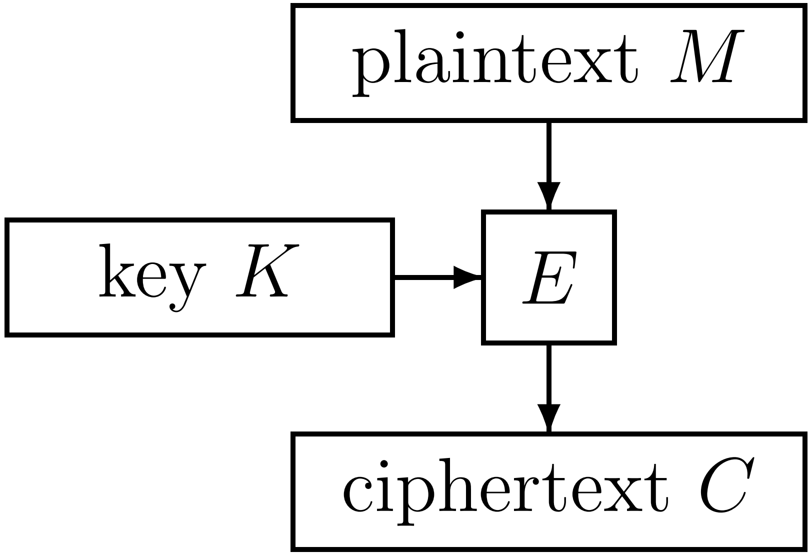
Authenticated Encryption Mode for Beyond the Birthday Bound Security

Tetsu Iwata
Nagoya University

iwata@cse.nagoya-u.ac.jp

Africacrypt 2008, Casablanca, Morocco
June 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

- success probability $O(\sigma^2/2^n)$
- birthday bound
- σ: amount of data adversary obtains (in blocks)
- n: block length of the underlying blockcipher (in bits)

Security Proofs with Beyond the Birthday Bound

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

Why Beyond the Birthday Bound?

- higher security is a valid goal
- huge gap between blockcipher security and mode security
  - blockcipher: $2^n - \delta$, mode: $2^{n/2} \cdots O(\sigma^2/2^n)$
  - The security of the blockcipher is *significantly lost* once it is plugged into the modes
  - CTR mode, CMAC, and GCM do not fully inherit the security of the blockcipher
- some applications require $n = 64$ (HIGHT, Present)
  - 2^{32} is small

Goal of This Paper

- design of an authenticated encryption mode, CIP
- CENC with Inner Product hash
- beyond the birthday bound security
- fix the security issue in the authenticity of CHM and GCM

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, NIST SP 800-38D)
- CHM (Iwata '06)
- $\cdots$

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

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

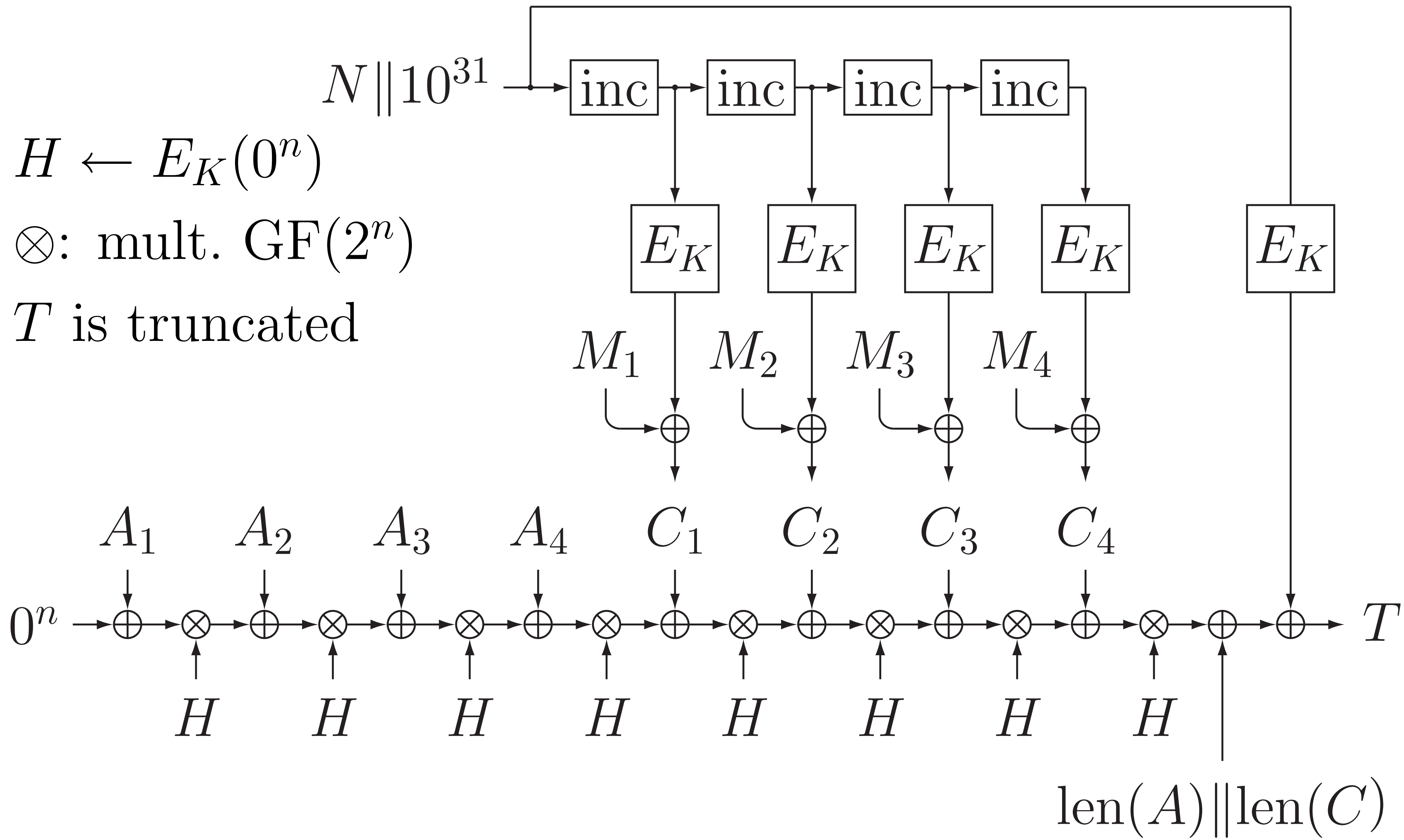
- M is encrypted and authenticated
- A is authenticated (and not encrypted)
- M and A can be any lengths
- $|C| = |M|$

