New Blockcipher Modes of Operation with Beyond the Birthday Bound Security

Tetsu Iwata

Ibaraki University

March 17, 2006

Fast Software Encryption, FSE 2006, Graz, Austria, March 15–17, 2006

Blockcipher Modes

Algorithms that provide

- privacy (encryption mode)
- authenticity (MAC)
- privacy and authenticity (AE mode)
- $\cdots$

based on blockciphers.

Blockcipher Modes

Algorithms that provide

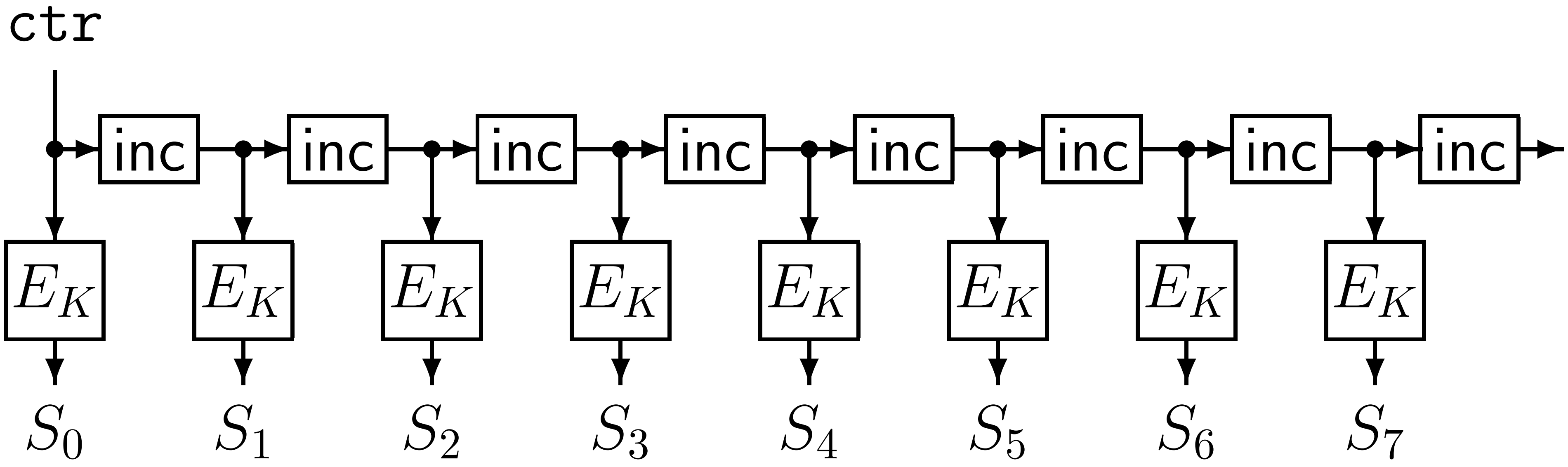
- ▷ privacy (encryption mode)
- • authenticity (MAC)
- ▷ privacy and authenticity (AE mode)
- • $\cdots$

based on blockciphers.

Known Encryption Modes

- ▷ CTR
- CBC
- OFB
- CFB
- ECB
- ...

CTR



- $S = (S_0, S_1, \ldots, S_7)$: keystream
- Encryption: $C = M \oplus S$
- Decryption: $M = C \oplus S$

Advantages of CTR

- provable security
- security proofs with the standard PRP assumption
- highly efficient
- single blockcipher key
- fully parallelizable
- allows precomputation of keystream
- allows random access

Security Definition

- "Indistinguishability from random strings"

  (Rogaway, Bellare, Black, Krovetz, '03)

