

COPA v2

Elena Andreeva COSIC, KU Leuven, Belgium

Andrey Bogdanov DTU, Denmark

Atul Luykx COSIC, KU Leuven, Belgium

Bart Mennink COSIC, KU Leuven, Belgium

Elmar Tischhauser DTU, Denmark

Kan Yasuda NTT, Japan

DIAC'15, Singapore

September 28, 2015



How it All Started?

2013: COPA published

[Parallelizable and Authenticated Online Ciphers](#)

Asiacrypt'13, E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, E. Tischhauser, K. Yasuda

2014: COPA analyzed in RUP model



[How to Securely Release Unverified Plaintext in Authenticated Encryption](#)

Asiacrypt'14, E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, K. Yasuda

2014: COPA v1 submitted to CAESAR

CAESAR Round 1

1.ACORN	11.AVALANCHE	21.FASER	31.MORUS	41.POET	51.Silver
2.++AE	12.Artemia	22.HKC	32.Marble	42.POLAWIS	52.Tiaoxin
3.AEGIS	13.Ascon	23.HS1-SIV	33.McMAmbo	43.PRIMATEs	53.TriviA-ck
4.AES-CMCC	14.CBA	24.ICEPOLE	34.Minalpher	44.Prost	54.Wheesht
5.AES-COBRA	15.CBEAM	25.Joltik	35.NORX	45.Raviyoyla	55.YAES
6.AES-COPA	16.CLOC	26.Julius	36.OCB	46.SCREAM	56.iFeed[AES]
7.AES-CPFB	17.Calico	27.KIASU	37.OMD	47.SHELL	57. π -Cipher
8.AES-JAMBU	18.Deoxys	28.Ketje	38.PAEQ	48.SILC	
9.AES-OTR	19.ELmD	29.Keyak	39.PAES	49.STRIBOB	
10.AEZ	20.Enchilada	30.LAC	40.PANDA	50.Sablier	

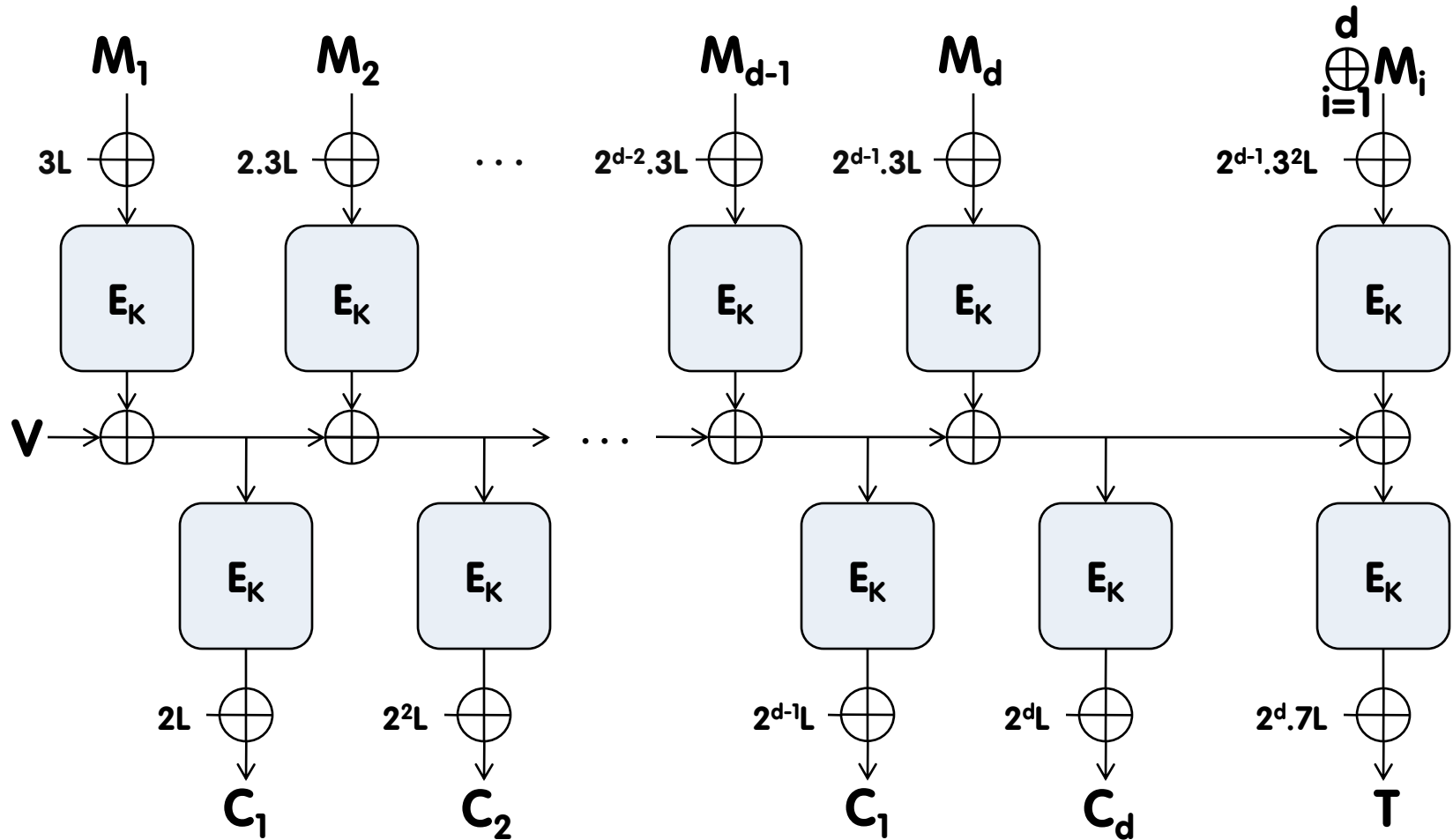
-  based on COPA /in some of the modes/
-  resemblances with COPA

