

Authenticated Encryption Mode for Beyond the Birthday Bound Security

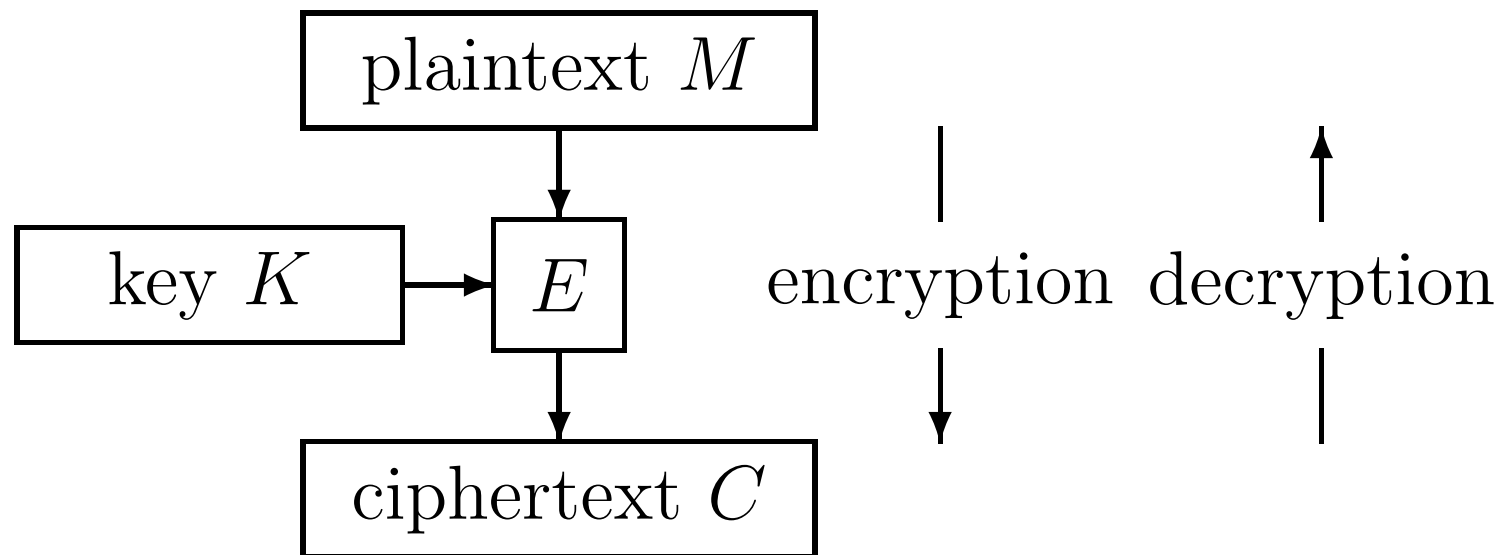
Tetsu Iwata
Nagoya University

`iwata@cse.nagoya-u.ac.jp`

ESC, Echternach Symmetric Crypto seminar

January 11, 2008

Blockcipher



- $|M| = |C| = n$ (block length), $|K| = k$ (key length)
- designed to withstand various known attacks (diff. attack, linear attack,...)
- indistinguishable from a random permutation even if the adversary obtains $2^n - \delta$ plaintext-ciphertext pairs

Blockcipher Modes

- privacy: CBC mode, CTR mode,...
- authenticity: CBC MAC, CMAC, PMAC,...
- privacy and authenticity: GCM, OCB, EAX,...

Security Proofs

- birthday bound
- success probability $O(\sigma^2/2^n)$
- σ : amount of data adversary obtains

Security Proofs with Beyond the Birthday Bound

- privacy: CENC, NEMO
- authenticity: RMAC, Poly1305, MACH
- privacy and authenticity: Generic Composition, CHM

Beyond the Birthday Bound?

- higher security is a valid goal
- huge gap between blockcipher security and mode security
 - blockcipher: $2^n - \delta$, mode: $2^{n/2}$
- some applications require $n = 64$ (HIGHT, Present)
 - 2^{32} is small

Goal of This Talk

- design of authenticated encryption mode, AE1
- beyond the birthday bound security
- fix several problems in existing modes

Authenticated Encryption

- two security goals:
 - privacy
 - authenticity
- two design approaches
 - generic composition: secure encryption + secure MAC (BN00, K01)
 - one algorithm of dedicated design, more efficient than generic composition

Authenticated Encryption Using Blockcipher

- IAPM, IACBC (Jutla '01)
- XCBC, XECBS (Gligor, Donescu '01)
- OCB (Rogaway '01)
- GCM (McGrew and Viega '04)
- CHM (Iwata '06)
- ...

GCM (McGrew, Viega '04, NIST SP 800-38D)

- Galois Counter Mode
- recommended by NIST as NIST SP 800-38D
- IETF 4160, payload encryption in IPSec
- IEEE 802.1AE, Media Access Control Security, frame data encryption in Layer 2 of the Ethernet
- IEEE P1619.1, tape storage encryption