- Scenario: Adaptive chosen plaintext attack

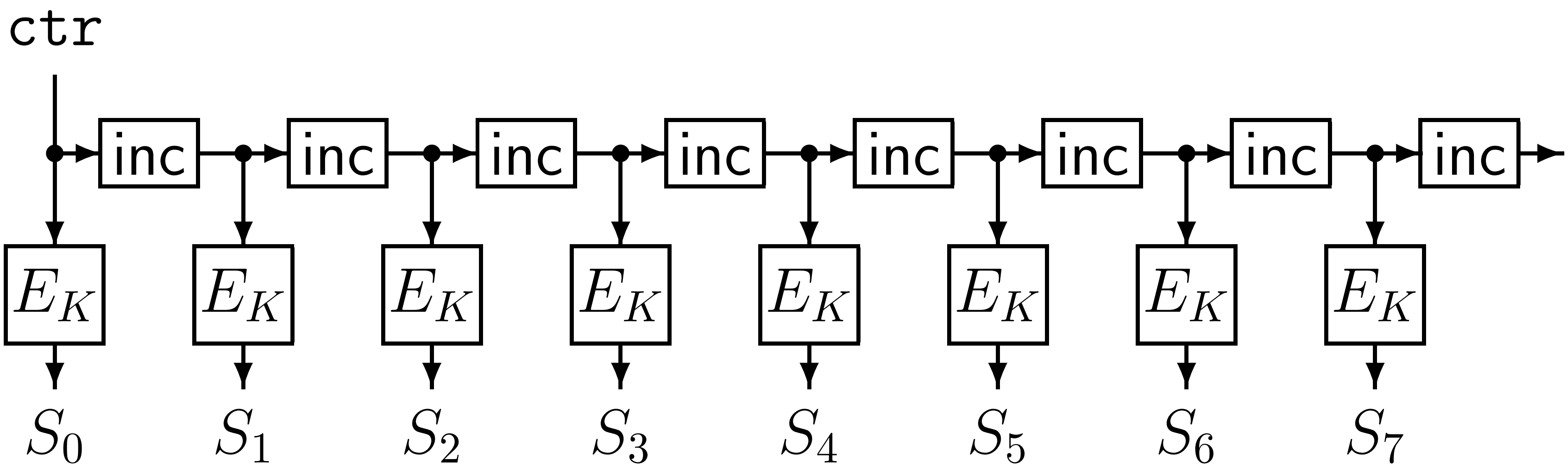
- Goal: To distinguish between

  – "real ciphertext"

  – "truly random string"

  (of the same length as ciphertext)

Keystream Generation Part of CTR



$S_i \neq S_j$ since $E_K(\cdot)$ is a permutation.

Keystream Generation Part of CTR

- If $S = (S_0, \ldots, S_{\sigma-1})$ is the keystream of CTR,

$$\Pr(S_i = S_j) = 0.$$

- If $S = (S_0, \ldots, S_{\sigma-1})$ is the truly random string,

$$\frac{0.3\sigma(\sigma - 1)}{2^n} \leq \Pr(S_i = S_j) \leq \frac{0.5\sigma(\sigma - 1)}{2^n}.$$

(n: length of S_i in bits, block size of E)

Keystream Generation Part of CTR

- For any A, $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CTR}}(A) \le \dfrac{0.5\sigma(\sigma-1)}{2^n}$.

Birthday Bound

- There exists A s.t. $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CTR}}(A) > \dfrac{0.3\sigma(\sigma-1)}{2^n}$.
  - ▷ A guesses "random string" if there is a collision.
  - ▷ Otherwise A guesses "ciphertext of CTR."

Security of CTR

CTR can **NOT** have beyond the birthday bound security (as long as $E_K(\cdot)$ is a permutation).

Our Work: New Encryption Mode

CENC $\cdots$ **C**ipher-based **ENC**ryption

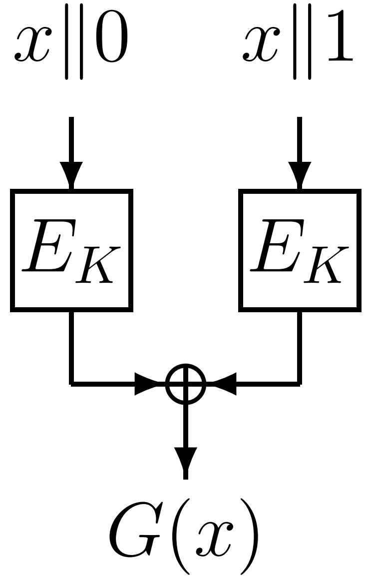
beyond the birthday bound security

without breaking advantages of CTR

The Basic Idea

- Convert $E_K(\cdot)$ into a function.
- $G_K(x) = E_K(x\|0) \oplus E_K(x\|1)$, $x \in \{0,1\}^{n-1}$