Encryption of GCM

$H \leftarrow E_K(0^n)$

$\otimes$: mult. $\mathrm{GF}(2^n)$

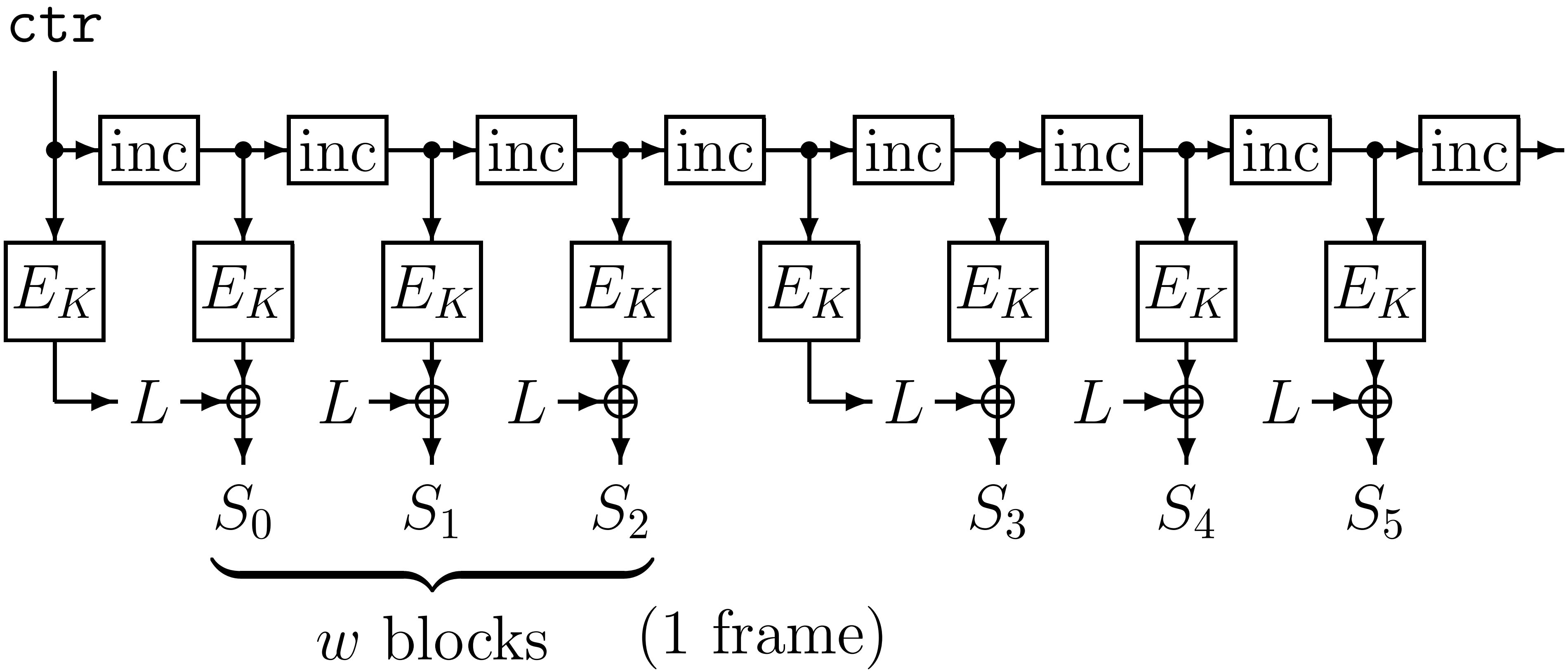
T is truncated



CHM (Iwata, FSE '06)

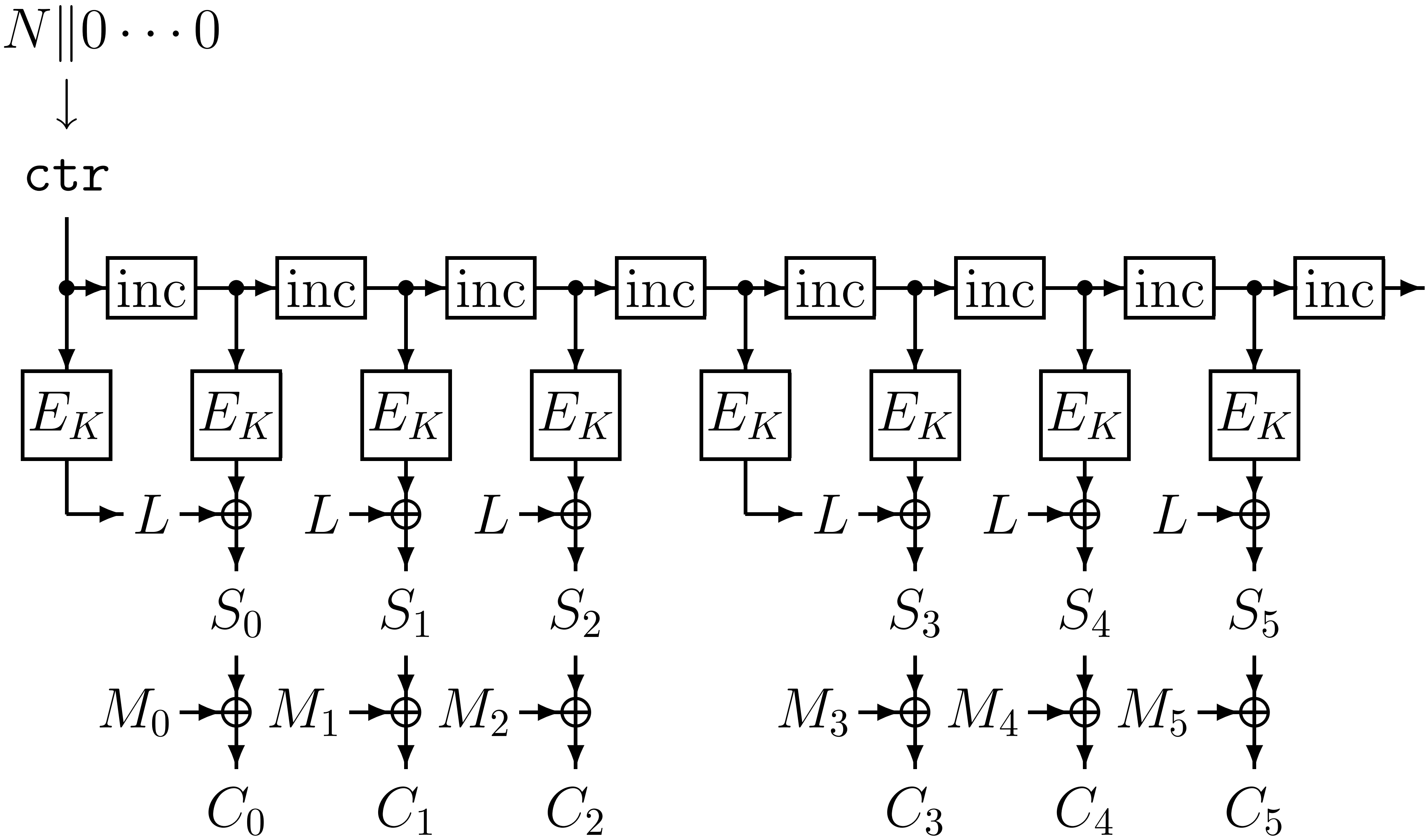
- CENC with Hash based MAC
- beyond the birthday bound security
  - CENC for encryption
  - encryption mode, Iwata, FSE '06
  - Parameters of CENC:
    * blockcipher $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
    * nonce length: ℓ_{nonce} bits, $\ell_{\text{nonce}} < n$
    * frame width: w