Why COPA

- Nonce reuse security protection
- Simple implementation
- Parallelizable
- Online
- Security reduced to BC
- E (forward) only BC in AE
- E^{-1} (backward) only BC in DV
- Variable tag size

COPA v2

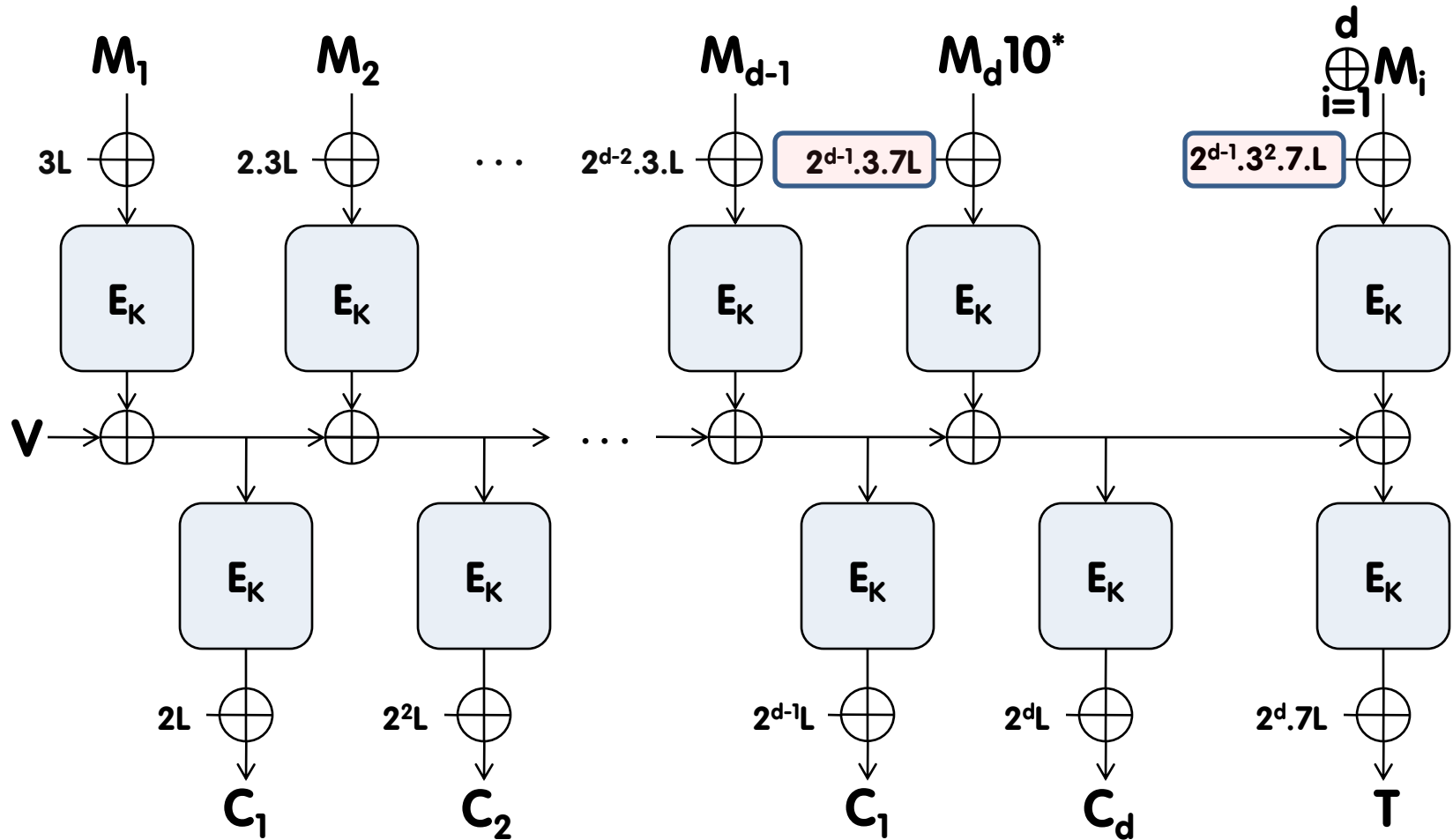
Messages of block size
(COPA v1)



