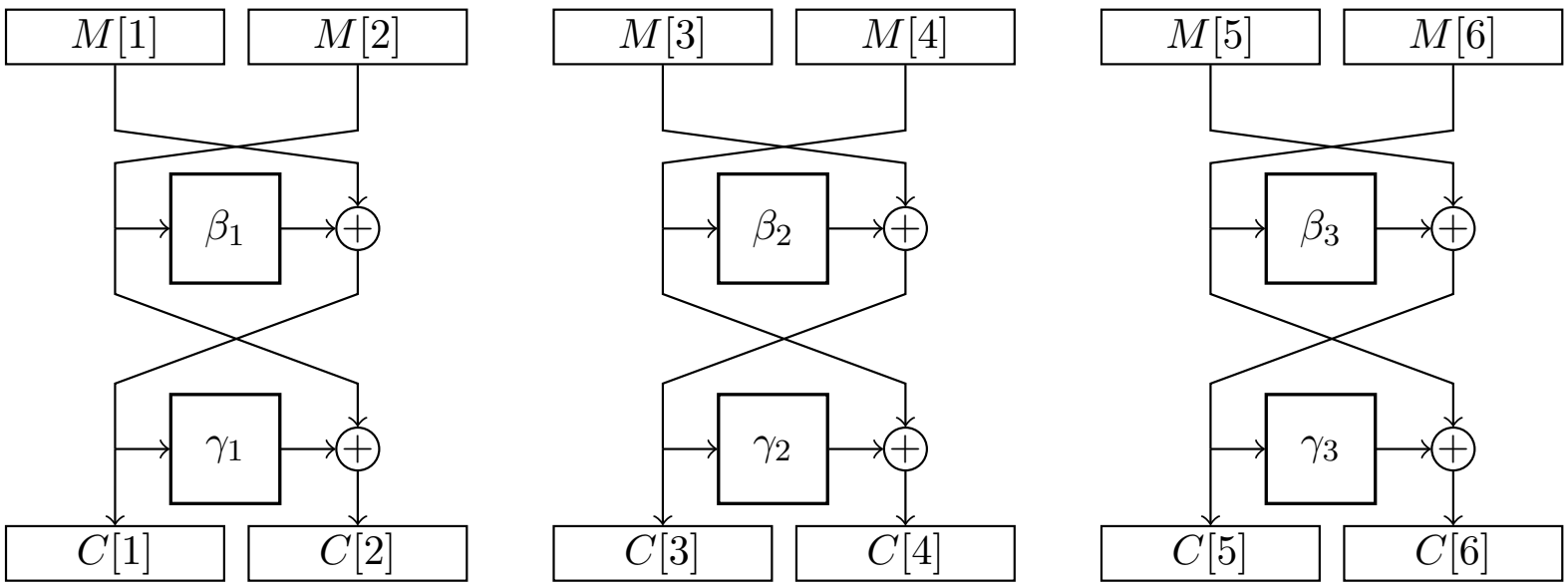
$\alpha_i, \beta_i, \gamma_i, \delta_i$: uniform random functions (URF)

Overview

COBRA:

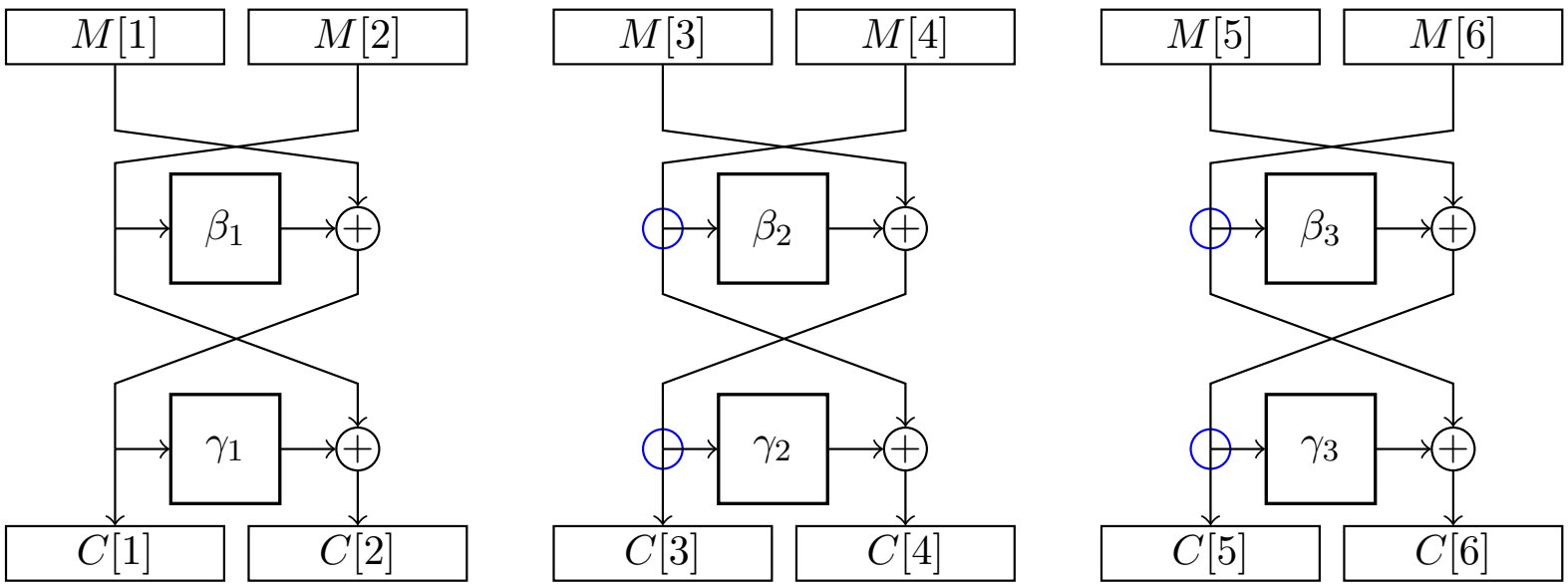
1. Misuse resistance
2. Online
3. GCM-like efficiency
    1. One multiplication per block
    2. One block cipher call per block
    3. Parallelizable
4. No block cipher inverse
5. Security reduction to block cipher

