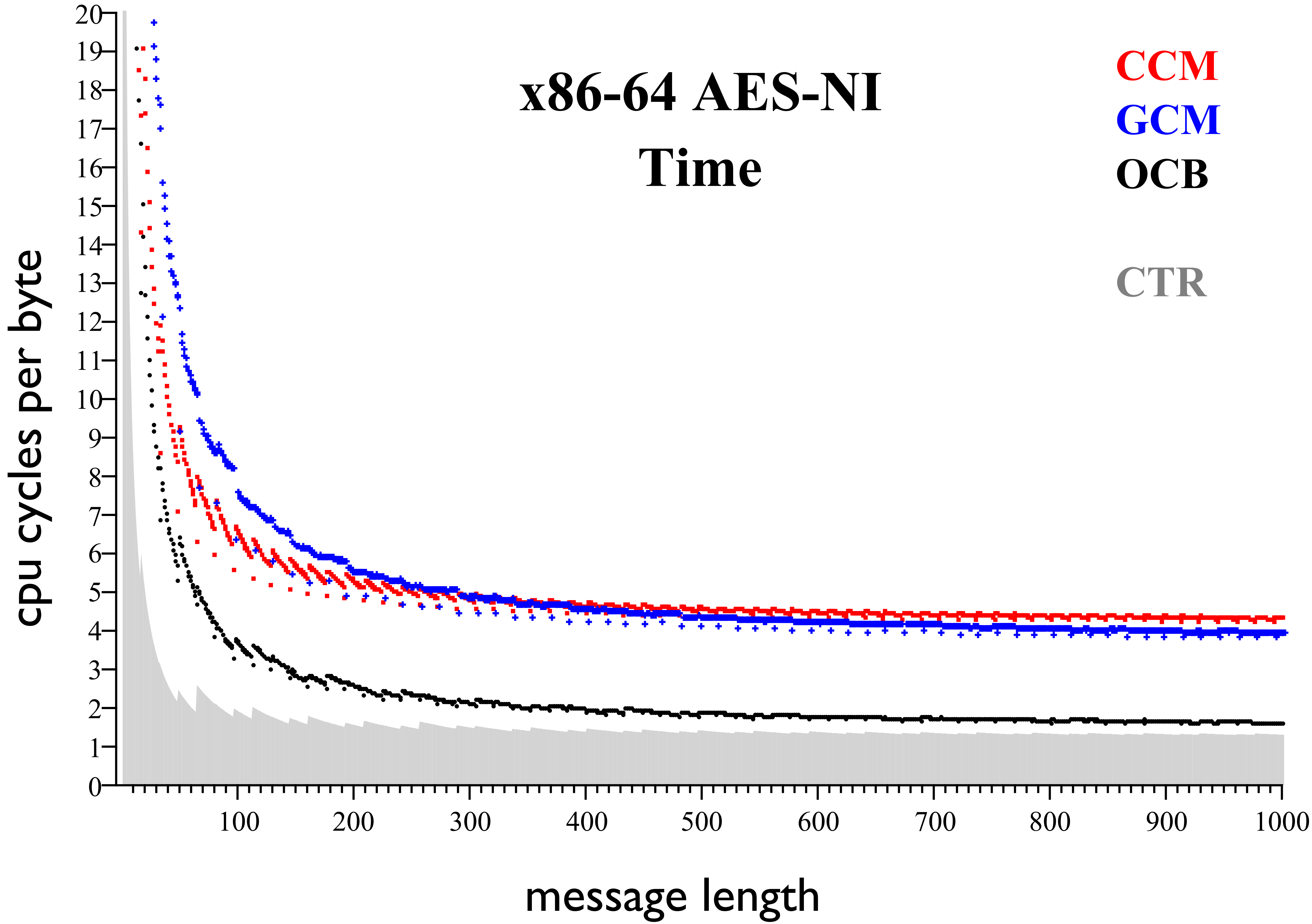
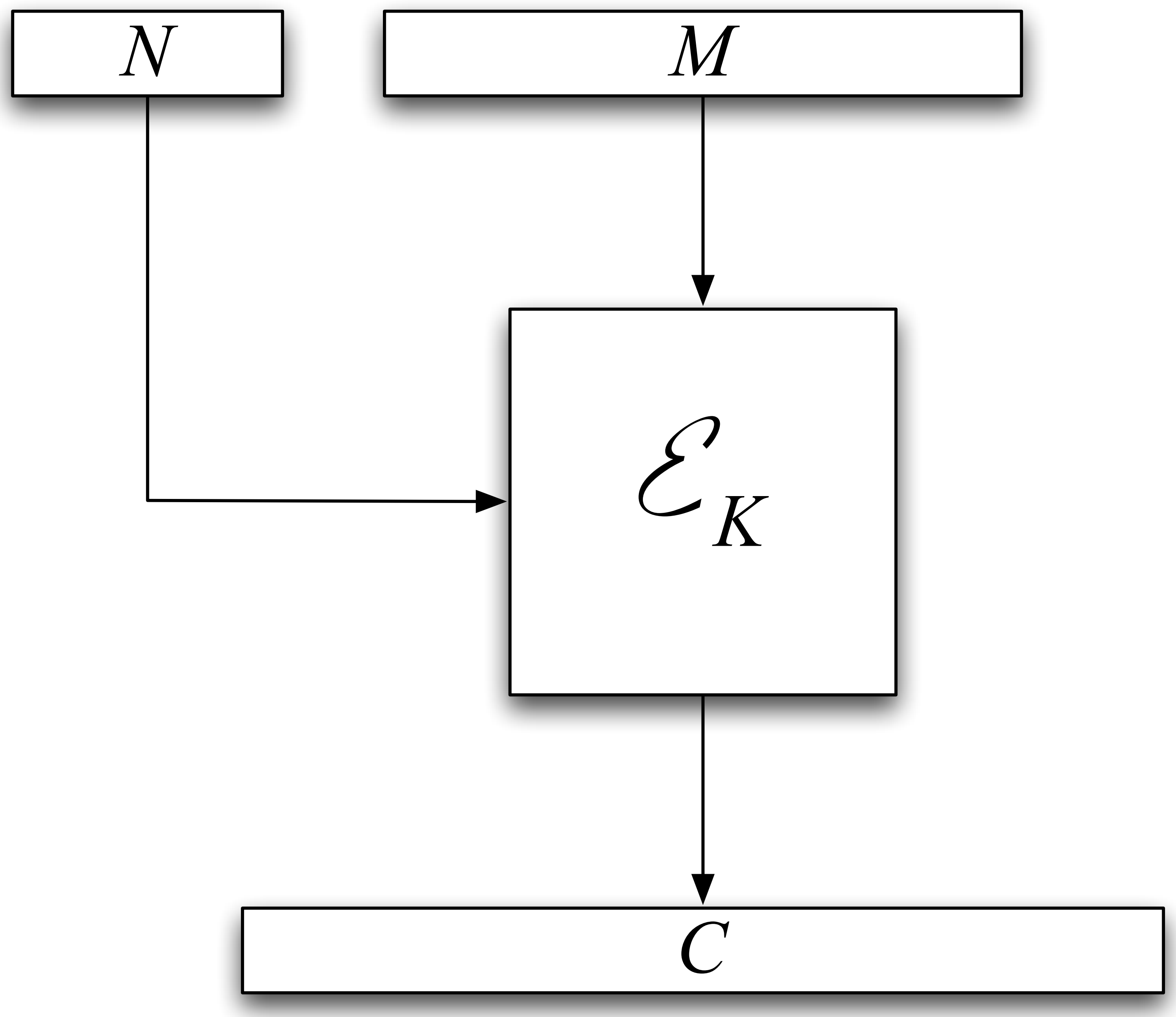
The Software Performance of Authenticated-Encryption Modes