Key Stream Generation of CENC

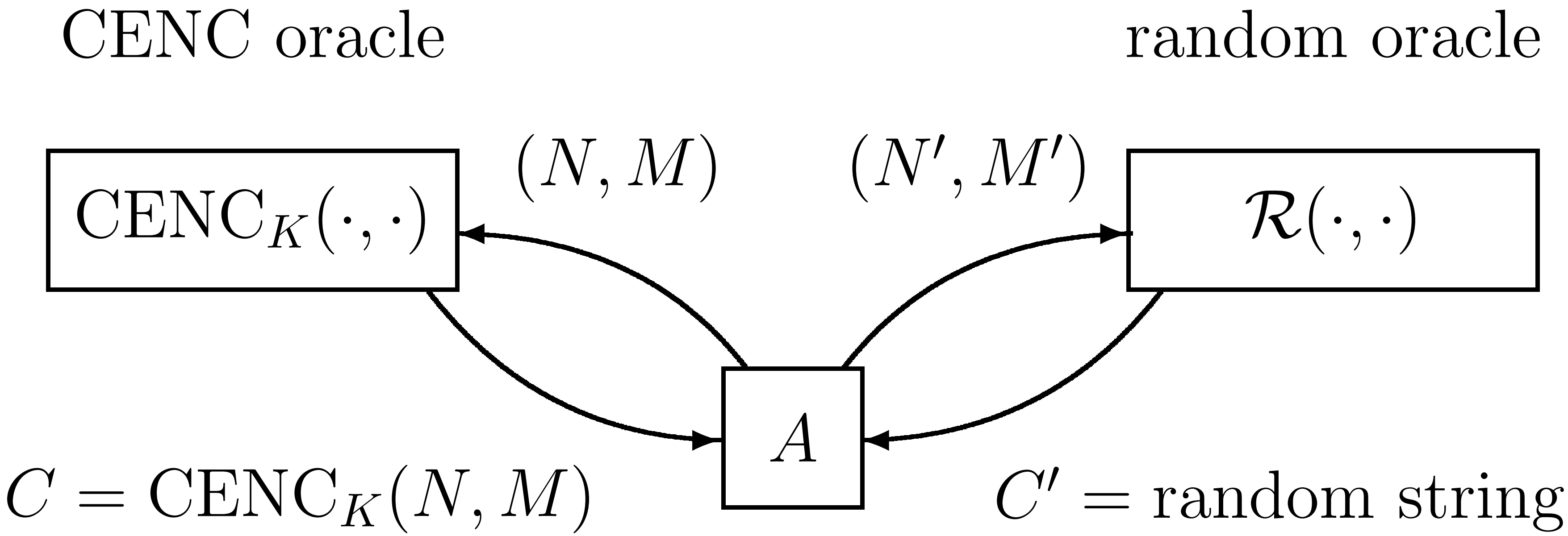


- L: mask
- w: frame width, default: $w = 2^8 = 256$
- N: nonce, $\mathtt{ctr} \leftarrow N \| 0 \cdots 0$, default: $|N| = \ell_{\text{nonce}} = n/2$

Encryption of CENC



Indistinguishability from Random String



A must not repeat the same nonce

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

Security Theorem of CENC

$$\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CENC}}(A) \le \frac{w\hat{\sigma}^3}{2^{2n-3}} + \frac{w\hat{\sigma}}{2^n}$$

- A: q queries with total of σ blocks
- $\hat{\sigma} = \sigma + qw$ $(\approx \sigma)$
- 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 $1 + \lceil |M|/n \rceil$ blocks of S

  ($\lceil |M|/n \rceil \cdots$ block length of M)

$$\boxed{\mathrm{CENC}_K(N)} \rightarrow \boxed{\quad S \quad}$$

$$\underbrace{\quad}_{\substack{1 \\ S_A}} \; \underbrace{\qquad\qquad}_{\substack{\lceil |M|/n \rceil \\ S_C}}$$