Building A Scheme: Starting Point



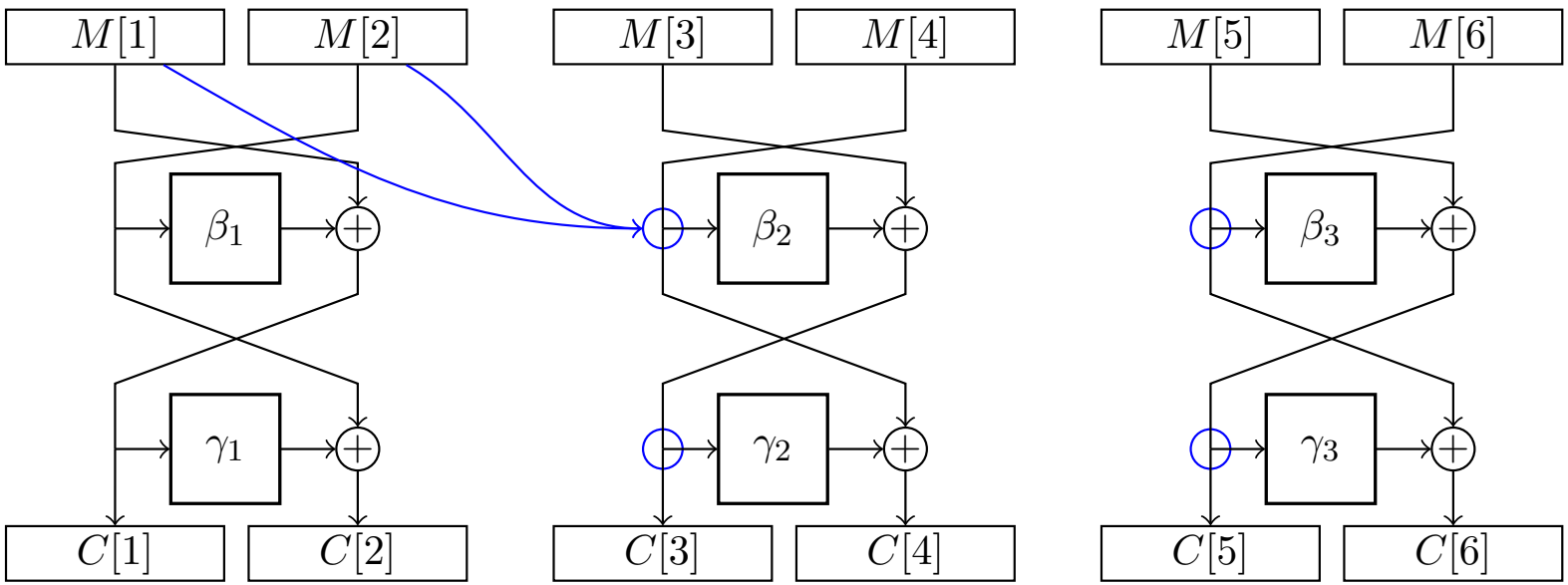
β_i, γ_i: uniform random functions (URF)