Ted Krovetz
Cal State Sacramento

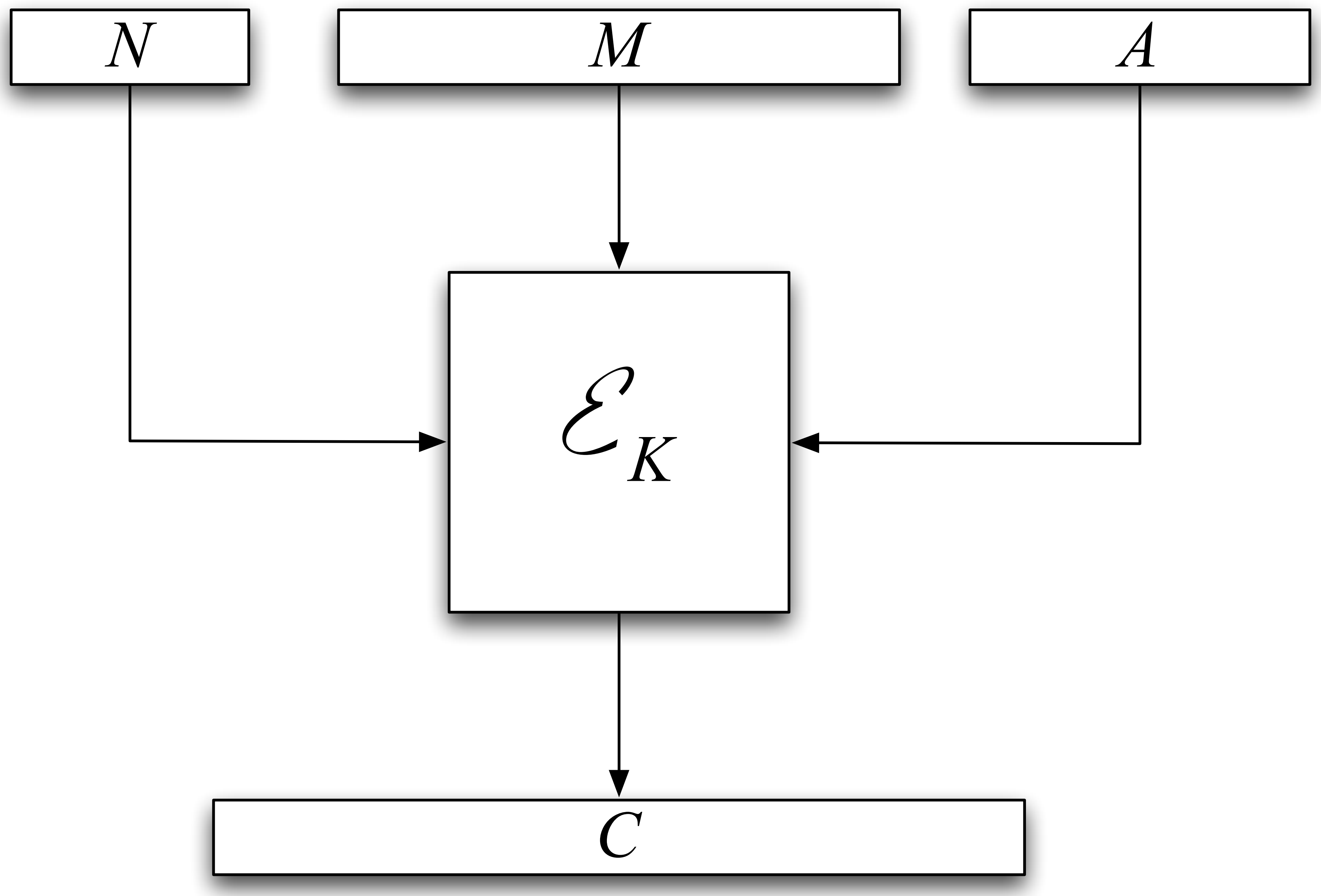
Phillip Rogaway
UC Davis


x86-64 AES-NI
Time
CCM
GCM
OCB
CTR
cpu cycles per byte
message length
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
100
200
300
400
500
600
700
800
900
1000