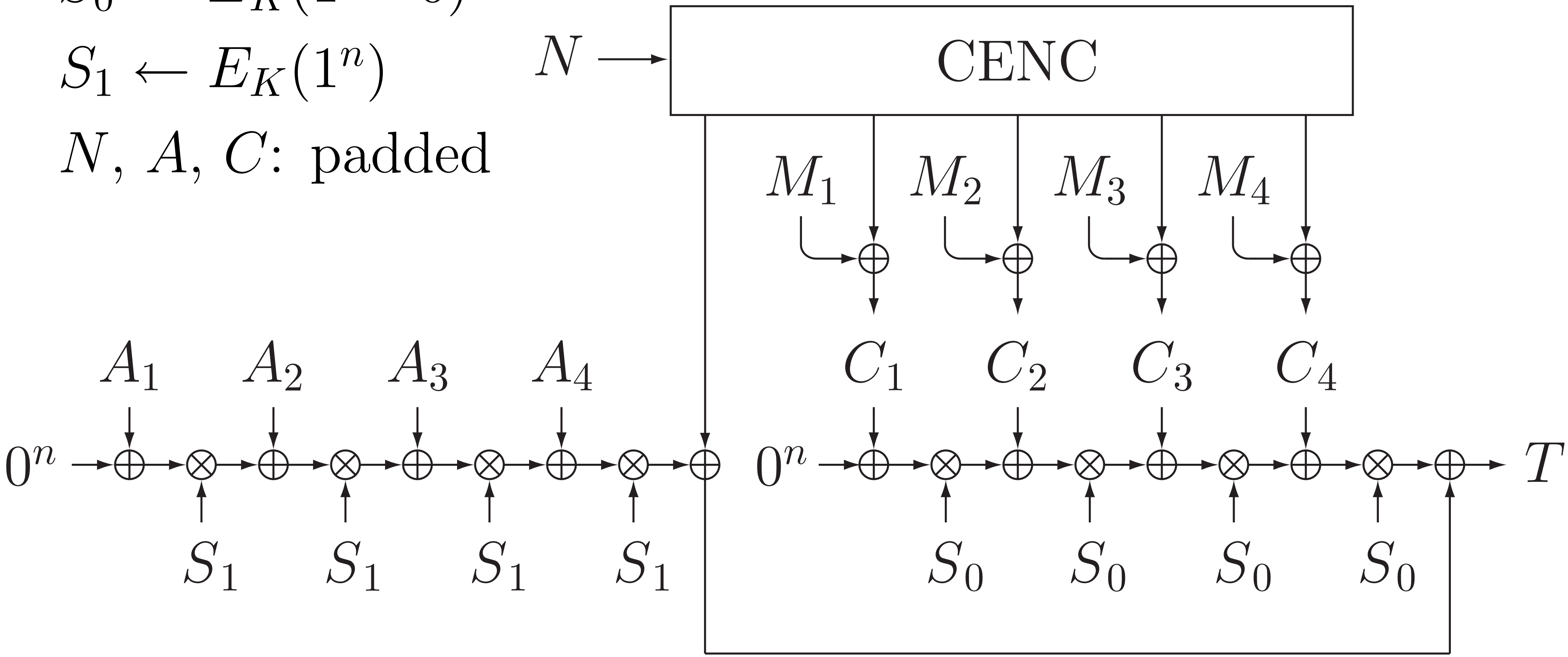
- $C \leftarrow M \oplus$ (first $|M|$ bits of S_C)
- $T \leftarrow \mathrm{Hash}_{S_0}(C) \oplus \mathrm{Hash}_{S_1}(A) \oplus S_A$ (truncate if needed)

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

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

- authenticity

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

- τ: tag length, $\tau \le n$
- $H_{\max}$, $M_{\max}$ are max. block lengths of header and plaintext

Security Issue

- T is τ bits

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

- Consider the case where τ is small, e.g. $\tau = 32$
- with only one message of length 2^{22} blocks (64 MBytes), the bound is 1/1024 (not acceptable in general)
- "beyond the birthday bound security" has little impact when τ is small
- same issue in GCM

CIP (This Talk)

- fix the security issue in CHM and GCM
  - can be used even when MAC is short
- beyond the birthday bound security
- allows parallel computation
- Encryption part: CENC
- MAC part: Based on Inner Product Hash