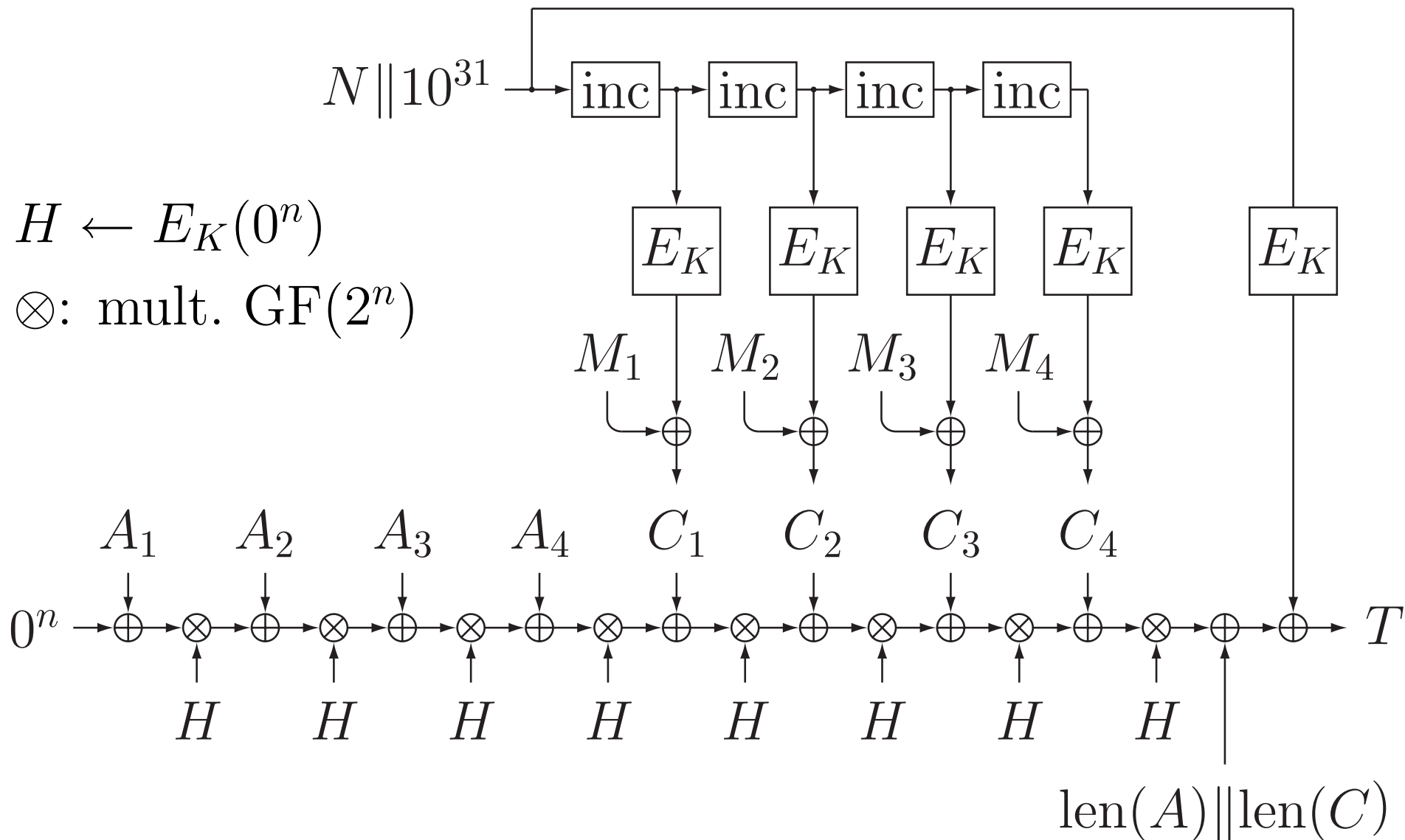
GCM (McGrew, Viega '04, NIST SP 800-38D)

- blockcipher E
- inputs: the key K , nonce N , plaintext M and header A
- outputs: the ciphertext C and tag T

$$(K, N, M, A) \rightarrow \boxed{\text{GCM}} \rightarrow (C, T)$$

- M is encrypted and authenticated
- A is authenticated (and not encrypted)
- M and A can be any lengths
- $|C| = |M|$

Encryption of GCM

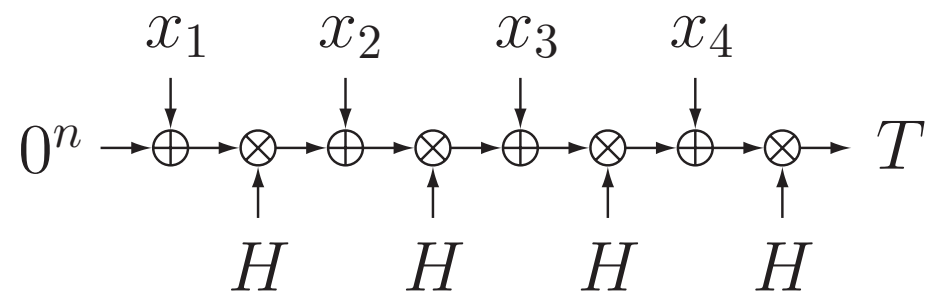


Properties

- combines CTR mode and polynomial hash over $\text{GF}(2^n)$
- uses single key
- provable security
 - privacy: $O(\sigma^2/2^n)$
 - authenticity: $O(\sigma^2/2^n)$
 - σ : length of data in blocks
- allows parallel calls of E
 - can boost the throughput of encryption

Properties

- polynomial hash is not parallelizable



- can be a bottleneck for hardware
(Sato et. al., ISC '07 can be used)
- C can not be processed until finishing A
 - can be a problem if C is ready before A
- usual birthday bound security

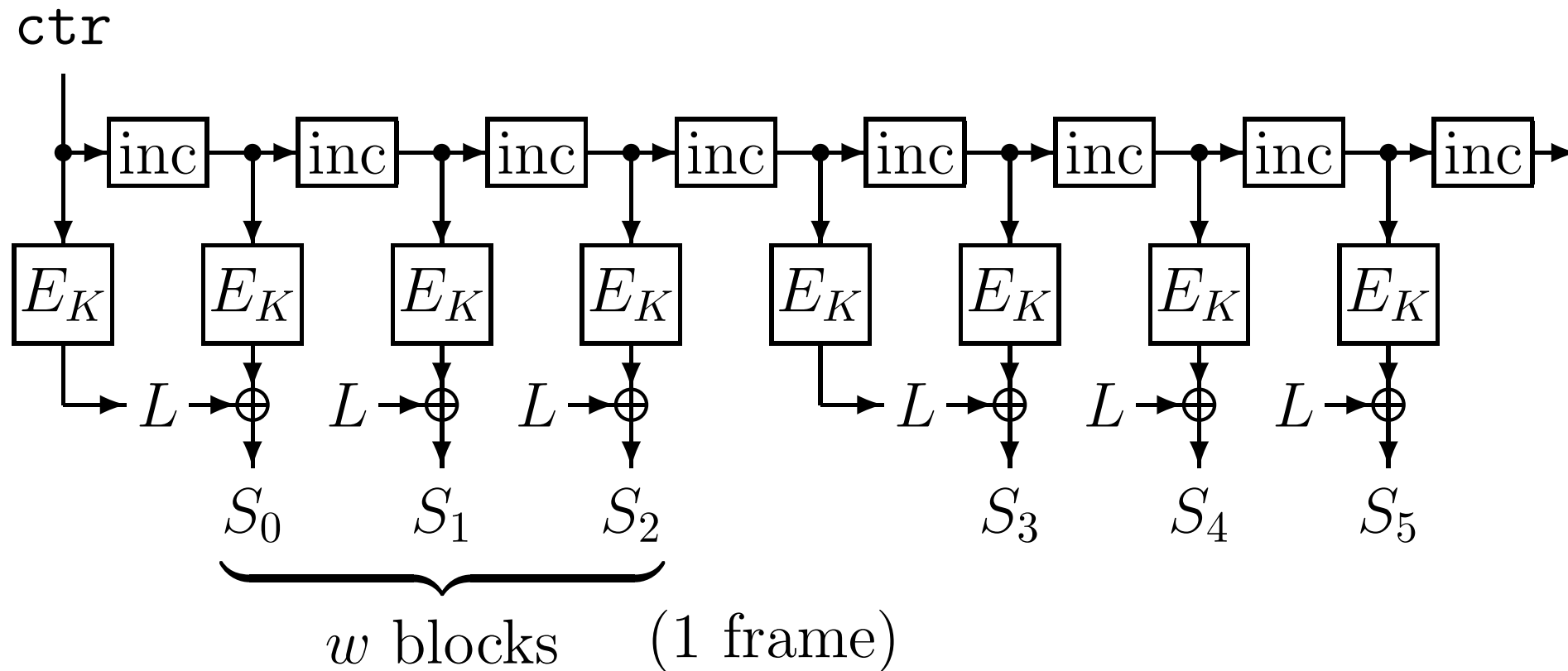
CHM (Iwata, FSE '06)