$$L = E_K(0)$$

COPA v2

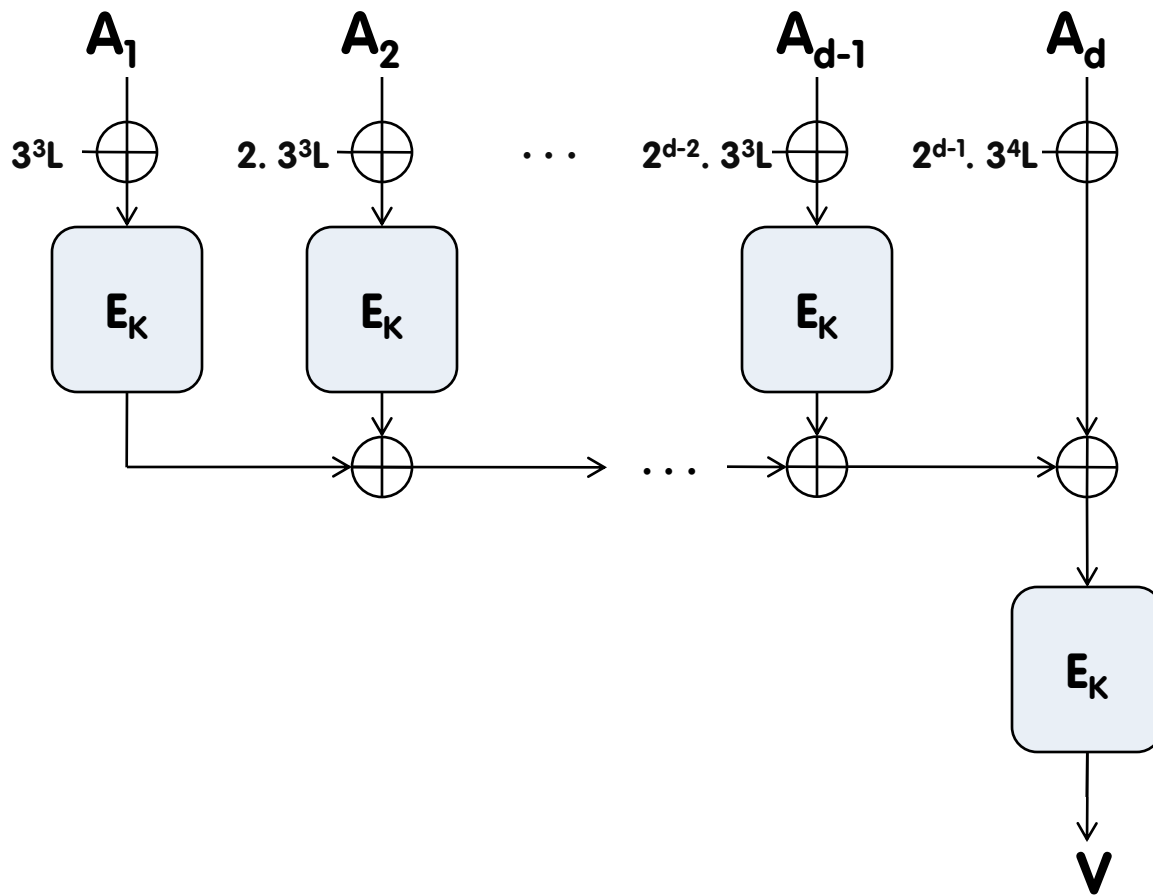
Messages not aligned with block size
(add padding and new final masks \neq COPAv1)