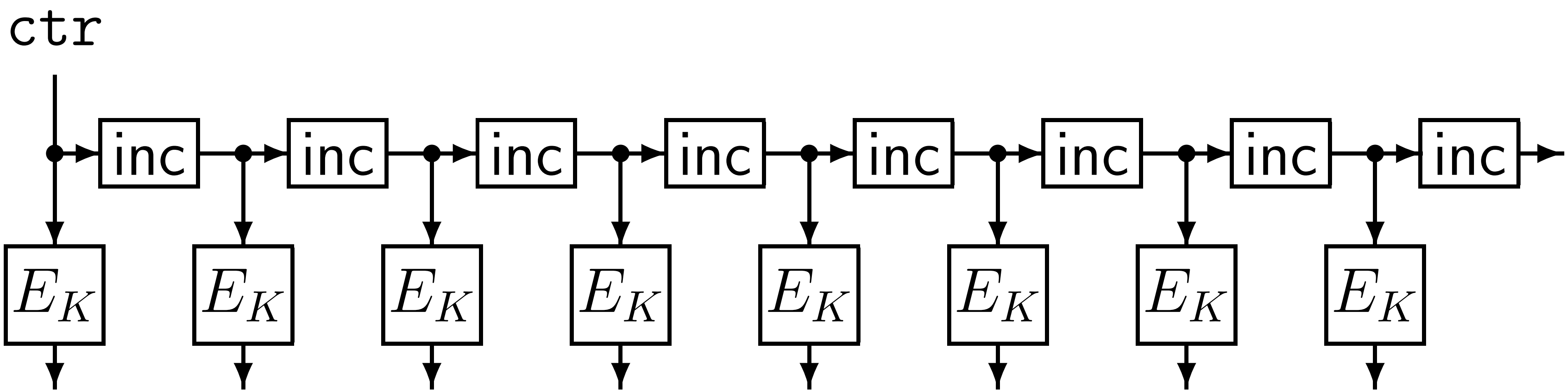
(Lucks '00, Bellare and Impagliazzo '99)



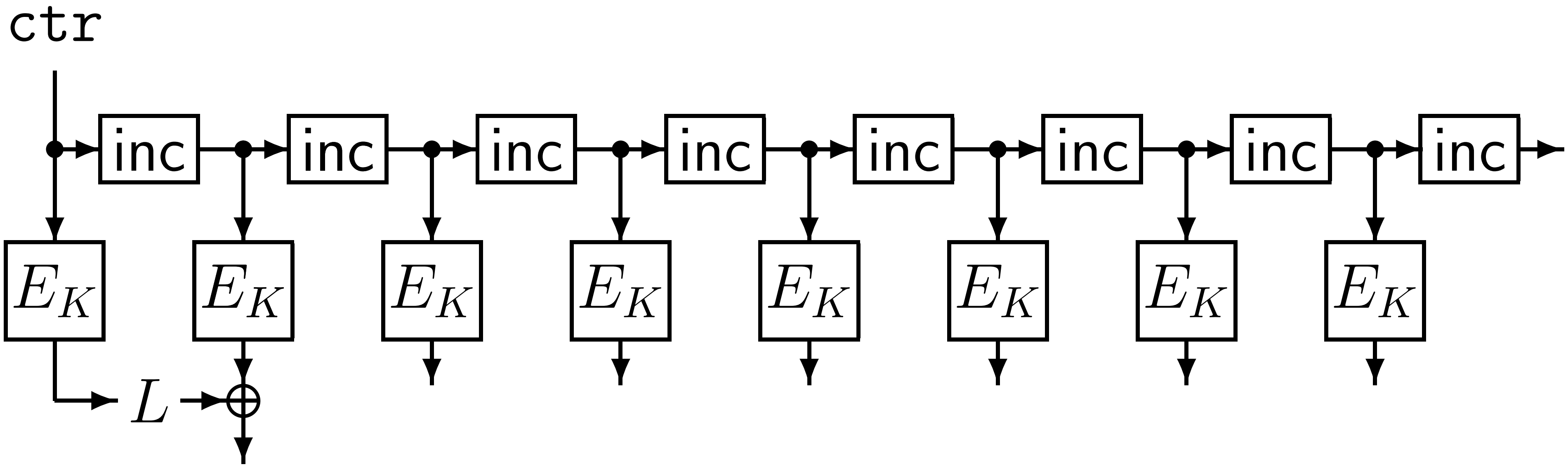
CENC Parameters

- Blockcipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$
- Nonce length: ℓ_{nonce} bits, $\ell_{\text{nonce}} < n$
- Frame width: w