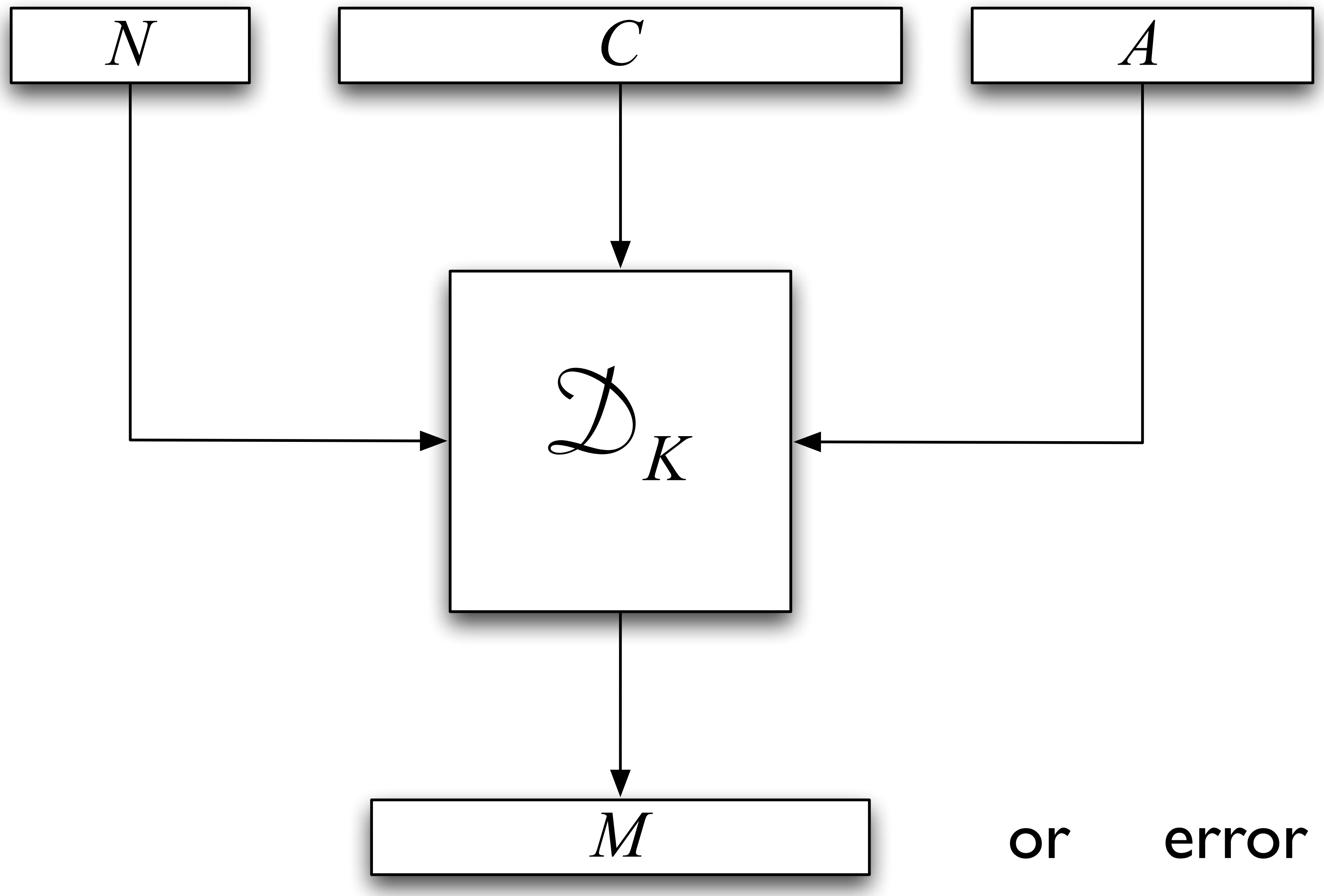
AE Syntax



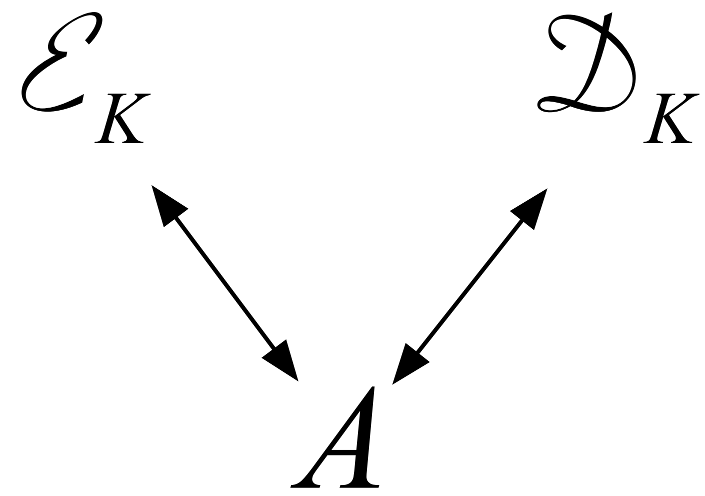
AEAD Syntax



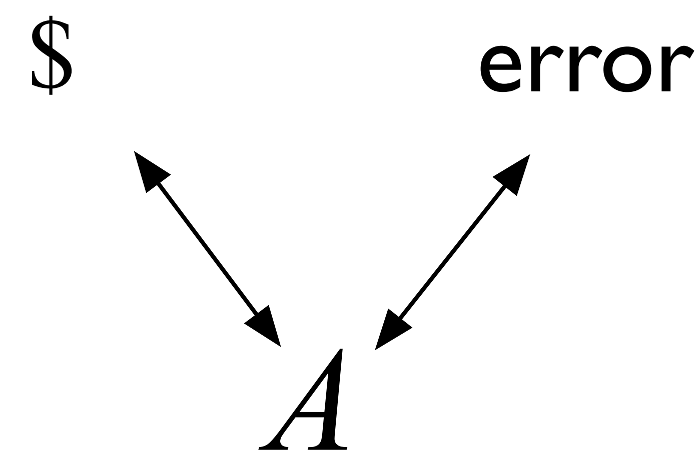
AEAD Decryption



Security Model



or



Pr[A = 1 | left scenario] - Pr[A = 1 | right scenario]