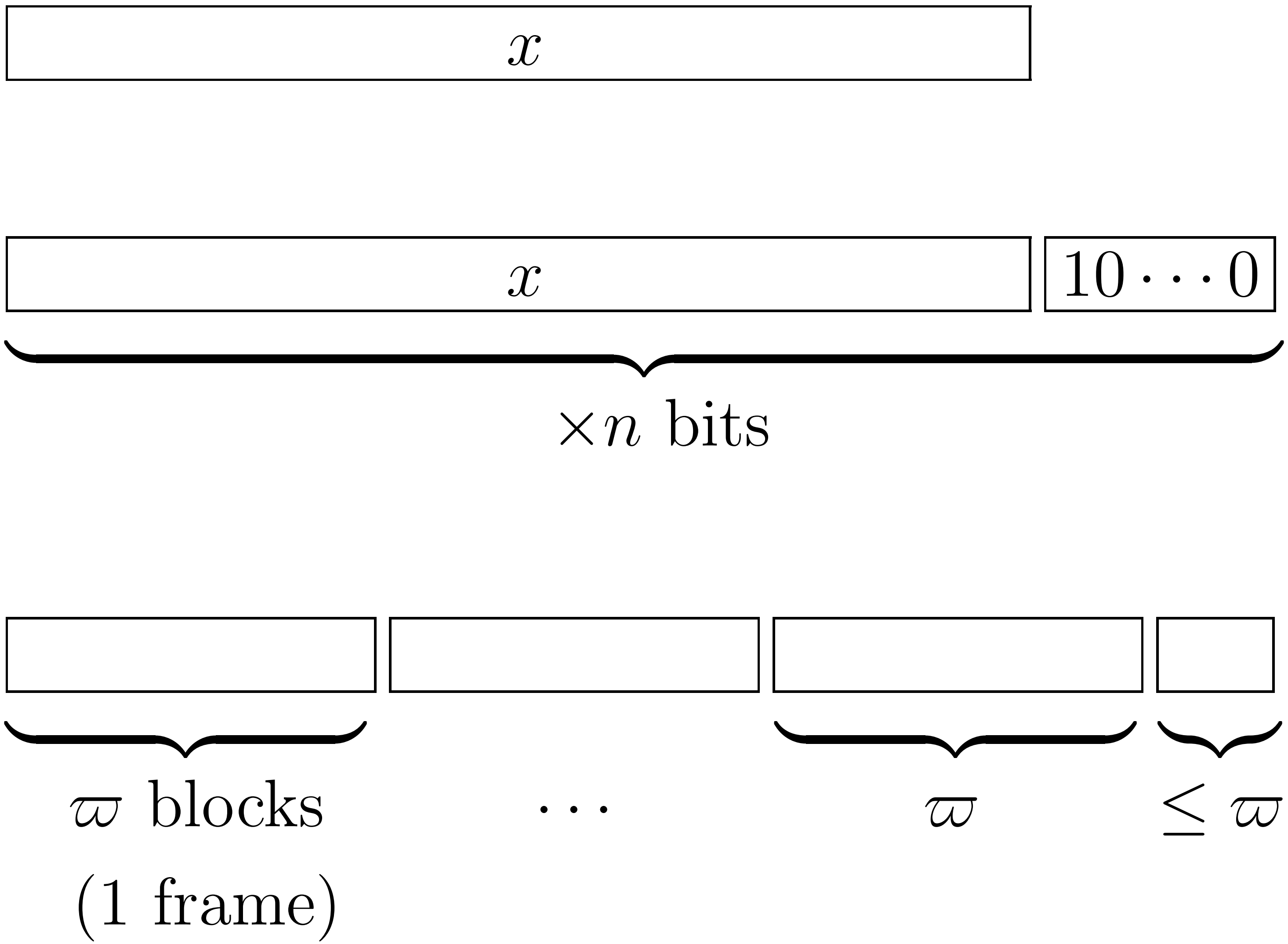
Inner Product Hash

- inputs: $x = (x_1, \ldots, x_t)$, key $k = (k_1, \ldots, k_t)$,
- output: $H_k(x) = (x_1, \ldots, x_t) \cdot (k_1, \ldots, k_t)$

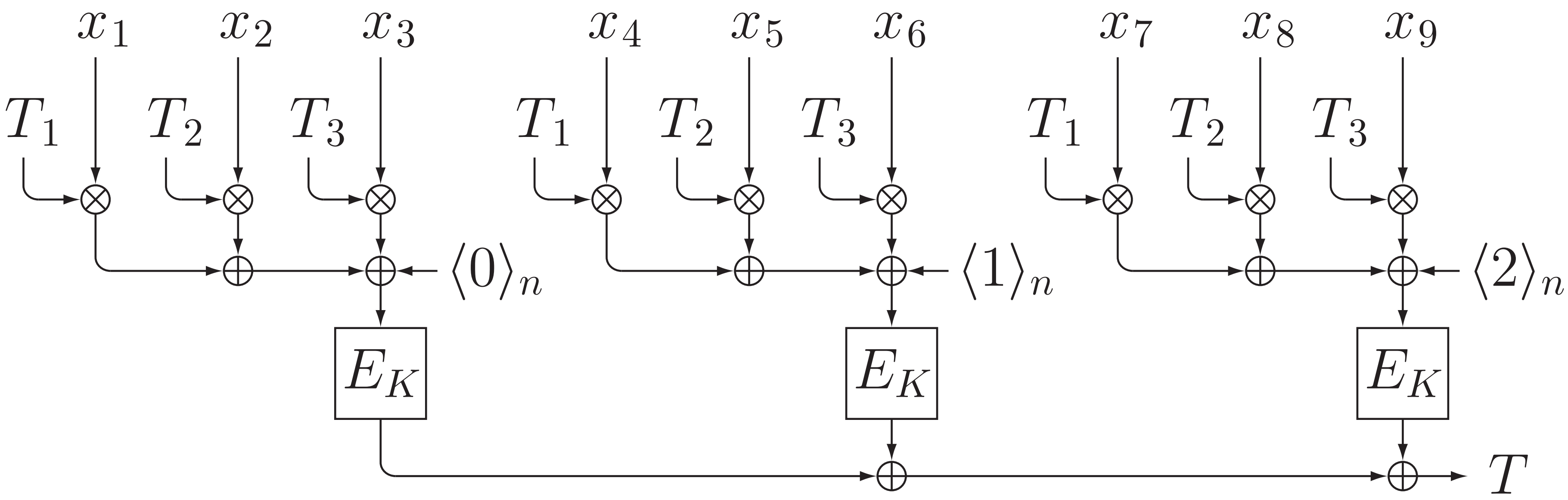
$$= x_1 \cdot k_1 \oplus \cdots \oplus x_t \cdot k_t$$

  multiplication over GF(2^n)
- fully parallelizable
- $|k|$ can be large, $|x| = |k|$
  - parse x intro a "frame," ($= \varpi$ blocks)
  - ϖ: frame width, small constant, default: $\varpi = 4$