- CENC with Hash based MAC
- C can not be processed until finishing A
 - A and C are MACed separately
- usual birthday bound security
 - uses CENC for encryption
 - CENC: encryption mode

Parameters of CENC

- blockcipher $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$
- nonce length: ℓ_{nonce} bits, $\ell_{\text{nonce}} < n$
- frame width: w

Key Stream Generation of CENC



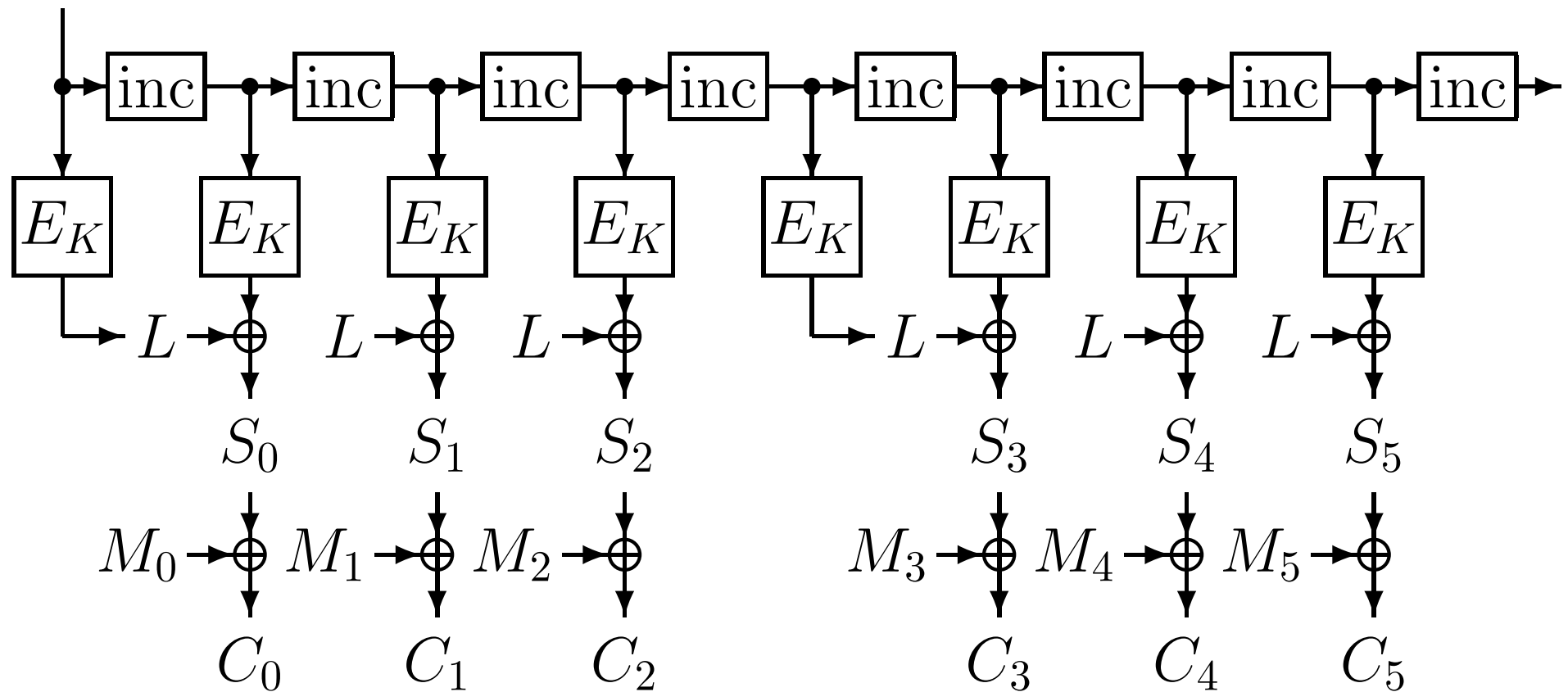
- L : mask
- w : frame width, default: $w = 2^8 = 256$
- N : nonce, $\text{ctr} \leftarrow N || 0 \dots 0$, default: $|N| = \ell_{\text{nonce}} = n/2$

Encryption of CENC

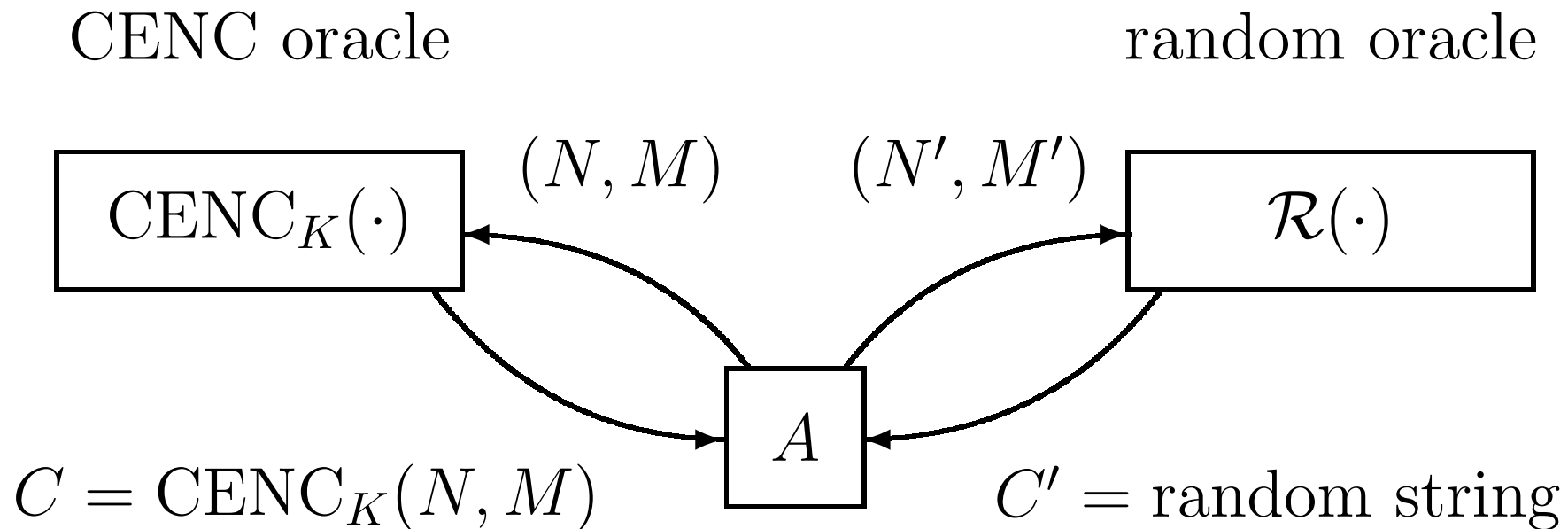
$N || 0 \dots 0$



ctr



Indistinguishability from Random String



A must not repeat the same nonce

$$\mathbf{Adv}_{\text{CENC}}^{\text{priv}}(A) \stackrel{\text{def}}{=} \left| \Pr_K(A^{\text{CENC}_K(\cdot, \cdot)} = 1) - \Pr_{\mathcal{R}}(A^{\mathcal{R}(\cdot, \cdot)} = 1) \right|$$