Keystream Generation Part of CENC

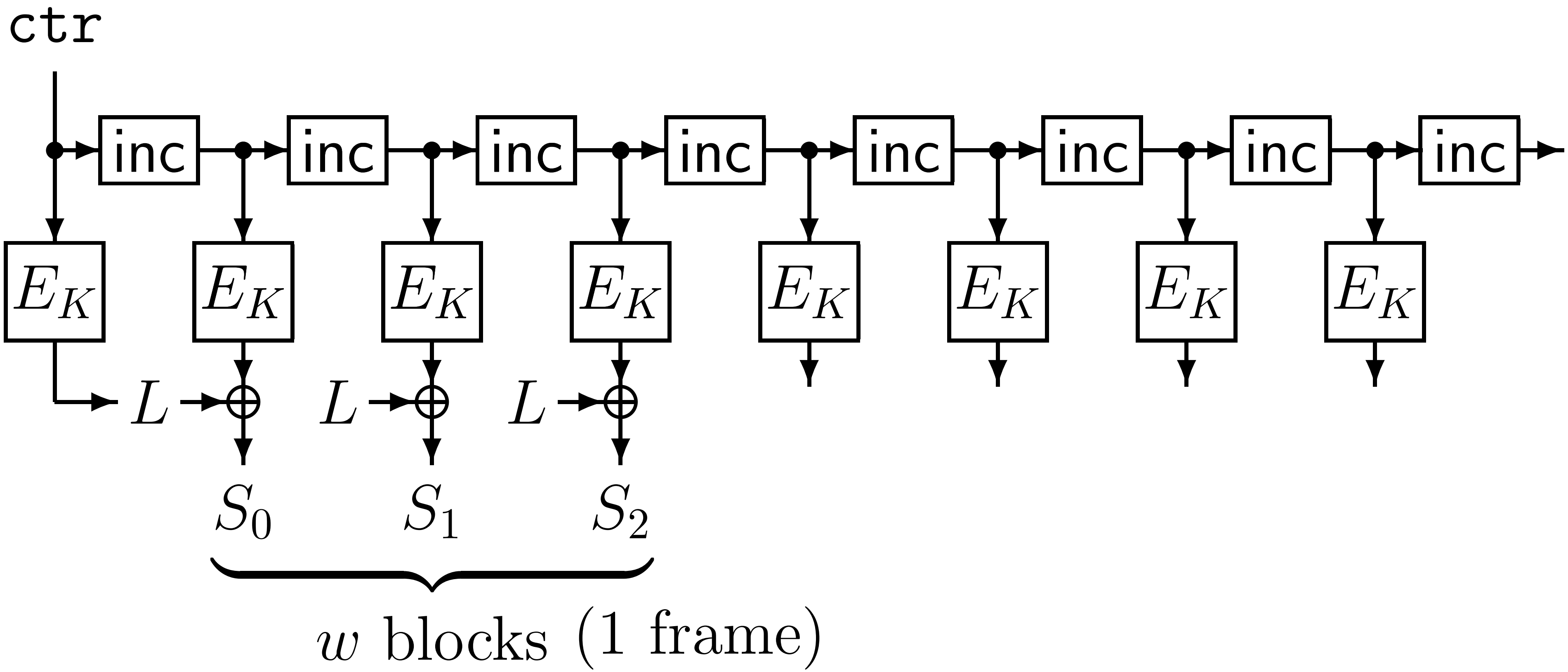


Keystream Generation Part of CENC



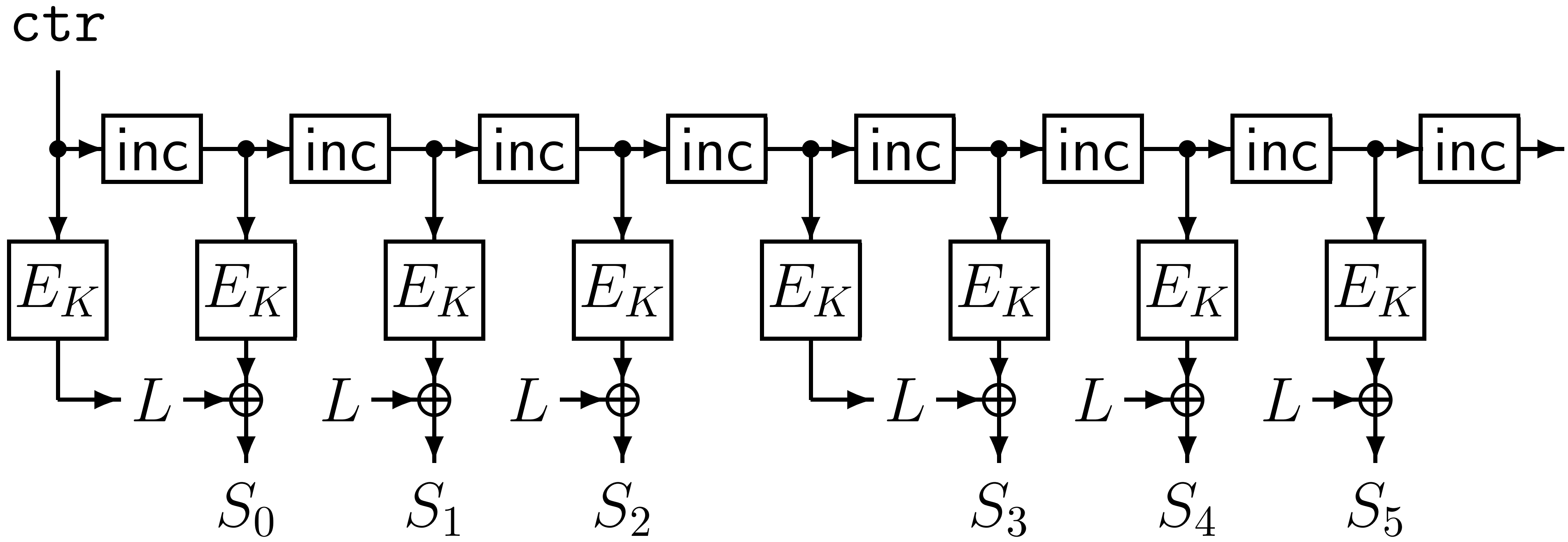
- L: mask