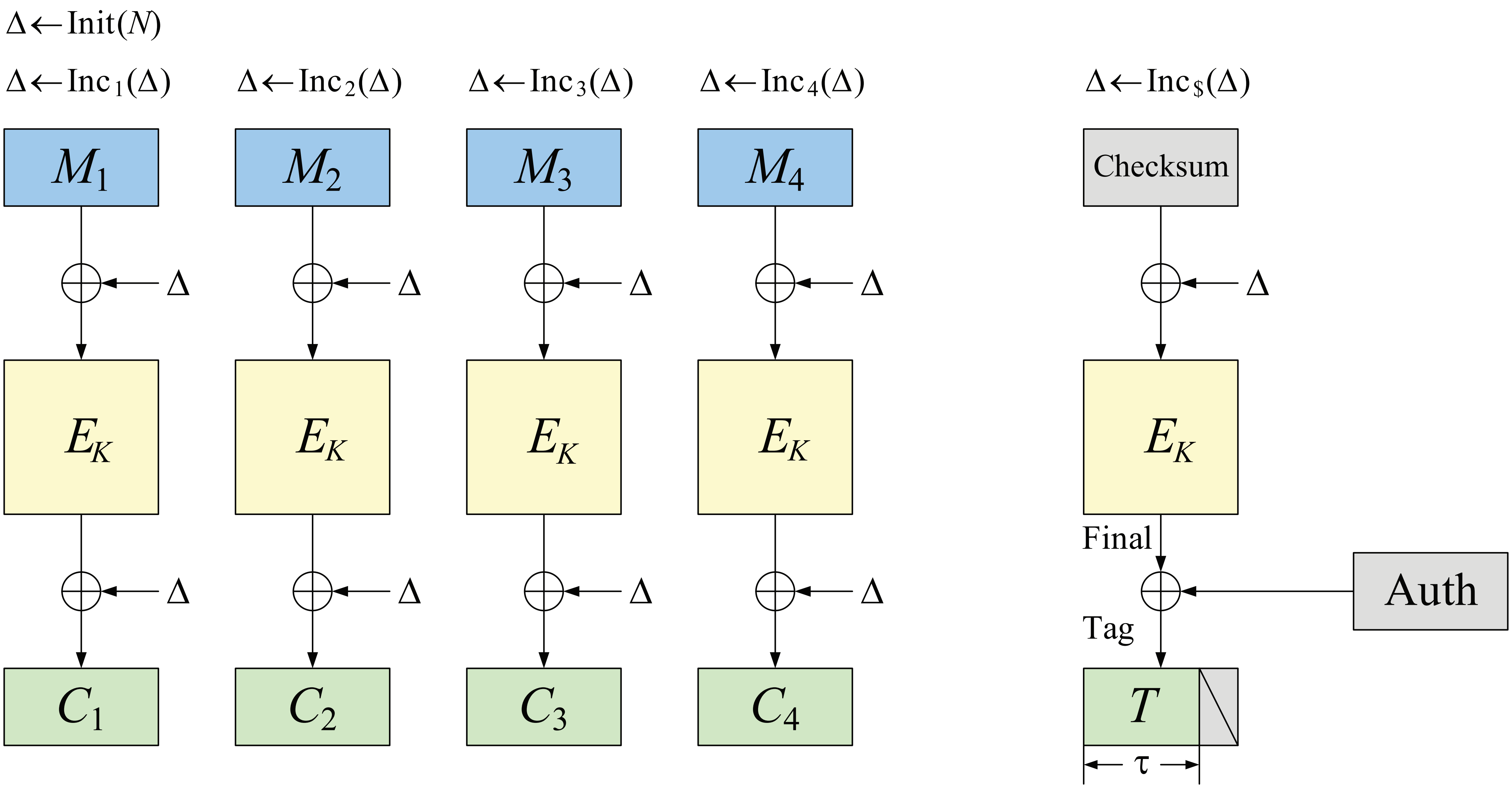
AE Approaches

- Confusion/diffusion: Authentication part of the primitive. (Helix, SOBER,…)
- Composed: Mix of discrete encryption and authentication schemes. (GCM, CCM,…)
- Integrated: Symbiotic encryption and authentication. (IAPM, OCB,…)

AE Block Cipher Modes

scheme	ref	date	ty	high-level description	standard
EtM	[1]	2000	C	Encrypt-then-MAC (and other) generic comp. schemes	ISO 19772
RPC	[23]	2000	I	Insert counters and sentinels in blocks, then ECB	—
IAPM	[21]	2001	I	Seminal integrated scheme. Also IACBC	—
XCBC	[11]	2001	I	Concurrent with Jutla's work. Also XECB	—
✓ OCB1	[35]	2001	I	Optimized design similar to IAPM	—
TAE	[28]	2002	I	Recasts OCB1 using a tweakable blockcipher	—
✓ CCM	[39]	2002	C	CTR encryption + CBC MAC	NIST 800-38C
CWC	[24]	2004	C	CTR encryption + GF($2^{127}-1$)-based CW MAC	—
✓ GCM	[31]	2004	C	CTR encryption + GF(2^{128})-based CW MAC	NIST 800-38D
EAX	[2]	2004	C	CTR encryption + CMAC, a cleaned-up CCM	ISO 19772
✓ OCB2	[34]	2004	I	OCB1 with AD and alleged speed improvements	ISO 19772
CCFB	[29]	2005	I	Similar to RPC [23], but with chaining	—
CHM	[18]	2006	C	Beyond-birthday-bound security	—
SIV	[36]	2006	C	Deterministic/misuse-resistant AE	RFC 5297
CIP	[17]	2008	C	Beyond-birthday-bound security	—
HBS	[20]	2009	C	Deterministic AE. Single key	—
BTM	[19]	2009	C	Deterministic AE. Single key, no blockcipher inverse	—
✓ OCB3	new	2010	I	Refines the prior versions of OCB	—