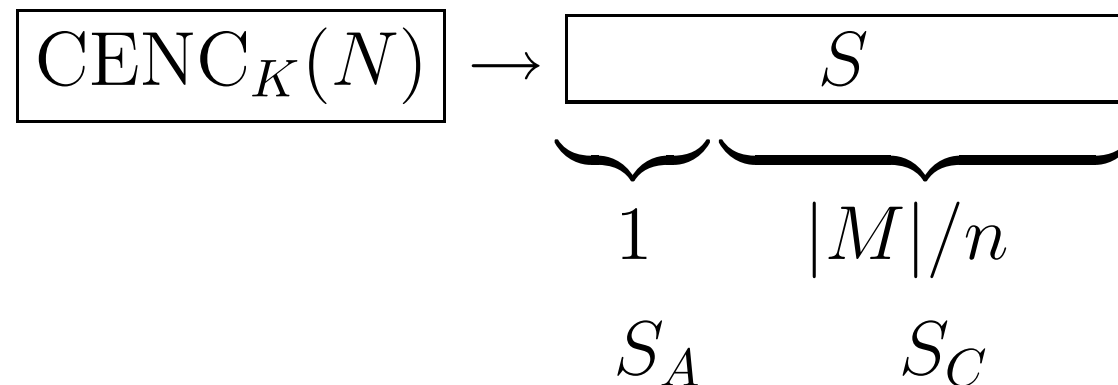
Security Theorem of CENC

$$\mathbf{Adv}_{\text{CENC}}^{\text{priv}}(A) \leq \frac{w\hat{\sigma}^3}{2^{2n-3}} + \frac{w\hat{\sigma}}{2^n} + \mathbf{Adv}_E^{\text{prp}}(B)$$

- A : q queries with total of σ blocks
- B : $(w + 1)\hat{\sigma}/w$ queries
- $\hat{\sigma} = \sigma + qw$
- beyond the birthday bound

CHM (Iwata, FSE '06)

- CENC with Hash based MAC
- $S_0 \leftarrow E_K(1^{n-1}0)$, $S_1 \leftarrow E_K(1^n)$,
- use CENC to produce $1 + |M|/n$ blocks of S



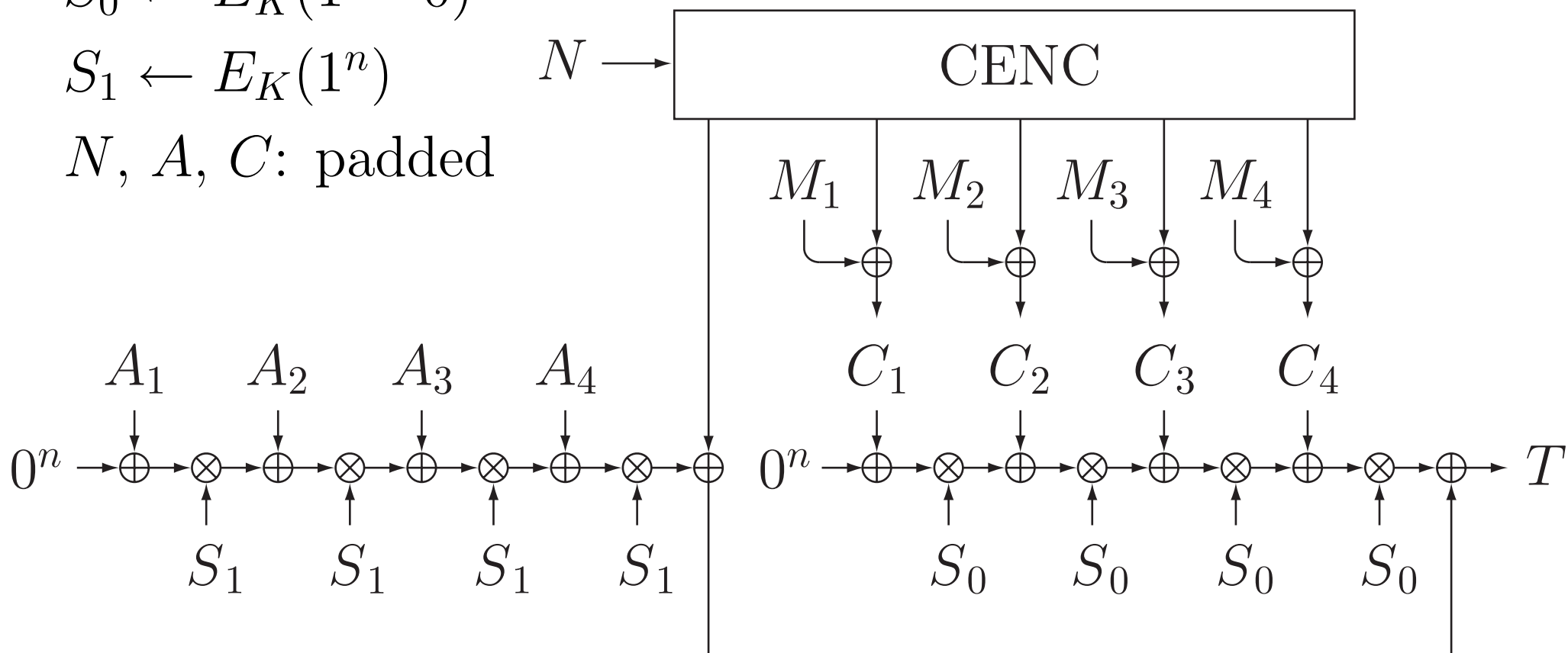
- $C \leftarrow M \oplus$ (first $|M|$ bits of S_C)
- $T \leftarrow \text{Hash}_{S_0}(C) \oplus \text{Hash}_{S_1}(A) \oplus S_A$ (truncate if needed)