Building A Scheme: Starting Point



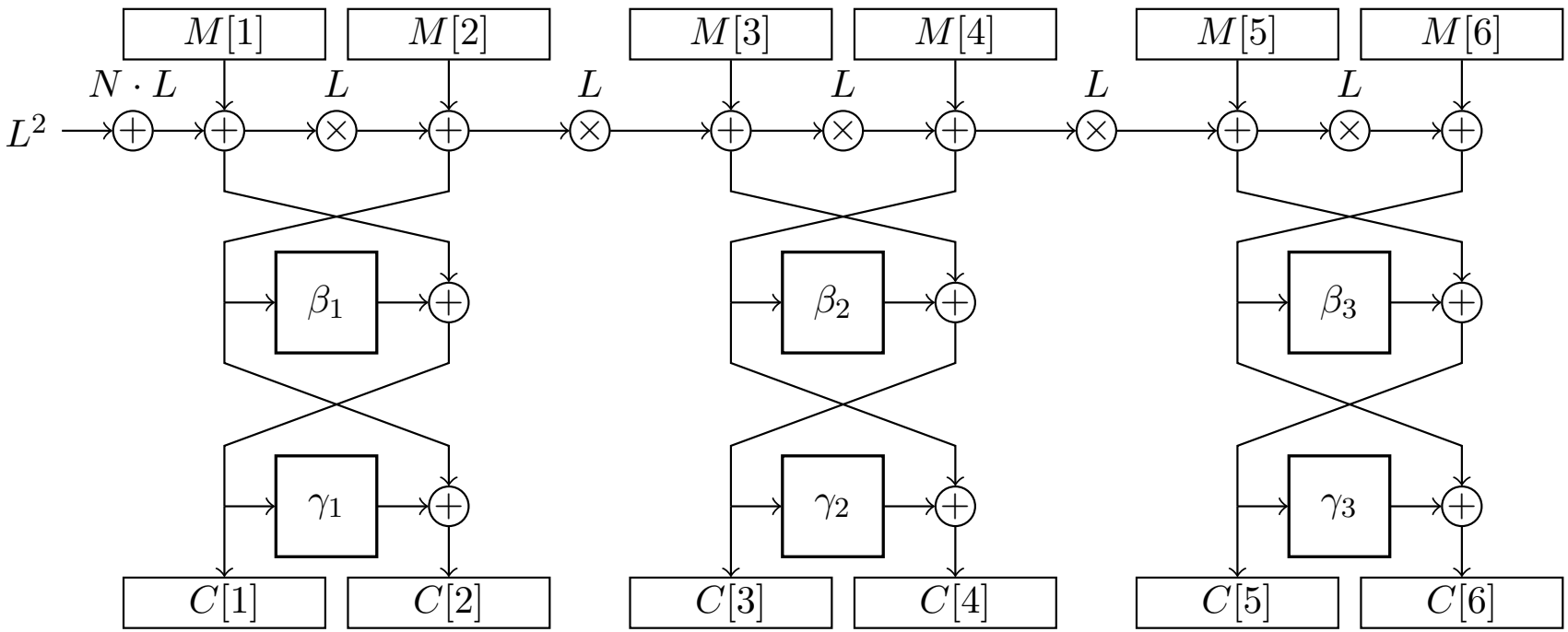
β_i, γ_i: uniform random functions (URF)

Building A Scheme: Starting Point



β_i, γ_i: uniform random functions (URF)