$$L = E_K(0)$$

COPA v2

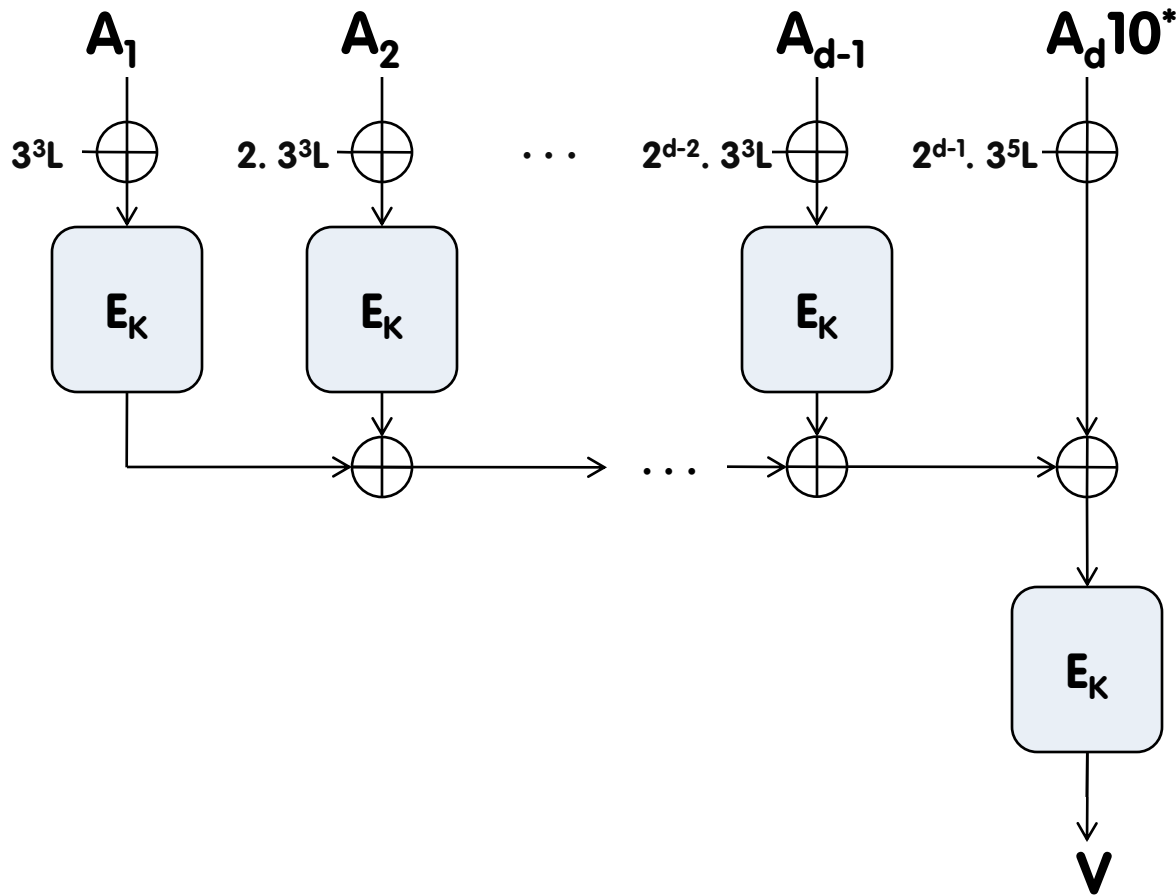
AD of block size
(COPA v1)



$$L = E_K(0)$$

COPA v2

AD not aligned with block size
(COPA v1)



$$L = E_K(0)$$

Related Research

2014 and 2015

■ Security:

[XLS is not a Strong Pseudorandom Permutation](#)

Asiacrypt'14, M. Nandi

[Revisiting Security Claims of XLS and COPA](#)

ePrint Archive 444/2015, M. Nandi

[On the Security of the COPA and Marble Authenticated Encryption Algorithms against \(Almost\) Universal Forgery Attack](#)

ePrint Archive 079/2015, Jiqiang Lu

■ Performance:

[AES-Based Authenticated Encryption Modes in Parallel High-Performance Software](#)

ePrint Archive 186/2014, A. Bogdanov, M. Lauridsen, E. Tischhauser

[Comb to Pipeline: Fast Software Encryption Revisited](#)

FSE'15 A. Bogdanov, M. Lauridsen, E. Tischhauser

[Energy evaluation of AES-Based Authenticated Encryption Algorithms](#)

DIAC'15, S. Banik, A. Bogdanov, F. Regazzoni

Some Performance Figures

Mode	128	256	512	1024	2048
McOE-G	7.77	7.36	7.17	7.07	7.02
COPA	3.37	2.64	2.27	2.08	1.88
POET	6.89	5.74	5.17	4.88	4.74
Julius	4.18	4.69	3.24	3.08	3.03

Comparison of AES-full modes with nonce reuse protection on various message lengths (in bytes) on Intel's Haswell i5 microarchitecture

Mode	128	256	512	1024	2048	4096	8192
COPA	2.77	2.16	1.86	1.70	1.63	1.59	1.58

COPA performance on Intel's Haswell i7 microarchitecture

Future Work

- **Improve performance**
 - nonce optimization
 - minimize initialization/finalization steps
 - reduced round BC versions
 - optimized implementation
- **Improve functionality**
 - incremental tags
- **Increase security guarantees**
 - beyond Birthday Bound variants

Thank you!

copa@esat.kuleuven.be