OCB Schematic

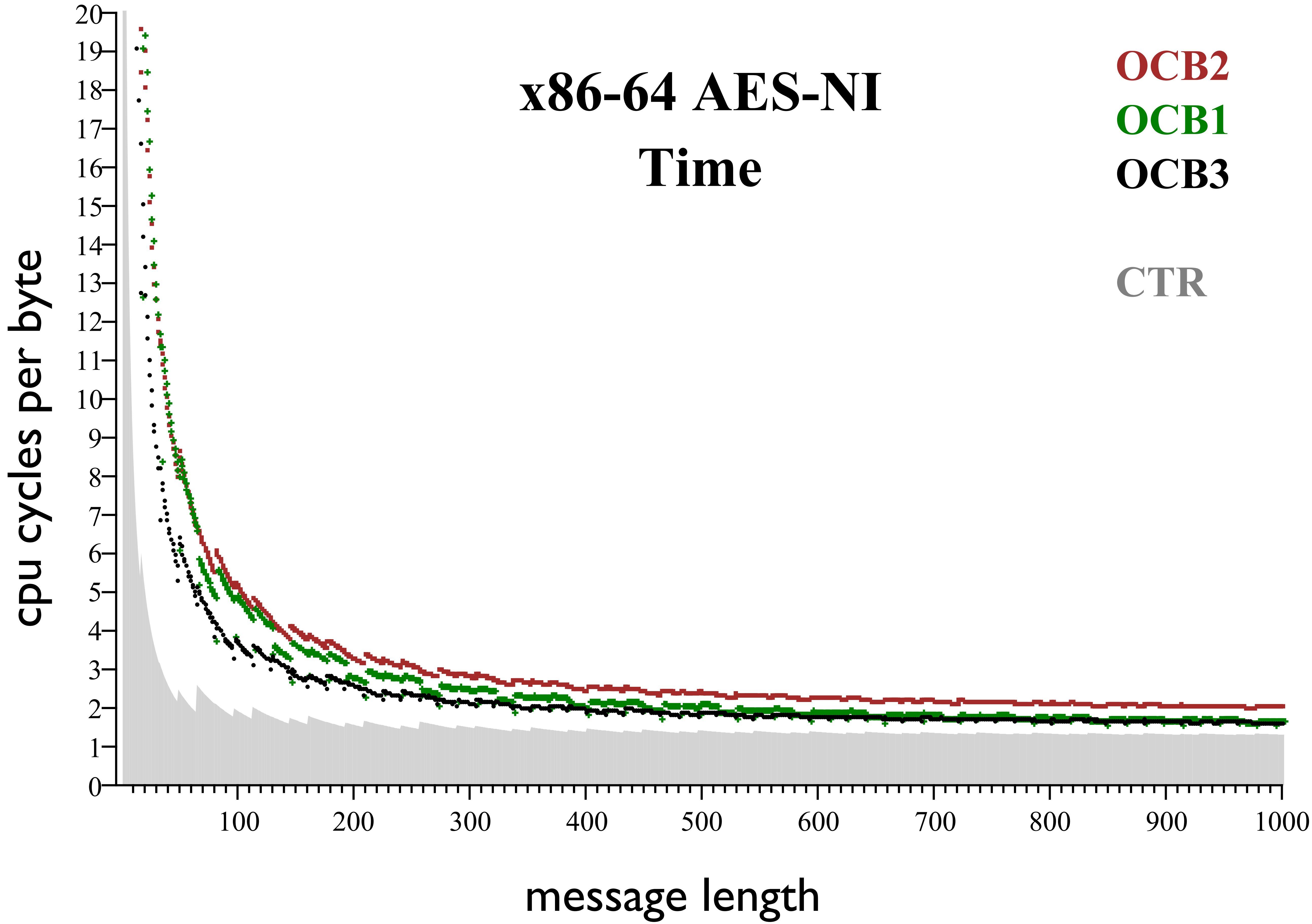


Common to OCB1/2/3

- $|C| = |P|$ + authentication tag
- Birthday-bound security
- Parallelizable
- Timing-attack resistant (if cipher is)

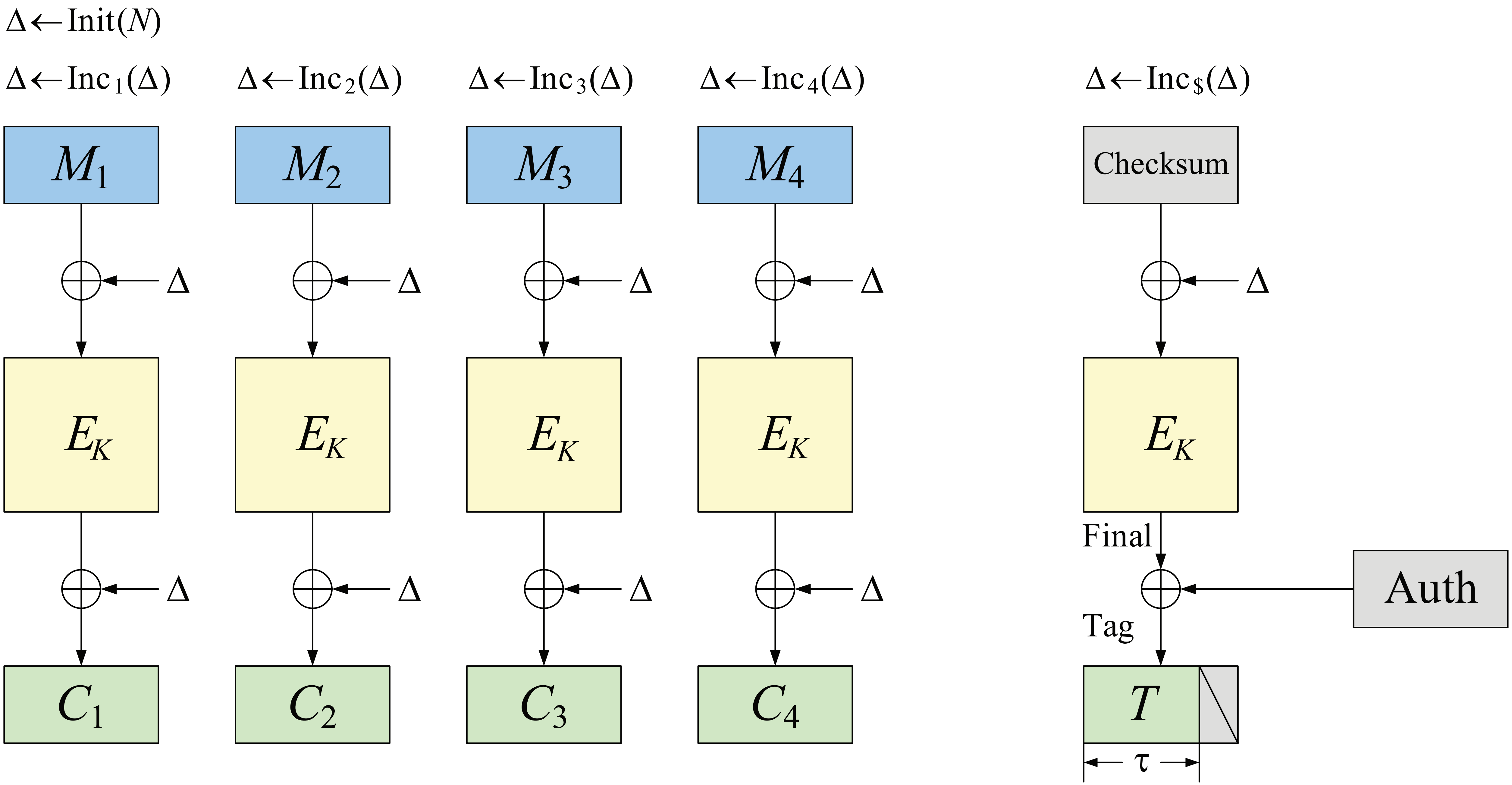
OCB Differences

	OCB1 (2001)	OCB2 (2004)	OCB3 (2011)
Increment	Table ops	Arithmetic	Table ops
Associated Data	No	Yes	Yes
Cipher Calls	M/n+2	M/n+2	M/n+1.02
Stalls	2	2	0