Padding for Hash

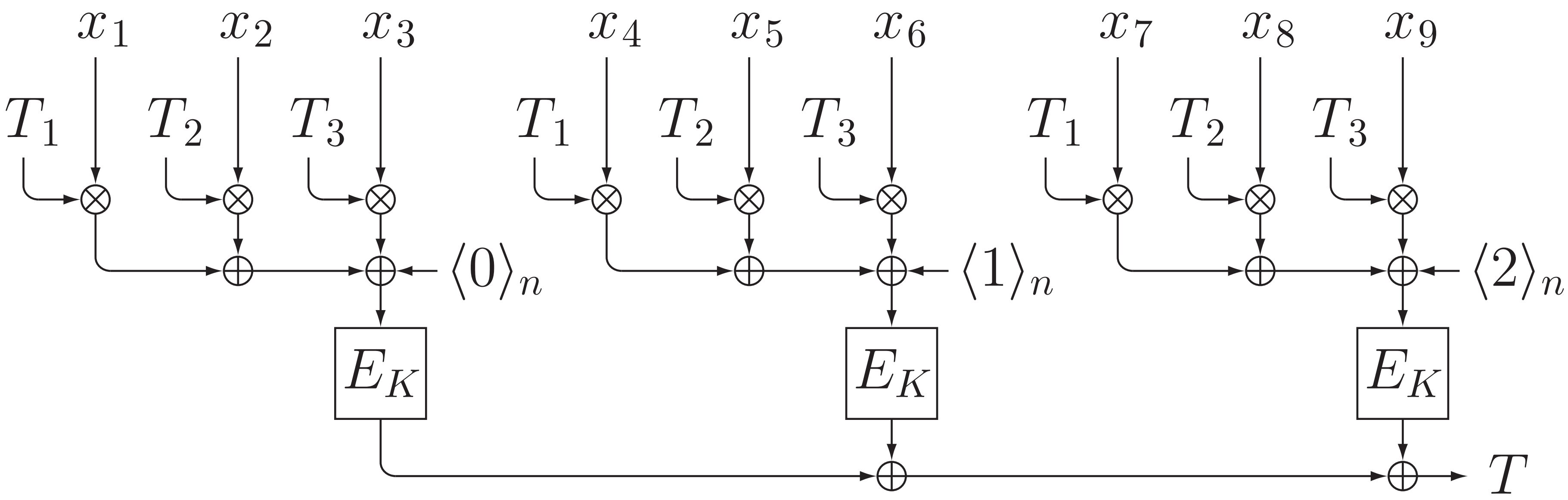


MAC Part of CIP



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

MAC Part of CIP



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

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

- H is ϵ-AXU if $\forall x, x'$ $(x \neq x')$ and $\forall y \in \{0,1\}^\tau$,

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

- **Proposition** $\forall x, x'$ $(x \neq x')$ and $\forall y \in \{0,1\}^\tau$,

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

  - x: ℓ frames, x': ℓ' frames, $\ell + \ell' - 1 \leq 2^{n-1}$
  - A makes at most $\ell + \ell'$ queries
- The only term that depends on τ is $2/2^\tau$
- It does not depend on the input length