Building A Scheme: Adding Dependency

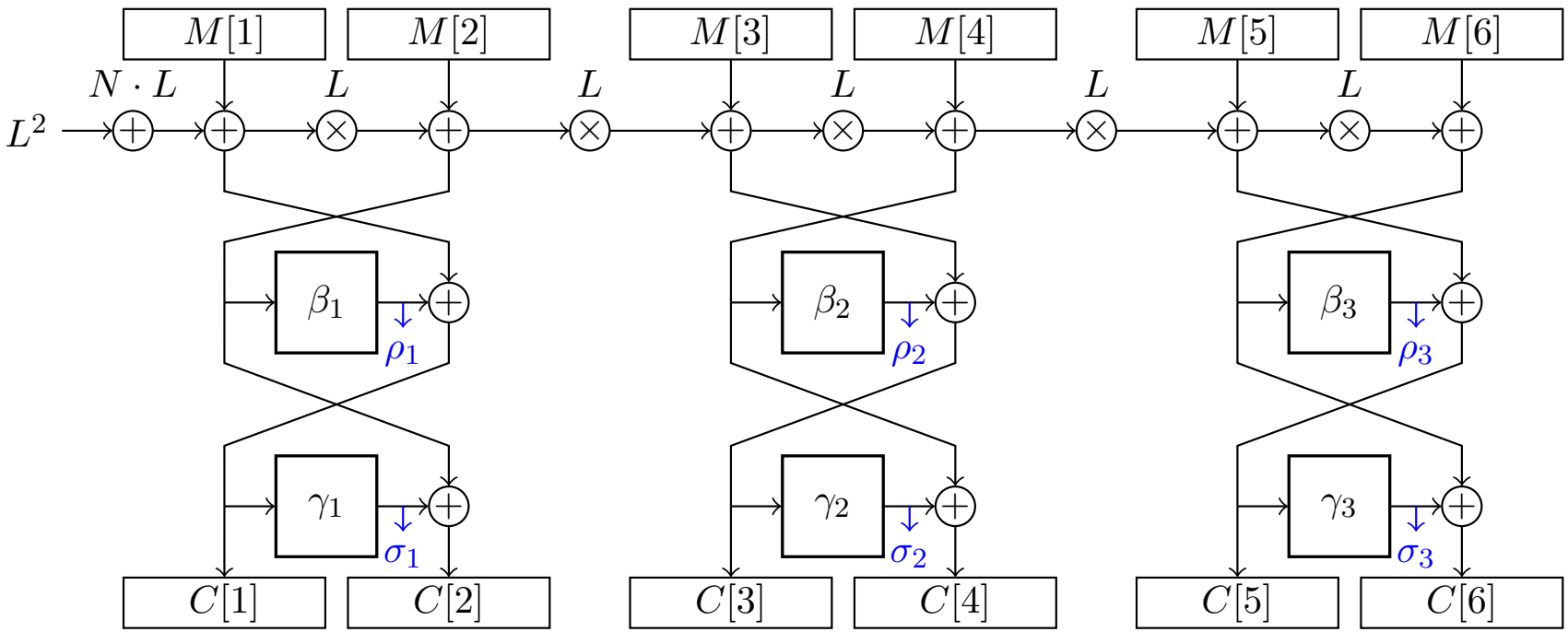


β_i, γ_i: URFs

L: secret value derived from the key

N: nonce

Building A Scheme: Adding Dependency

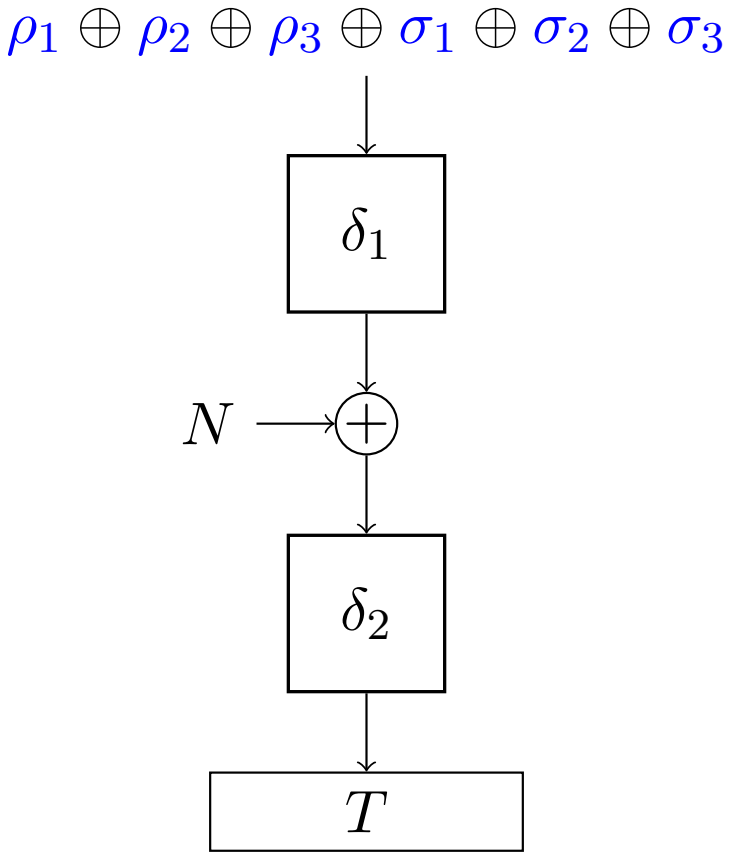


β_i, γ_i: URFs

L: secret value derived from the key