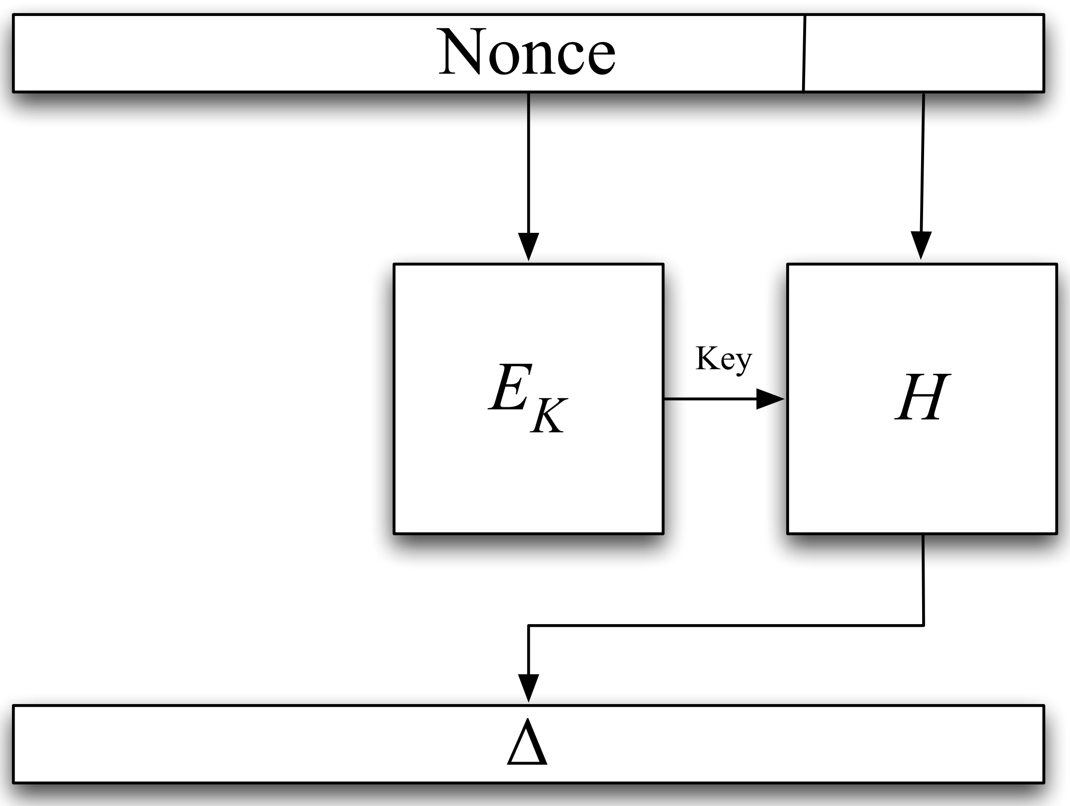
x86-64 AES-NI
Time
OCB2
OCB1
OCB3
CTR
cpu cycles per byte
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
100
200
300
400
500
600
700
800
900
1000
message length

OCB Schematic



Initial Offset

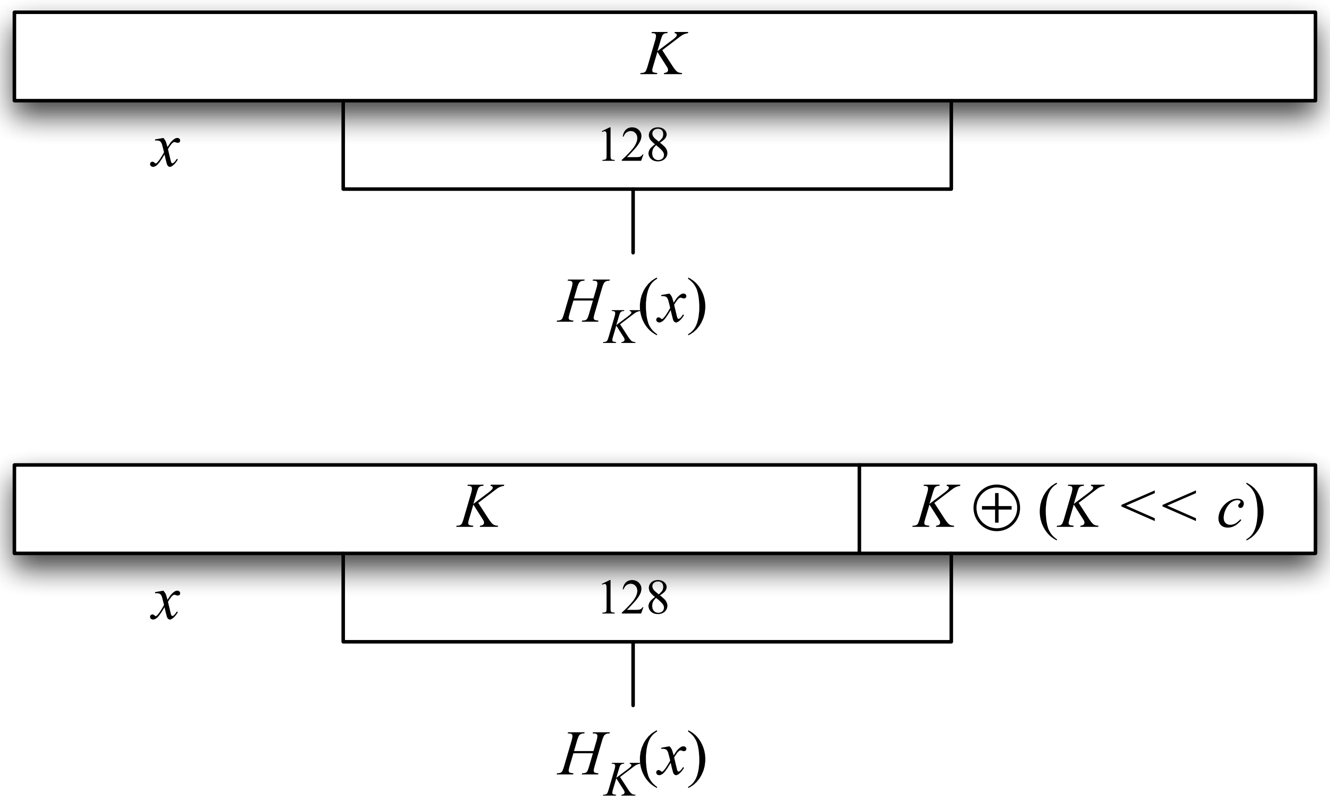
- Before: $\Delta = E(\text{Nonce})$.
- Now:



- Amortized cost: 1/64 E + 1 H per message.

Initial Offset

- *H* is small-domain xor-universal hash.