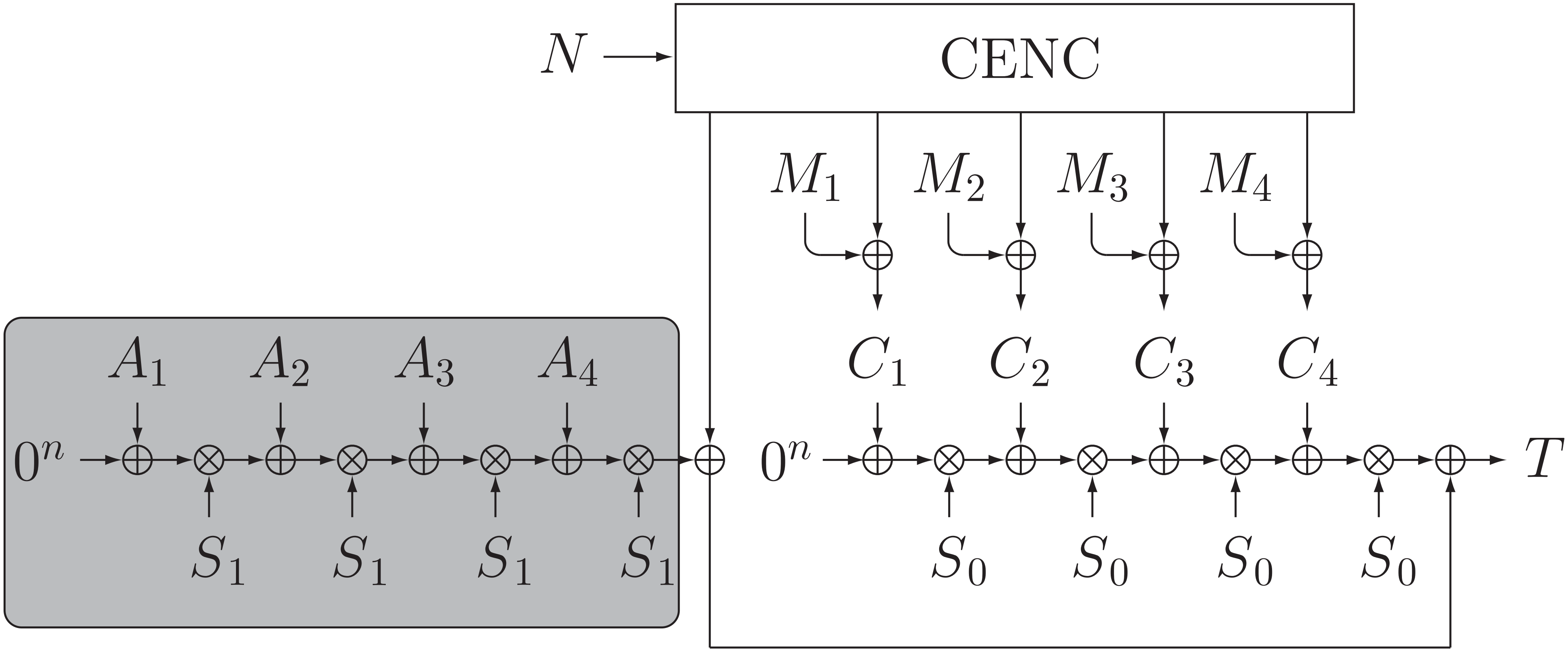
Encryption of CIP

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

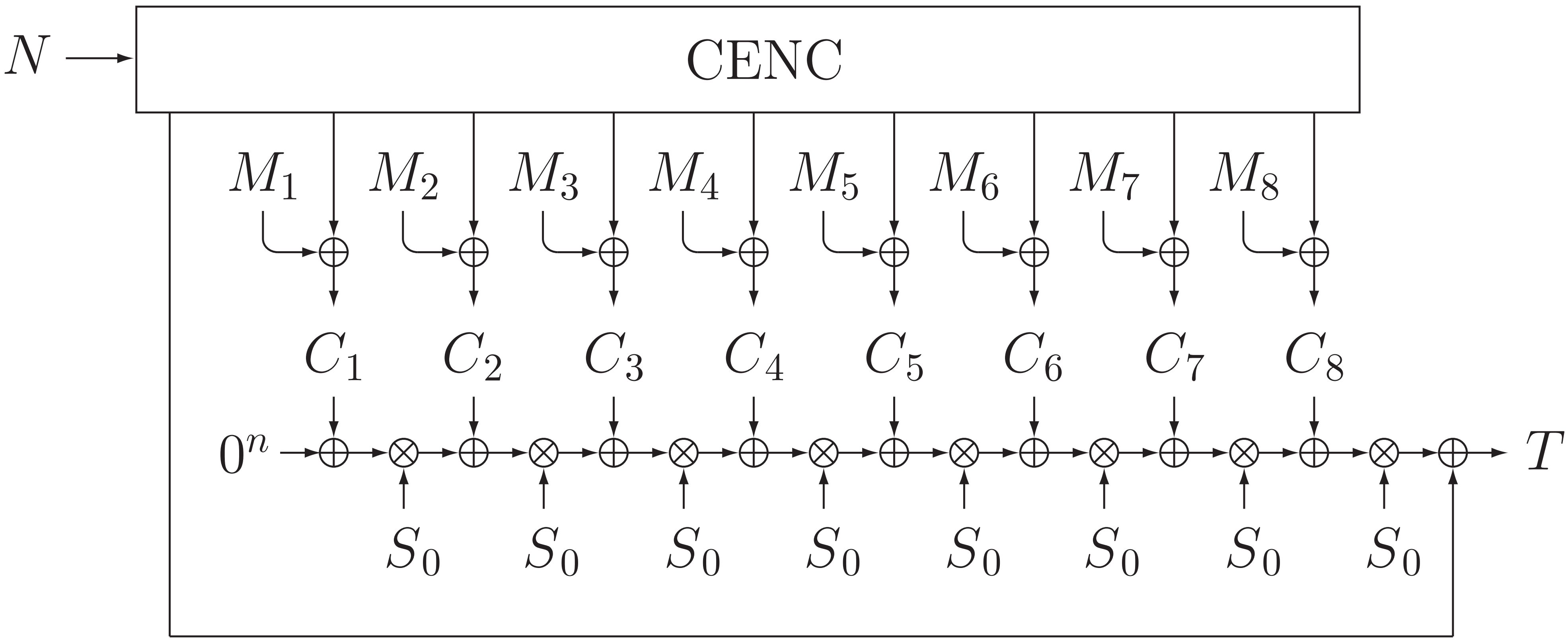
$$(K, N, M) \rightarrow \boxed{\text{CIP}} \rightarrow (C, T)$$