Encryption of CHM

$$S_0 \leftarrow E_K(1^{n-1}0)$$

$$S_1 \leftarrow E_K(1^n)$$

N, A, C : padded



Security Theorems

- privacy

$$\mathbf{Adv}_{\text{CHM}}^{\text{priv}}(A) \leq \frac{w\tilde{\sigma}^2}{2^{2n-6}} + \frac{w\tilde{\sigma}^3}{2^{2n-3}} + \frac{1}{2^n} + \frac{w\tilde{\sigma}}{2^n}$$

- authenticity

$$\mathbf{Adv}_{\text{CHM}}^{\text{auth}}(A) \leq \frac{w\tilde{\sigma}^2}{2^{2n-6}} + \frac{w\tilde{\sigma}^3}{2^{2n-3}} + \frac{1}{2^n} + \frac{w\tilde{\sigma}}{2^n} + \frac{(1 + H_{\max} + M_{\max})}{2^\tau}$$

- beyond the birthday bound, $\tau \leq n$: tag length
- H_{\max}, M_{\max} are max. block lengths of header and plaintext

Properties

- combines CENC and polynomial hash
- uses single key
- A and C are MACed separately
- better than the birthday bound security
 - problem if τ is small (e.g. $\tau = 32$ or 48)
 - similar to GCM

$$\mathbf{Adv}_{\text{CHM}}^{\text{auth}}(A) \leq \dots + \frac{(1 + H_{\max} + M_{\max})}{2^{\tau}}$$

- polynomial hash is not parallelizable (as in GCM)
 - can be a bottleneck for hardware

Inner Product Hash

- fully parallelizable
- inputs: $x = (x_1, \dots, x_t)$, key $k = (k_1, \dots, k_t)$,
- output: $H_k(x) = (x_1, \dots, x_t) \cdot (k_1, \dots, k_t)$
 $= x_1 \cdot k_1 \oplus \dots \oplus x_t \cdot k_t$

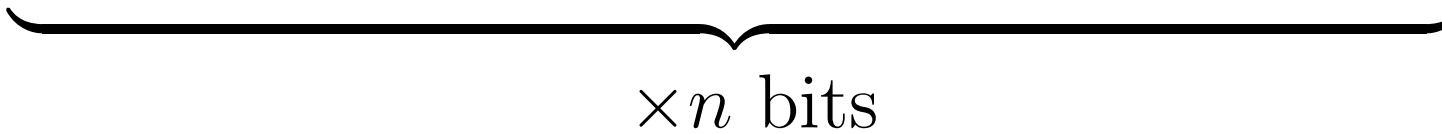
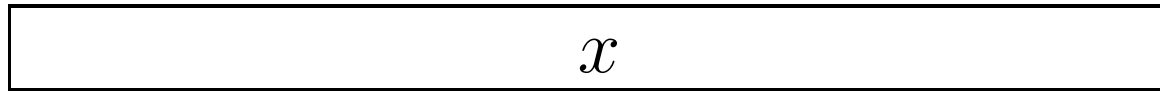
multiplication over $\text{GF}(2^n)$

- $|k|$ can be large, $|x| = |k|$

AE1 (This Talk)

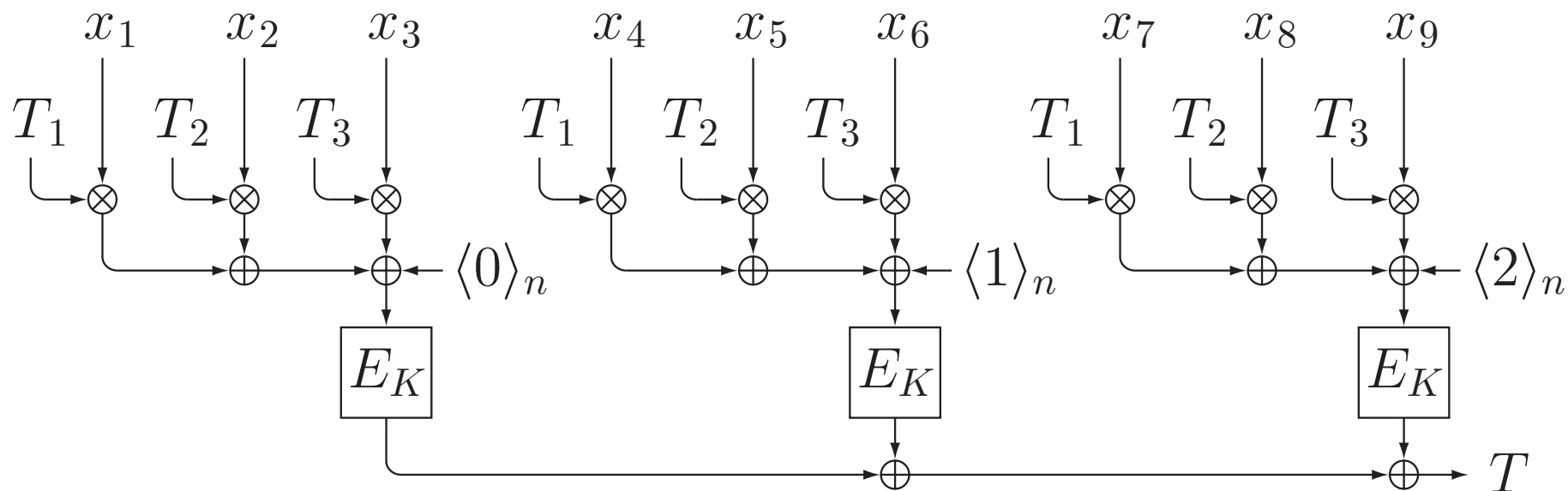
- uses blockcipher
- can be used even if τ is small
- allows parallel computation
 - ϖ : frame width, default: $\varpi = 2$ or 4
- Hash part
 - input x , keys $K, T_1, \dots, T_{\varpi}$ (constant size)
 - output T