N: nonce

Building A Scheme: Adding Authenticity

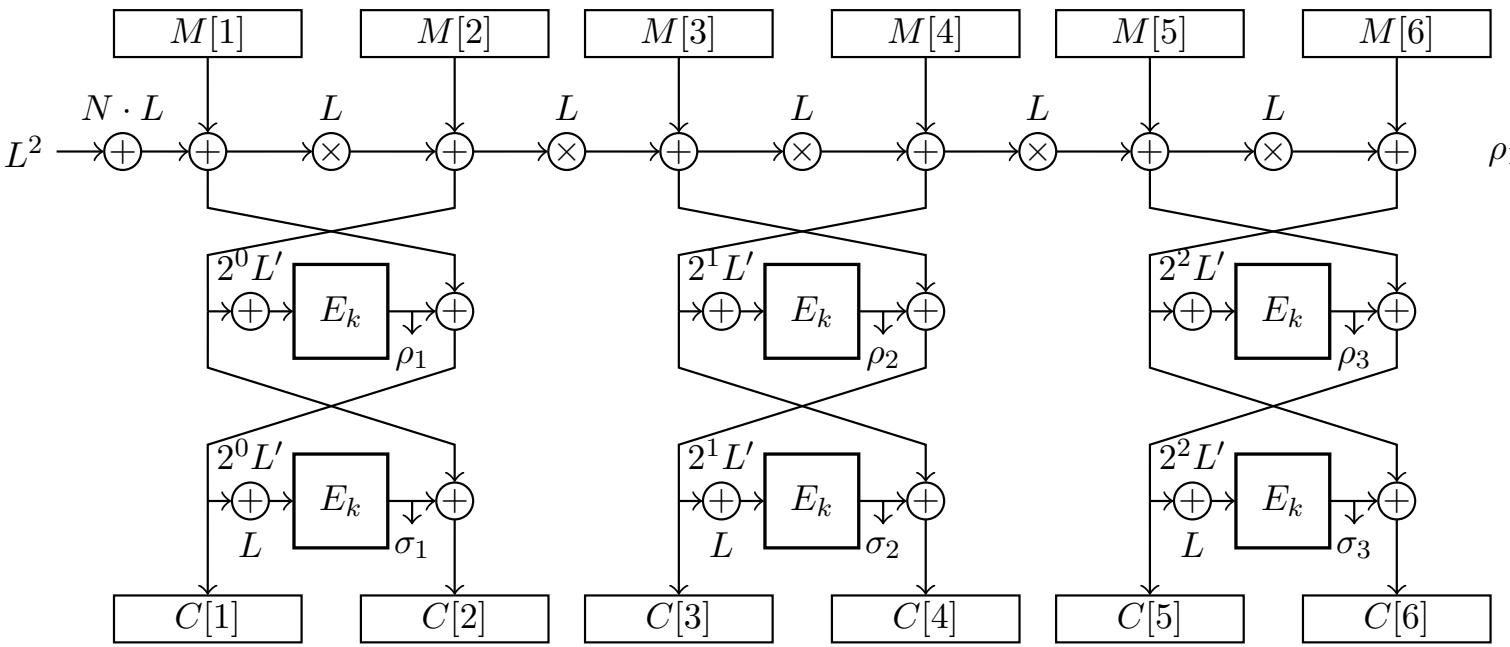


ρ_i, σ_i: outputs of URFs

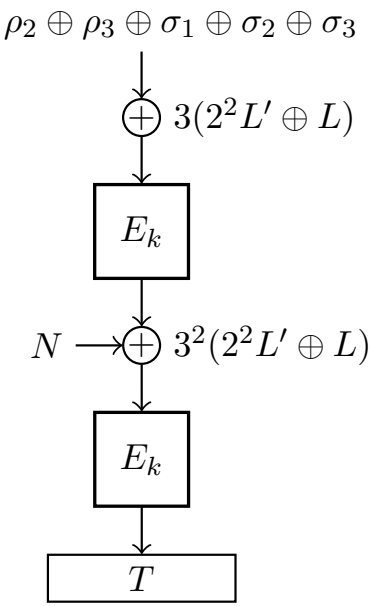
δ_i: URFs

N: nonce

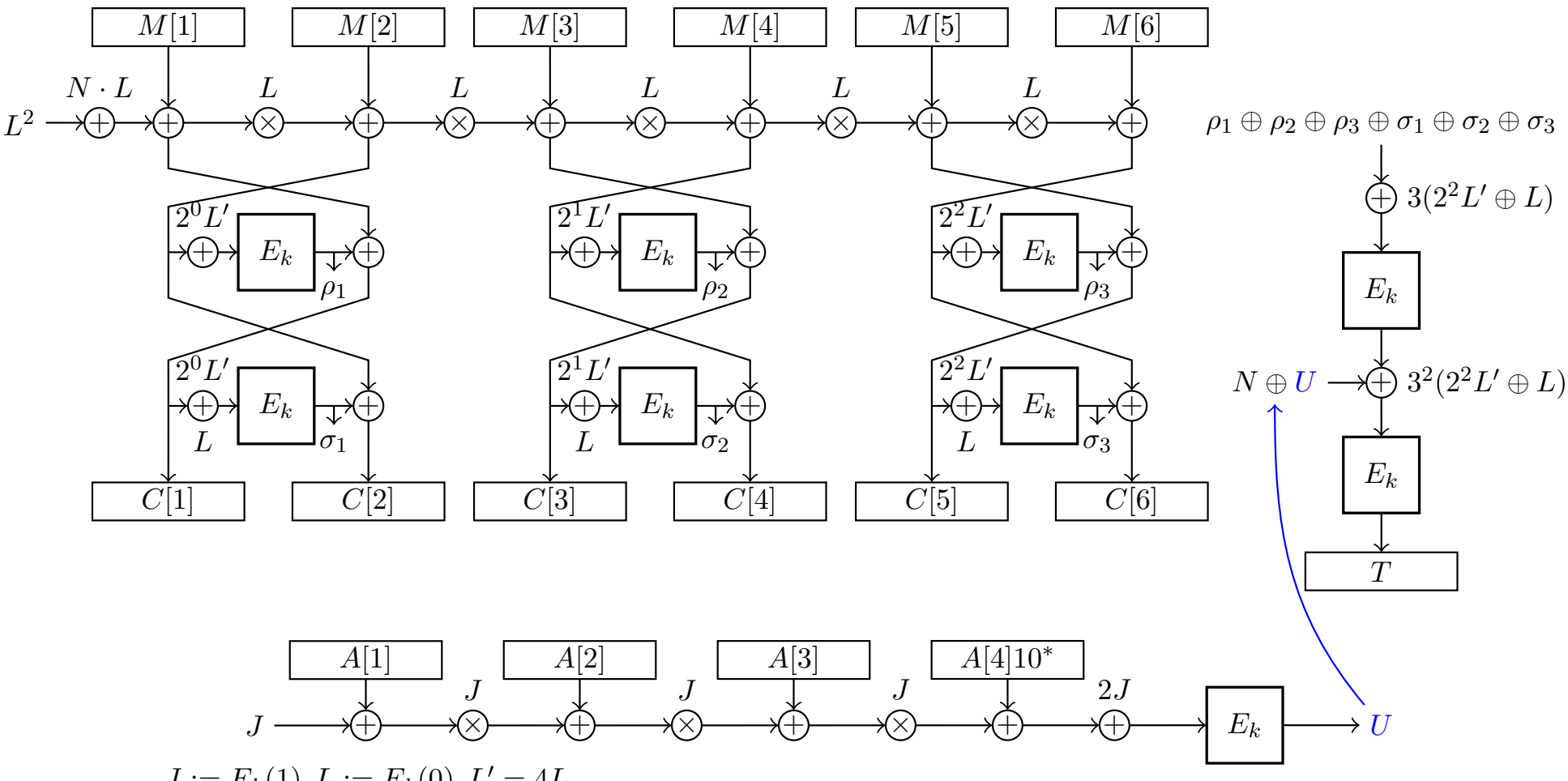
Our Scheme: COBRA



$L := E_k(0), L' = 4L$