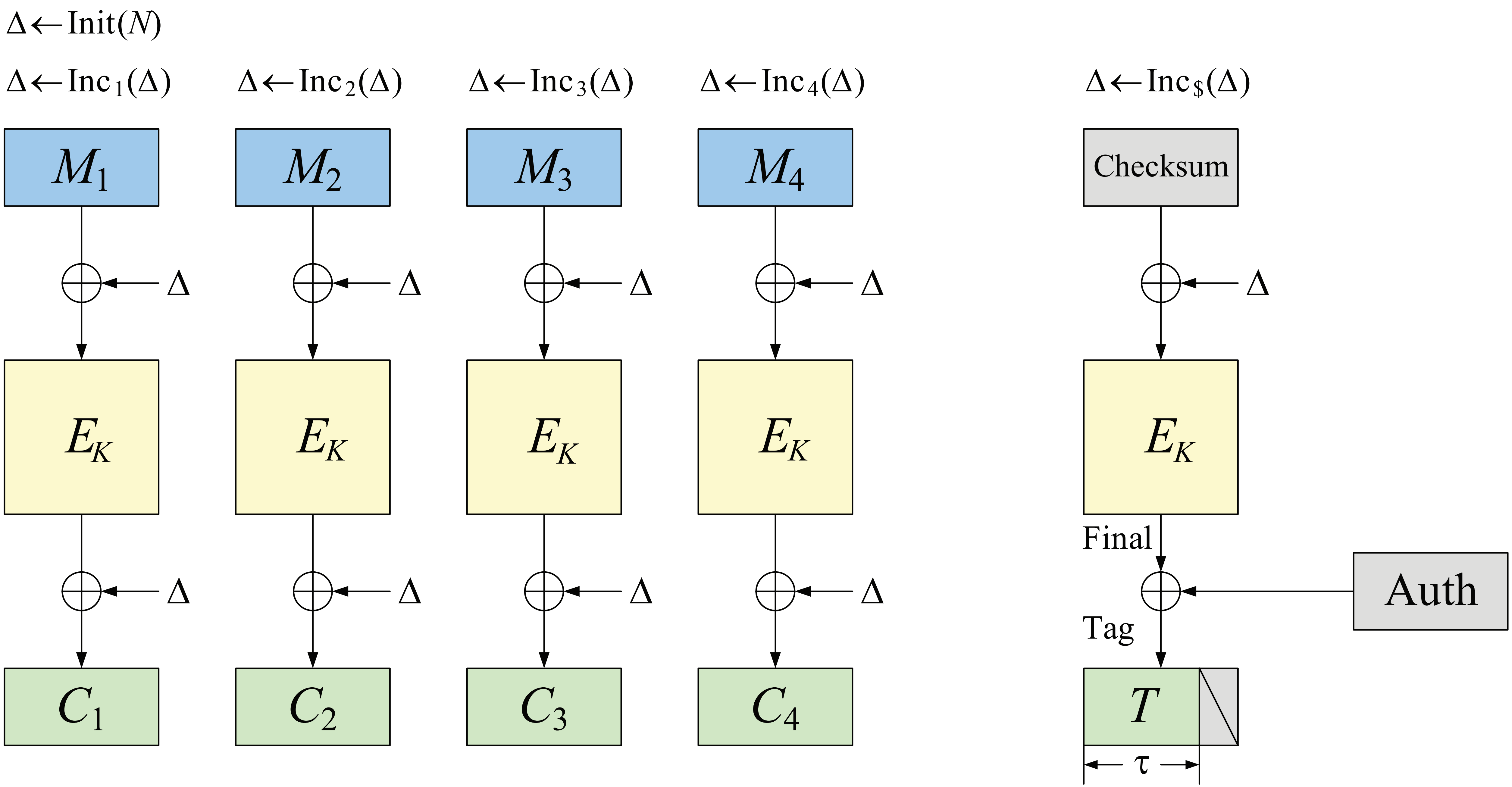


	$c = 5$	$c = 8$	$c = 9$	$c = 11$
domain	0…123	0…84	0…119	0…117

Proof H is Universal

- For each c and all $i \neq j$
  - Let $F(K) = H_K(i) \oplus H_K(j)$
  - Show $F(K)$ linear
- Test appropriate matrices are full rank.