Padding for Hash



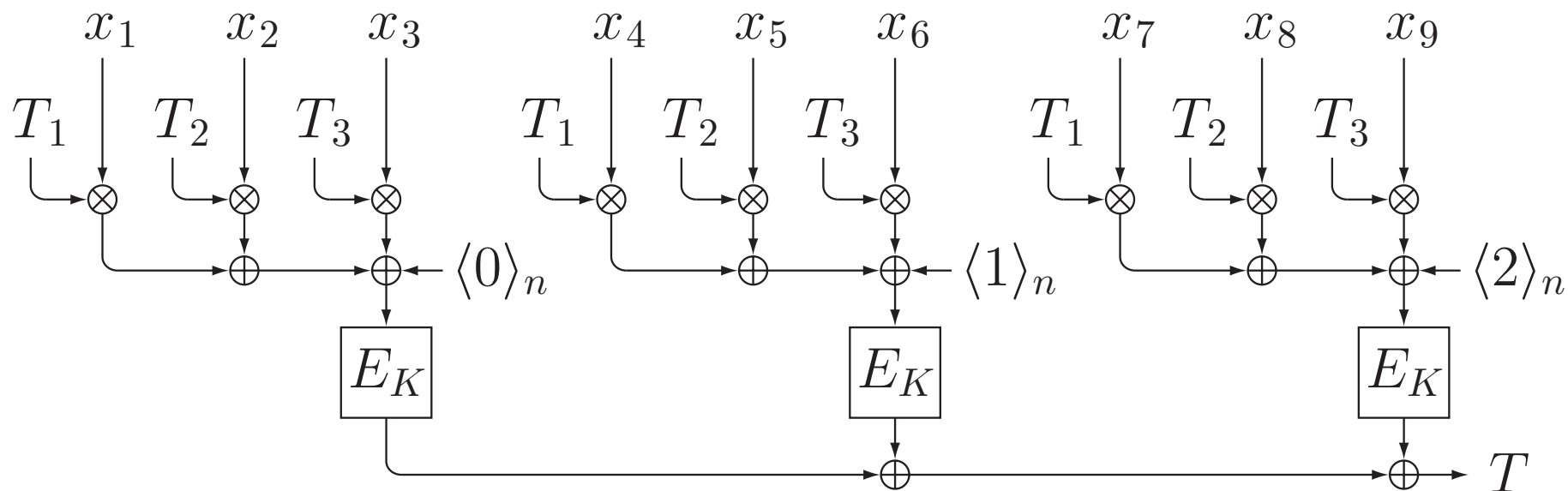
(1 frame)

Hash of AE1



- combines inner product $(x_1, \dots, x_\varpi) \cdot (T_1, \dots, T_\varpi)$ and E
- long (but constant) key size
- about $|x|/n$ field multiplications and $|x|/\varpi n$ E calls

Hash of AE1



- frame counter to avoid trivial swap
- last block of x is non-zero (by padding)
- proof that AE1.Hash is ϵ -AXU

AE1.Hash is ϵ -AXU (ϵ -almost XOR universal)

- H is ϵ -AXU if $\forall x, x' (x \neq x')$ and $\forall y \in \text{GF}(2^\tau)$,

$$\Pr(H_K(x) \oplus H_K(x') = y) \leq \epsilon$$

- **Proposition** $\forall x, x' (x \neq x')$ and $\forall y \in \text{GF}(2^\tau)$,

$$\Pr(H_K(x) \oplus H_K(x') = y) \leq \frac{\ell + \ell' - 1}{2^n} + \frac{2}{2^\tau} + \mathbf{Adv}_E^{\text{prp}}(A)$$

– x : ℓ frames, x' : ℓ' frames, $\ell + \ell' - 1 \leq 2^{n-1}$

– A makes at most $\ell + \ell'$ queries

- $2/2^\tau$ is a constant

Encryption of AE1

- Replace the Hash in CHM with AE1.Hash
- inputs: the key K , nonce N , plaintext M
- outputs: the ciphertext C and tag T

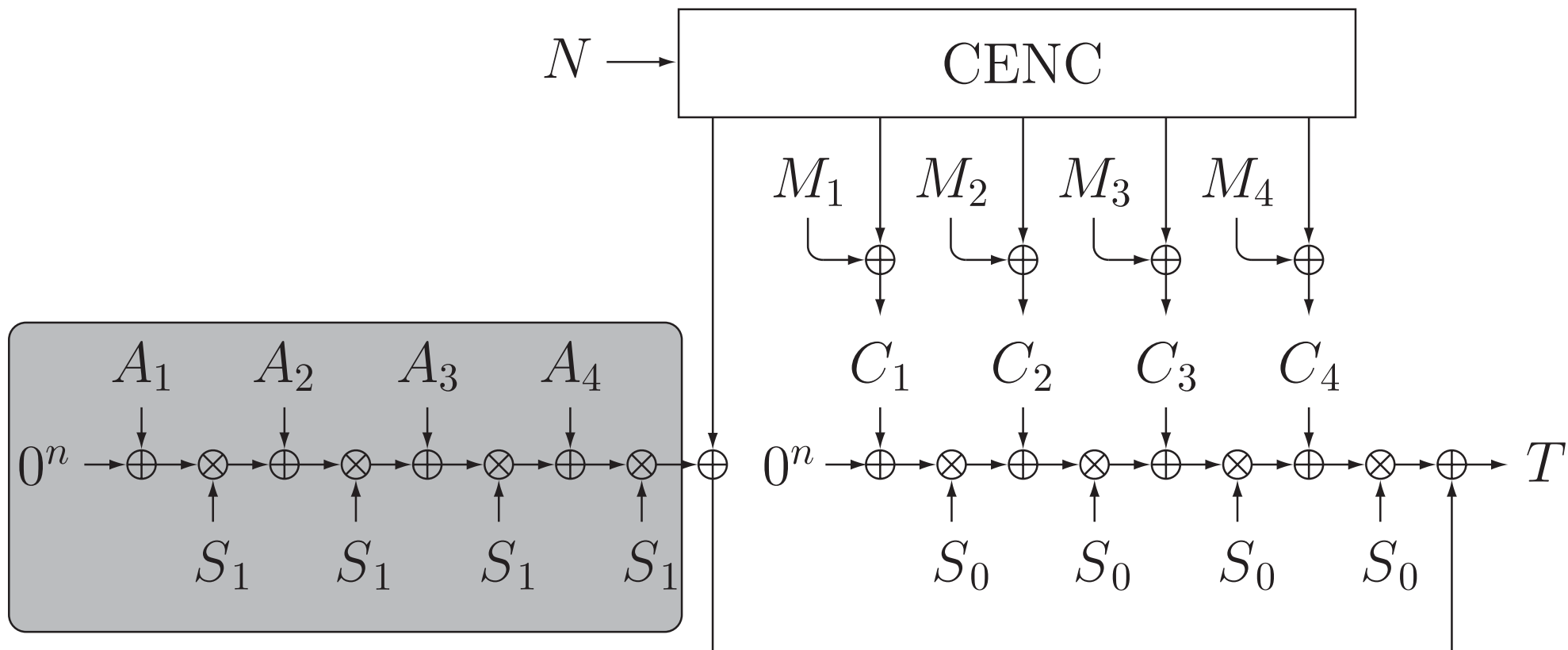
$$(K, N, M) \rightarrow \boxed{\text{AE1}} \rightarrow (C, T)$$