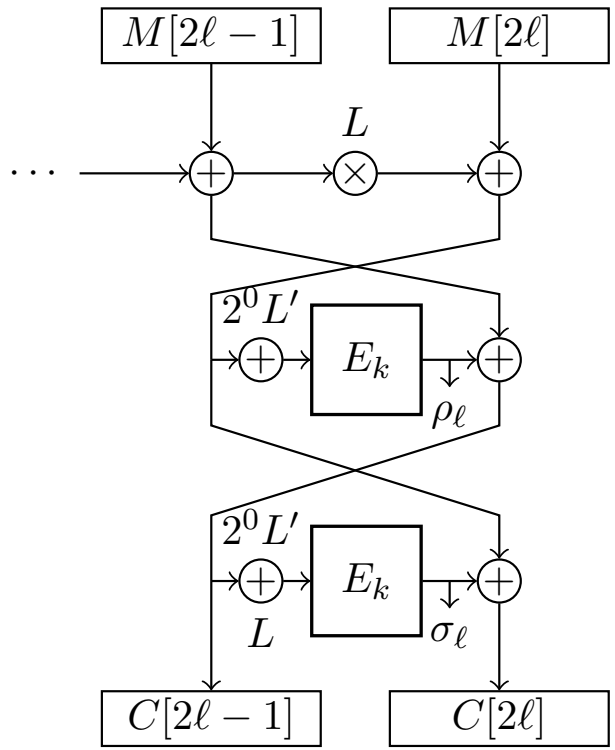


Our Scheme: COBRA



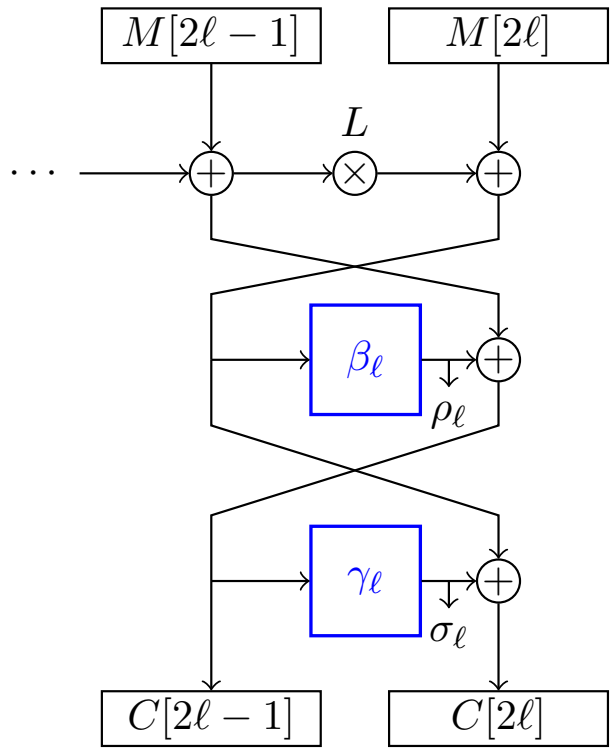
Proof Idea

1. Switch to URFs (at minimal cost)



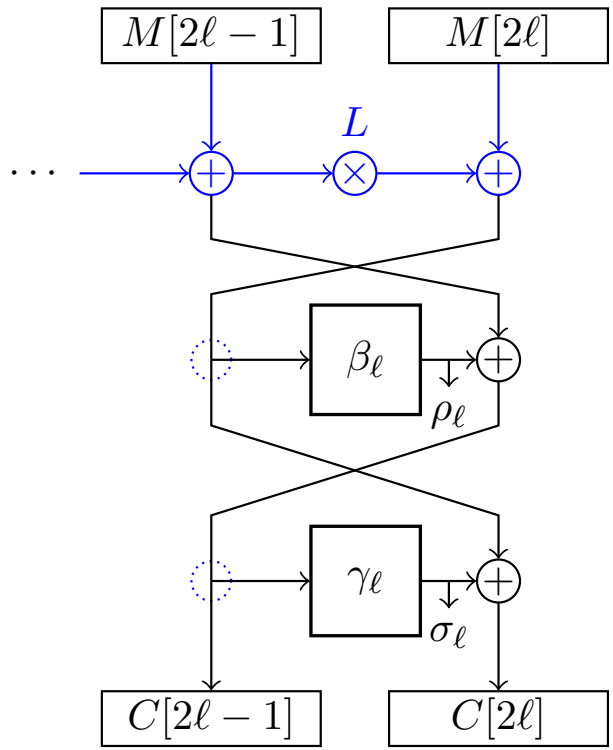
Proof Idea

1. Switch to URFs (at minimal cost)



Proof Idea

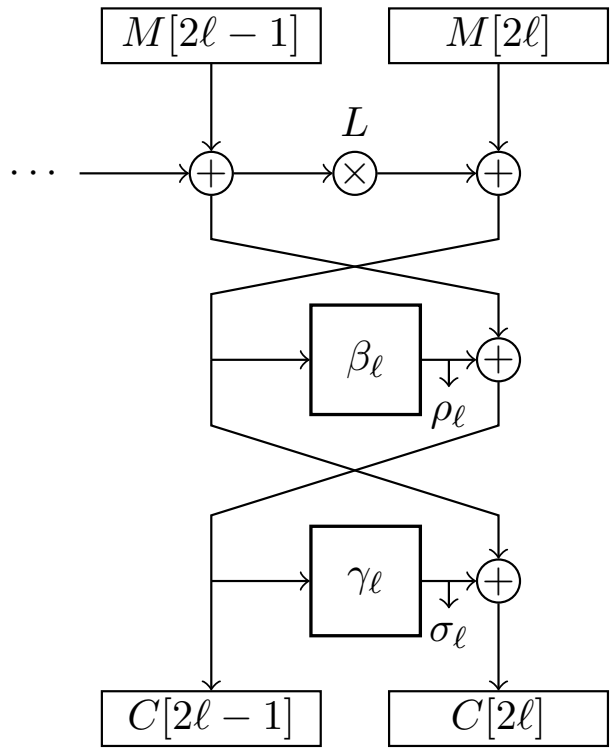