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

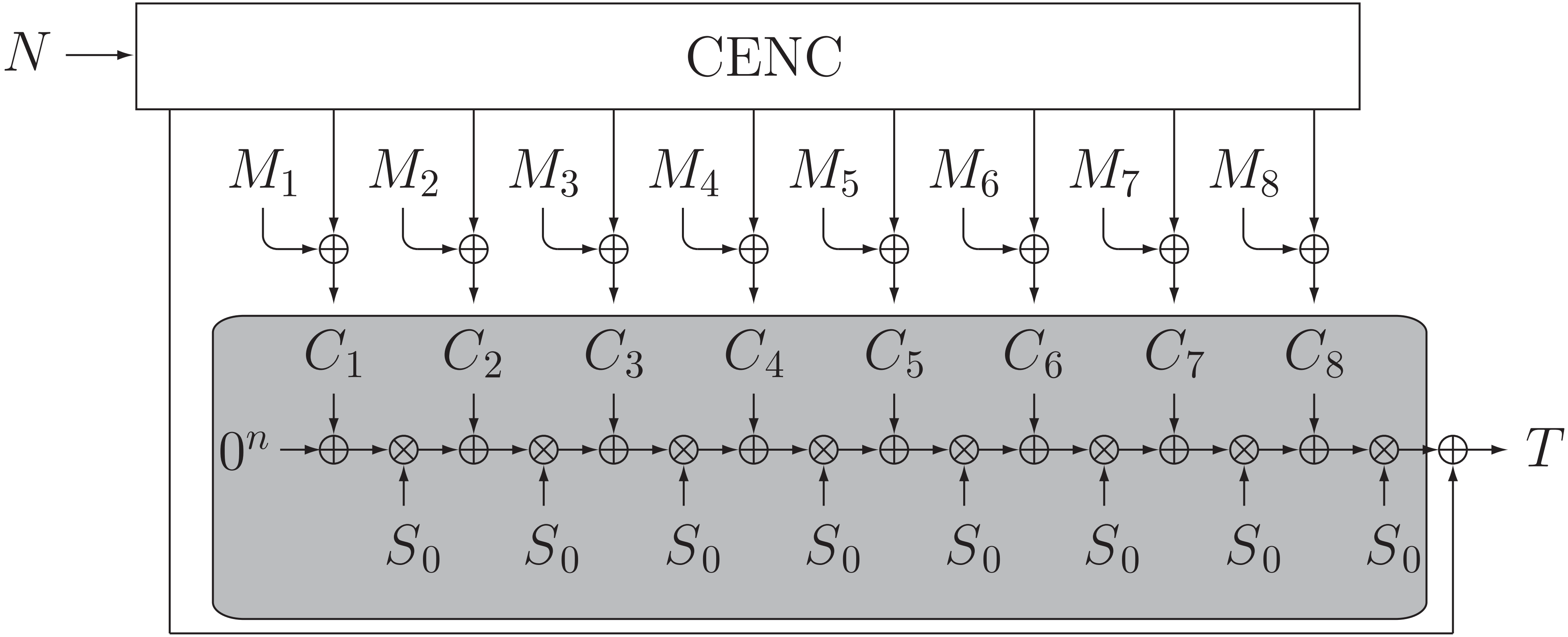
Encryption of CIP



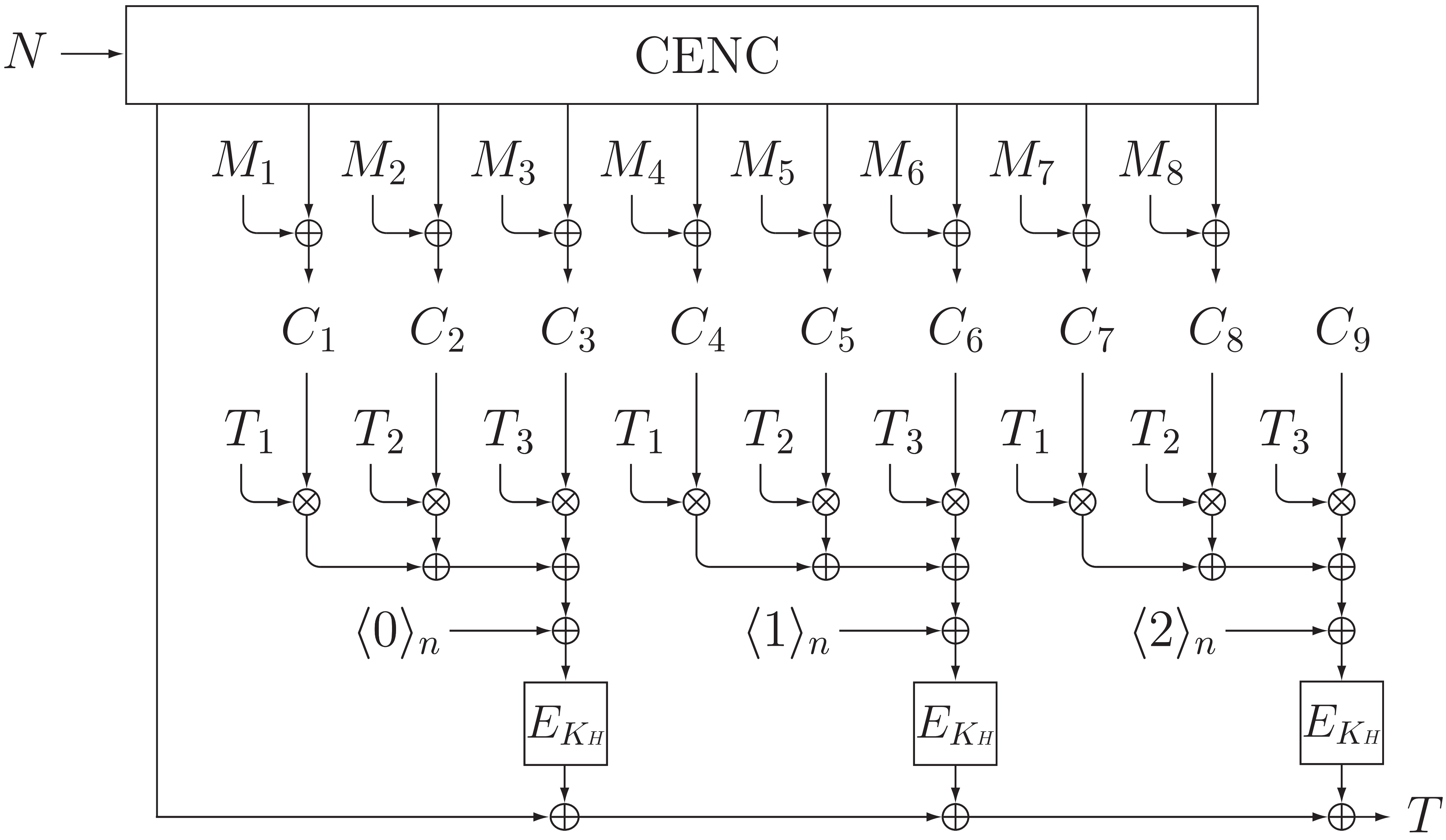
Encryption of CIP



Encryption of CIP



Encryption of CIP



Hash Key Derivation of CIP

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

Security Theorems of CIP

- privacy:
  - $\mathbf{Adv}^{\text{priv}}_{\text{CIP}}(A) \le \dfrac{wr^2\tilde{\sigma}^2}{2^{2n-4}} + \dfrac{w\tilde{\sigma}^3}{2^{2n-3}} + \dfrac{r^2}{2^{n+1}} + \dfrac{w\tilde{\sigma}}{2^n}$
  - follows from the security proof of CENC
- authenticity:
  - $\mathbf{Adv}^{\text{auth}}_{\text{CIP}}(A) \le \dfrac{wr^2\tilde{\sigma}^2}{2^{2n-4}} + \dfrac{w\tilde{\sigma}^3}{2^{2n-3}} + \dfrac{r^2}{2^{n+1}} + \dfrac{w\tilde{\sigma}}{2^n} + \dfrac{\sigma}{2^{n-1}} + \dfrac{2}{2^\tau} + \mathbf{Adv}^{\text{prp}}_{E}(D)$
  - follows from the result of CIP.Hash
- $r = \lceil k/n \rceil + 1$ (small const.), $\tilde{\sigma} = \sigma + q(w+1)$ $(\approx \sigma)$

Security Theorems of CIP (with AES)

- CIP can encrypt at most 2^{64} plaintexts
- max plaintext length is 2^{62} blocks (2^{36}GBytes)
- $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CIP}}(A) \leq \dfrac{\tilde{\sigma}^3}{2^{245}} + \dfrac{\tilde{\sigma}}{2^{119}}$
- $\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{CIP}}(A) \leq \dfrac{\hat{\sigma}^3}{2^{245}} + \dfrac{\hat{\sigma}}{2^{118}} + \dfrac{2}{2^{\tau}}$
- secure up to $\hat{\sigma} \ll 2^{81}$ blocks (2^{55}GBytes)
- The only term that depends on τ is $2/2^{\tau}$
- It does not depend on the message length
- CIP can be used even for short tag length.

Performance

- $m = \lceil |M|/n \rceil$ (block length of M)

	blockcipher calls	multiplications
GCM	m	m
CHM	$\frac{(w+1)m}{w}$	m
CIP	$\frac{(w+1)m}{w} + \frac{m}{\varpi}$	m

Performance

- $m = \lceil |M|/n \rceil$ (block size of M)

	blockcipher calls	multiplications
GCM	m	m
CHM	$\frac{257m}{256}$	m
CIP	$\frac{257m}{256} + \frac{m}{4}$	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: XOR MAC, RMAC, Poly1305, MACH,...
  - privacy and authenticity: Generic Composition, CHM, **CIP**

Conclusions

- beyond the birthday bound security
- introduce ϖ for a constant hash key length
- fix the security issue in CHM and GCM
  - can be used even when MAC is short

Future Work

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