OCB Schematic



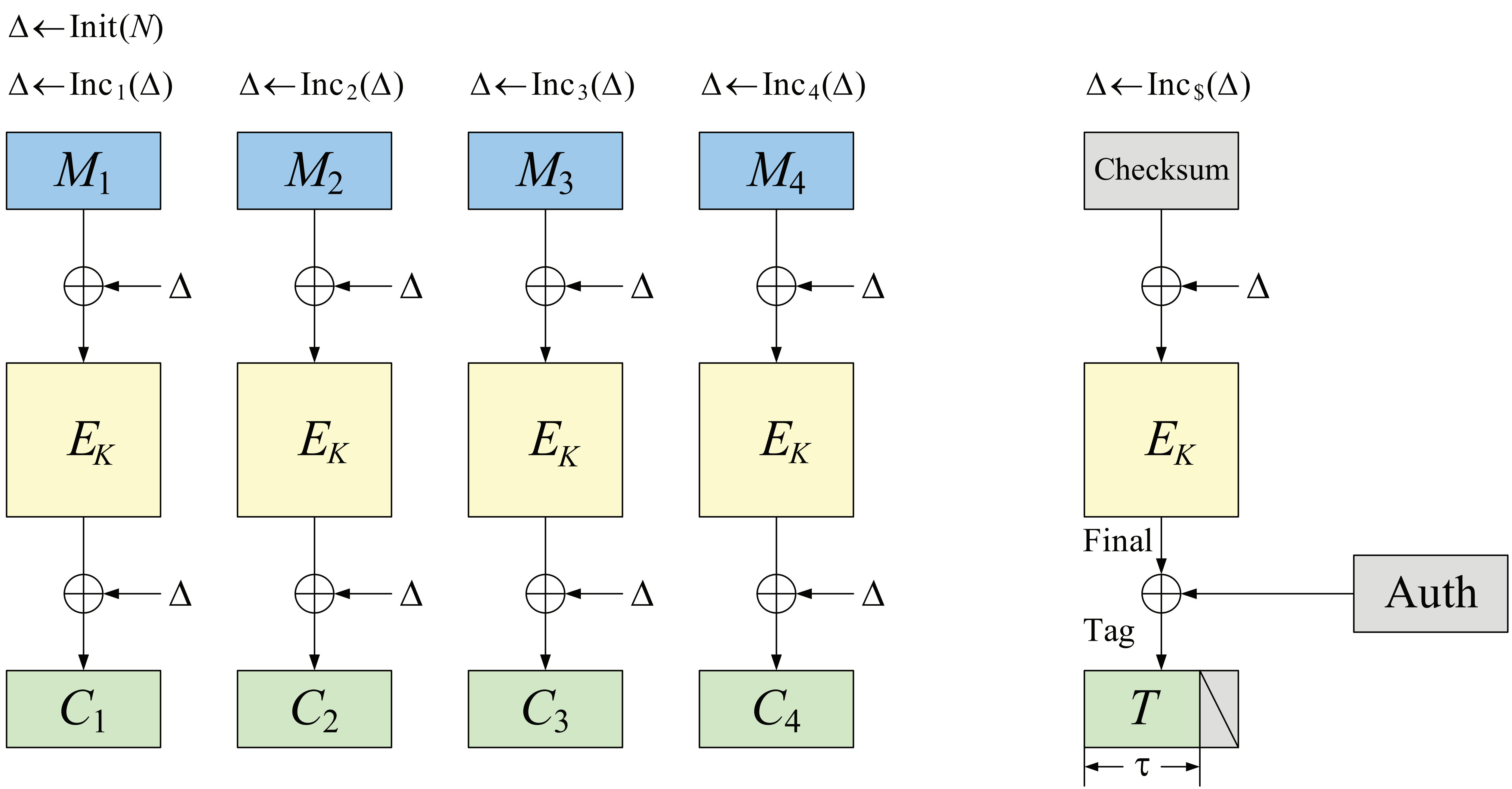
How to Increment

- OCB1: $\Delta_i = \bigoplus_{j=1\ldots i} (2^{\mathrm{ntz}(j)} \times \Delta_0)$
  $= \Delta_{i\text{-}1} \oplus \mathrm{Tbl}[\mathrm{ntz}(i)]$
- OCB2: $\Delta_i = 2^i \times \Delta_0$
  $= 2 \times \Delta_{i\text{-}1}$
- OCB3: Word-based LFSR? [CS]

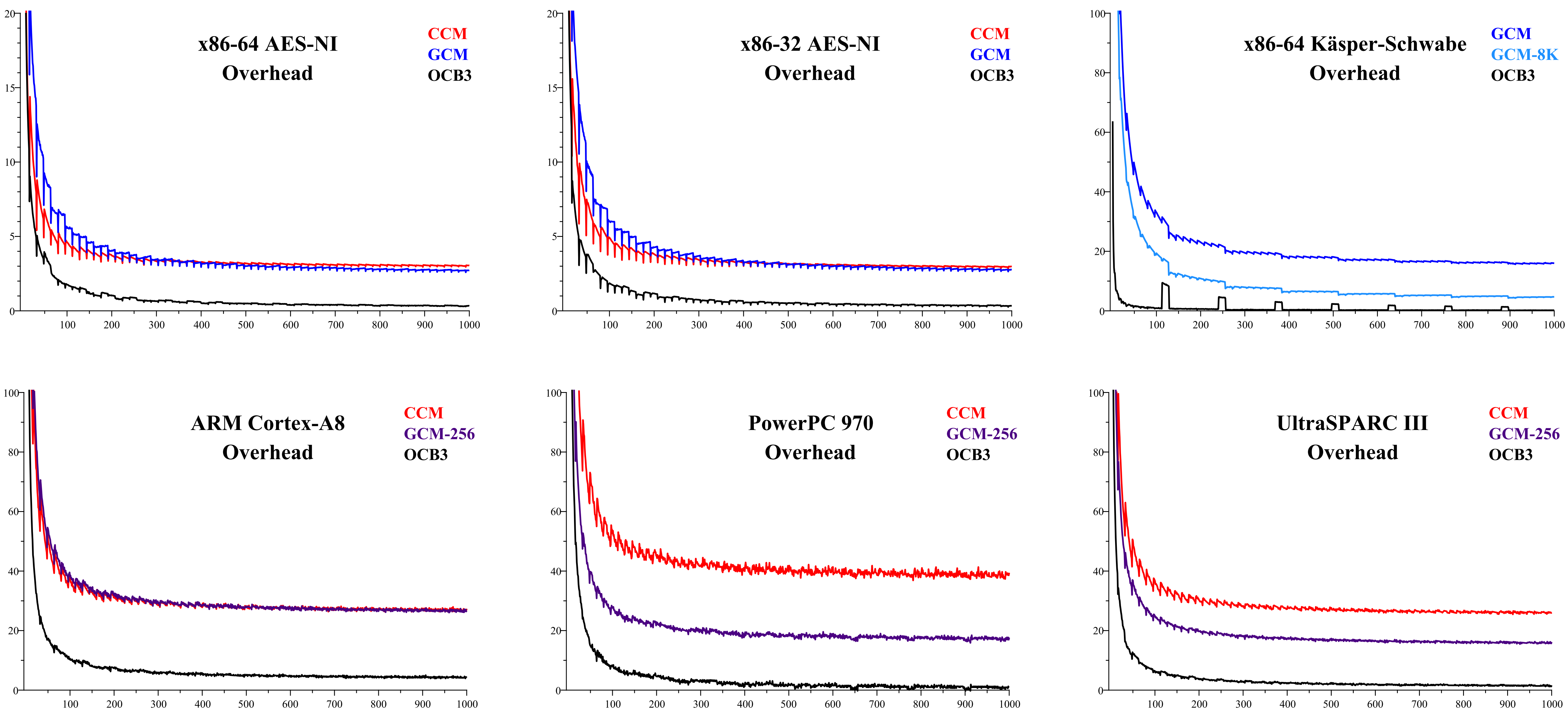
Word-based LFSR?

- $(A, B) = (B, 2A)$
  $(A, B) = (B, (A{<<}1) \oplus (A{>>}1) \oplus (B \wedge 148))$
  $(A, B, C, D) = (C, D, B, 2A \oplus B \oplus D)$
  $(A, B, C, D) = (C, D, B, (A{<<}1) \oplus (A{>>}1) \oplus (D \wedge 107))$
  $(A, B, C, D) = (C, D, B, (A{<<}1) \oplus (A{>>}1) \oplus (D{<<}15))$
- Each verified maximal by testing irreducibility of representative polynomial.
- None best on all architechtures.
  None faster than ntz + table-lookup.

OCB Schematic



Authentication Overhead



Effect of AES-NI

	Käsper/ Schwabe	Westmere AES-NI	How much better?
OCB	8.05 peak 9.24 IPI	1.48 peak 1.87 IPI	82% 80%
GCM	10.9 peak 15.2 IPI	3.73 peak 4.53 IPI	66% 70%
CTR	7.74 peak 8.98 IPI	1.27 peak 1.37 IPI	84% 85%

- OCB harnesses more improvement.
- More so under Sandy Bridge. OCB $\approx$ 1 cpb

Finally

- This is the last OCB. No more revisions.
- Submission to NIST this summer.
- www.cs.ucdavis.edu/~rogaway/ocb/performance has all the data and code used for this paper.