1. Switch to URFs (at minimal cost)
2. Collisions prevented by universal hash



Proof Idea

1. Switch to URFs (at minimal cost)
2. Collisions prevented by universal hash

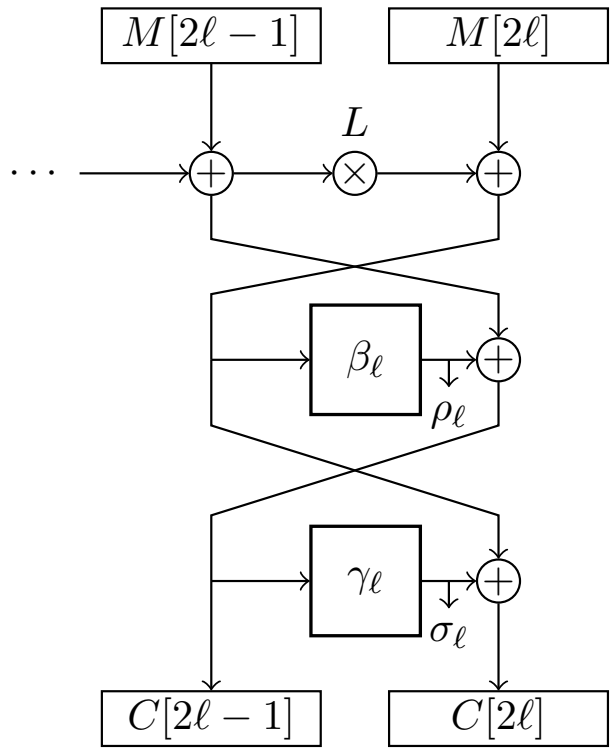
$\Rightarrow$ outputs are uniform and independent