- M is encrypted and authenticated, can be any length,
 $|C| = |M|$

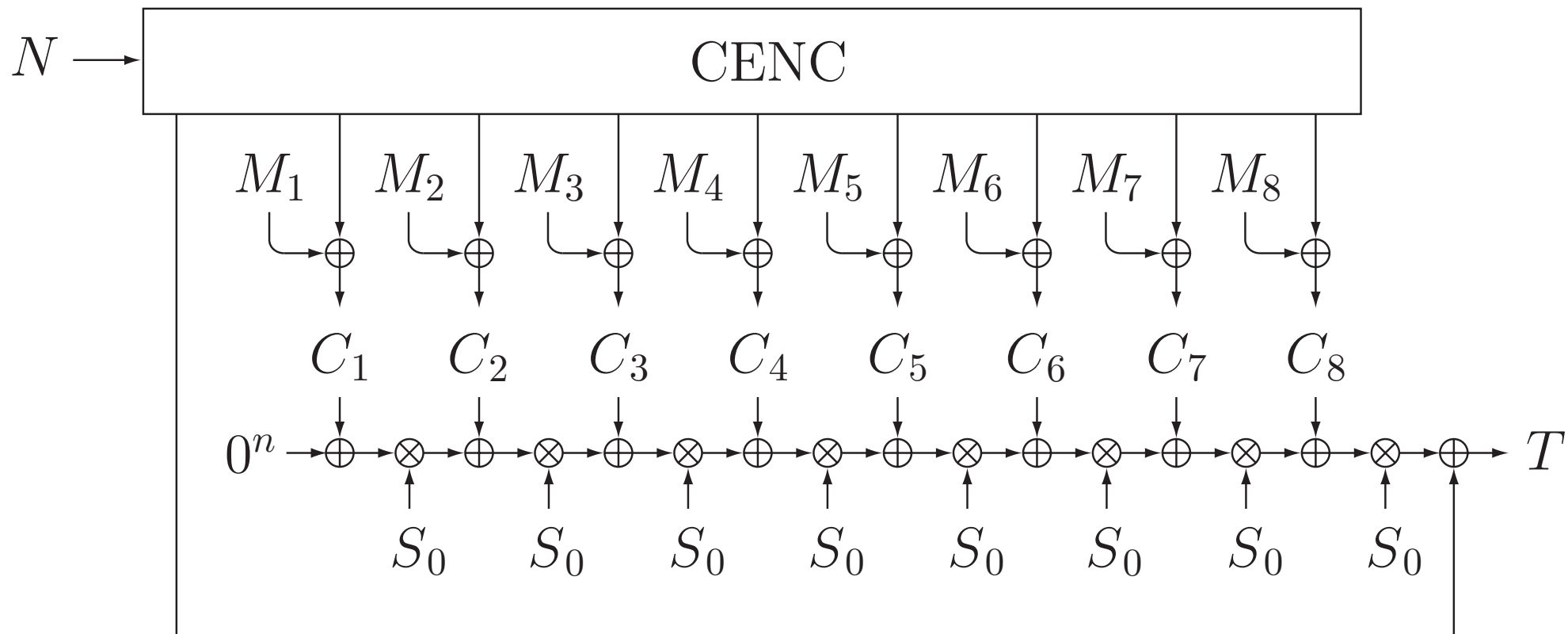
Hash Key Derivation of AE1

- Hash keys: $K_H, T_1, \dots, T_\varpi$
 - $K_H \leftarrow E_K(\langle 0 \rangle_{n/2} \| 1^{n/2}) \| \dots \| E_K(\langle \lceil k/n \rceil - 1 \rangle_{n/2} \| 1^{n/2})$
 - $T_1 \leftarrow E_K(\langle \lceil k/n \rceil \rangle_{n/2} \| 1^{n/2})$
 - $T_2 \leftarrow E_K(\langle \lceil k/n \rceil + 1 \rangle_{n/2} \| 1^{n/2})$
 - \dots
 - $T_\varpi \leftarrow E_K(\langle \lceil k/n \rceil + \varpi - 1 \rangle_{n/2} \| 1^{n/2})$

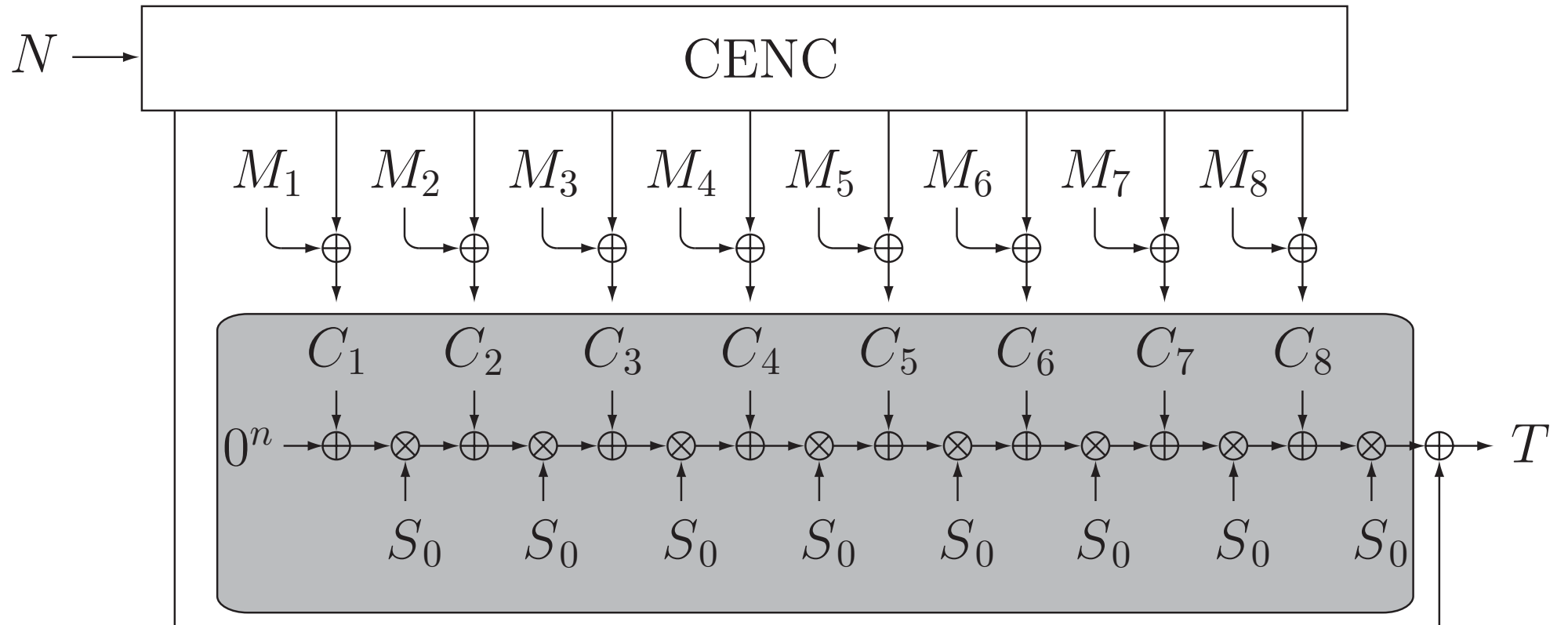
Encryption of AE1



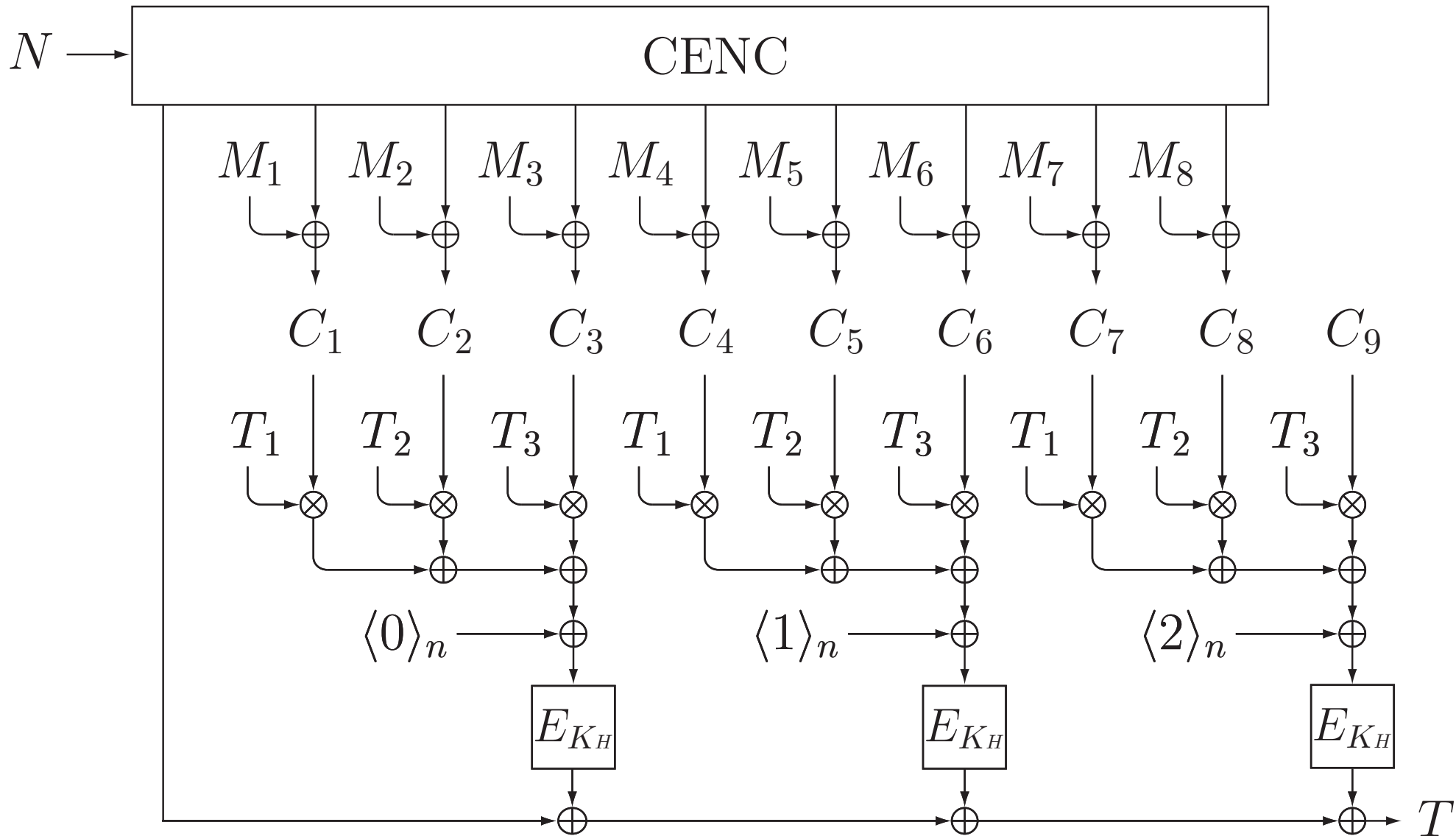
Encryption of AE1



Encryption of AE1



Encryption of AE1



Handling A

- use key derivation
- derive another K, T_1, \dots, T_ϖ
- make sure that blockcipher inputs are not re-used

Security Theorems of AE1

- privacy:

$$- \mathbf{Adv}_{\text{AE1}}^{\text{priv}}(A) \leq \frac{w\hat{\sigma}^3}{2^{2n-3}} + \frac{w\hat{\sigma}}{2^n}$$

- follows from the security of CENC

- privacy:

$$- \mathbf{Adv}_{\text{AE1}}^{\text{auth}}(A) \leq \frac{w\hat{\sigma}^3}{2^{2n-3}} + \frac{w\hat{\sigma}}{2^n} + \frac{\varpi^2}{2^{n+1}} + \frac{\sigma}{2^{n-1}} + \frac{2}{2^\tau}$$

- follows from the result of AE1.Hash

- $\hat{\sigma} = \sigma + q(w + 1)$

Security Theorems of AE1

- with AES,
 - AE1 can encrypt at most 2^{64} plaintexts
 - max plaintext length is 2^{62} blocks (2^{36} GBytes)
 - $\frac{\hat{\sigma}^3}{2^{245}} + \frac{\hat{\sigma}}{2^{120}}$ for privacy
 - $\frac{\hat{\sigma}^3}{2^{245}} + \frac{\hat{\sigma}}{2^{120}} + \frac{(\sigma + 1)}{2^{127}} + \frac{2}{2^\tau}$ for authenticity
 - secure up to $\hat{\sigma} \ll 2^{81}$ blocks (2^{55} GBytes)

Performance

- $m = |M|/n$ (block size of M), $a = |A|/n$ (block size of A)

	E calls	multiplications
GCM	m	$a + m$
CHM	$\frac{(w + 1)m}{w}$	$a + m$
AE1	$\frac{(w + 1)m}{w} + \frac{m}{\varpi} + \frac{a}{\varpi}$	$a + m$

- $w = 256, \varpi = 4$

Conclusions

- Many solutions for modes up to birthday bound security
 - privacy: CBC mode, CTR mode,...
 - authenticity: CBC MAC, CMAC, PMAC,...
 - privacy and authenticity: GCM, OCB, EAX,...
- Modes with beyond the birthday bound security
 - privacy: CENC, NEMO
 - authenticity: RMAC, Poly1305, MACH
 - privacy and authenticity: Generic Composition, CHM, **AE1**

Conclusions

- beyond the birthday bound security
- fix several problems in existing modes
 - parallelizability
 - introduce ϖ for constant Hash key length
 - can be used when MAC is truncated

Future Work

- better security, parallelizability with better efficiency (for software), handling arbitrary length nonce (limit in the length of one plaintext)