Proof Idea

1. Switch to URFs (at minimal cost)
2. Collisions prevented by universal hash

$\Rightarrow$ outputs are uniform and independent
$\Rightarrow$ No relation between block cipher outputs makes forgery difficult



High Level Comparison With Other Misuse Resistant Schemes

Scheme	Year	No BC Inverse	Parallelizable	Online
2 BC				
SIV	2006	✓	✗	✗
COPA	2013	✗	✓	✓
BC + UH				
HBS	2009	✗	✓	✗
BTM	2009	✓	✓	✗
McOE-G	2011	✗	✗	✓
COBRA	**2014**	✓	✓	✓

Table : Comparing misuse resistant AE modes of operation. BC := block cipher, UH := universal hash

Summary and Future Work

COBRA:

1. Misuse resistance
2. Online
3. GCM-like efficiency
    1. One multiplication per block
    2. One block cipher call per block
    3. Parallelizable
4. No block cipher inverse
5. Security reduction to block cipher

Summary and Future Work

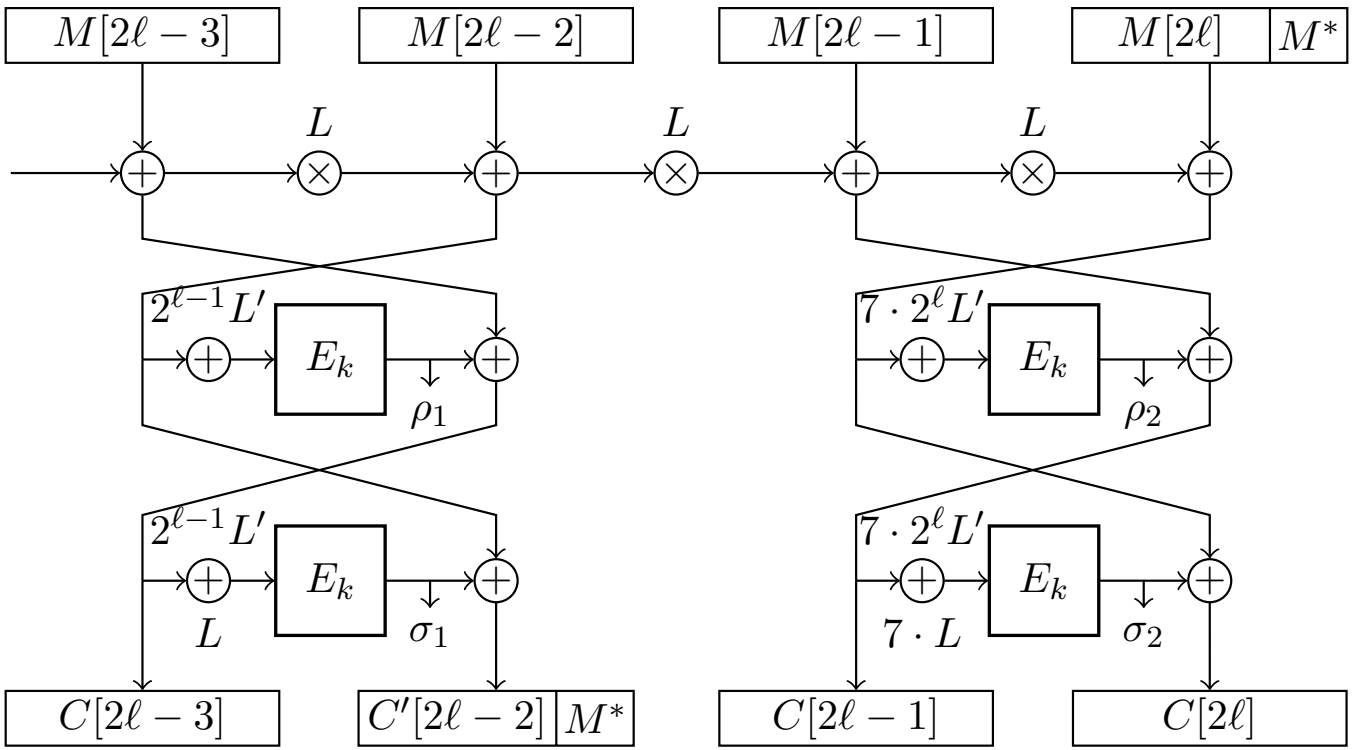
COBRA:

1. Misuse resistance
2. Online
3. GCM-like efficiency
    1. One multiplication per block
    2. One block cipher call per block
    3. Parallelizable
4. No block cipher inverse
5. Security reduction to block cipher

Submission to CAESAR

Software implementation results

Fractional Data: $\ell > 1$, $0 < |M[2\ell]| < n$



Fractional Data: $\ell > 2$ and $0 < |M[2\ell - 1]| \leq n$