Keystream Generation Part of CENC

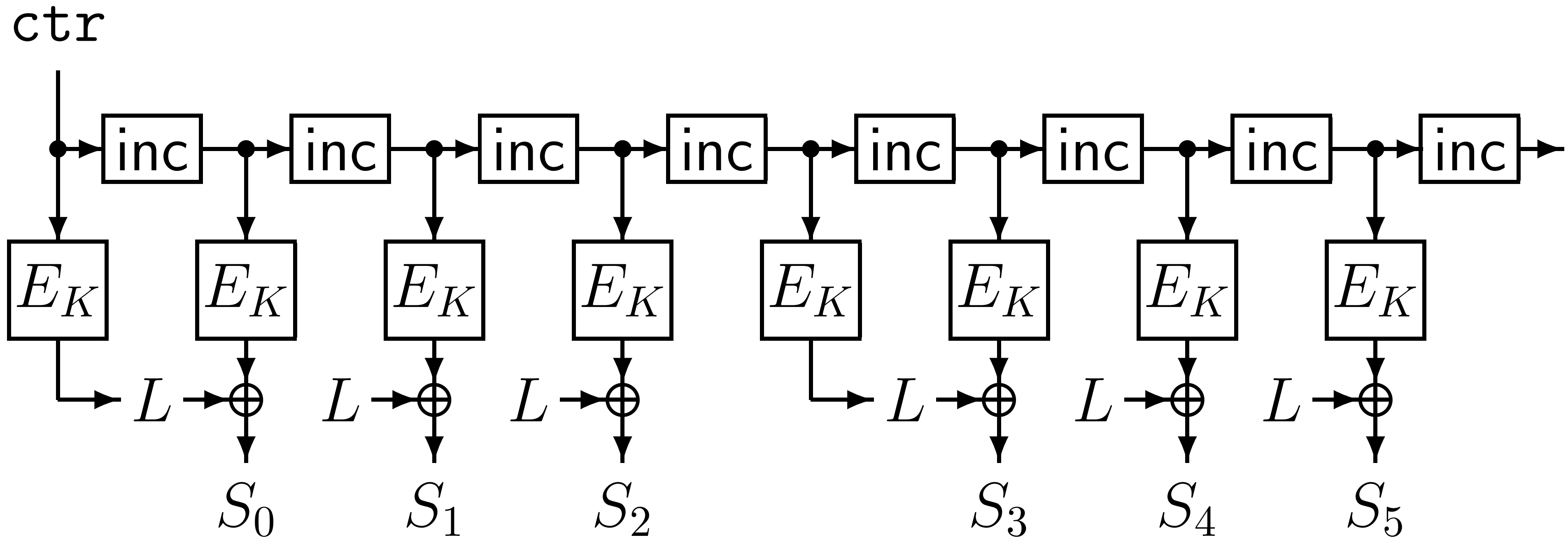


- w: frame width, default: $w = 2^8 = 256$

Keystream Generation Part of CENC

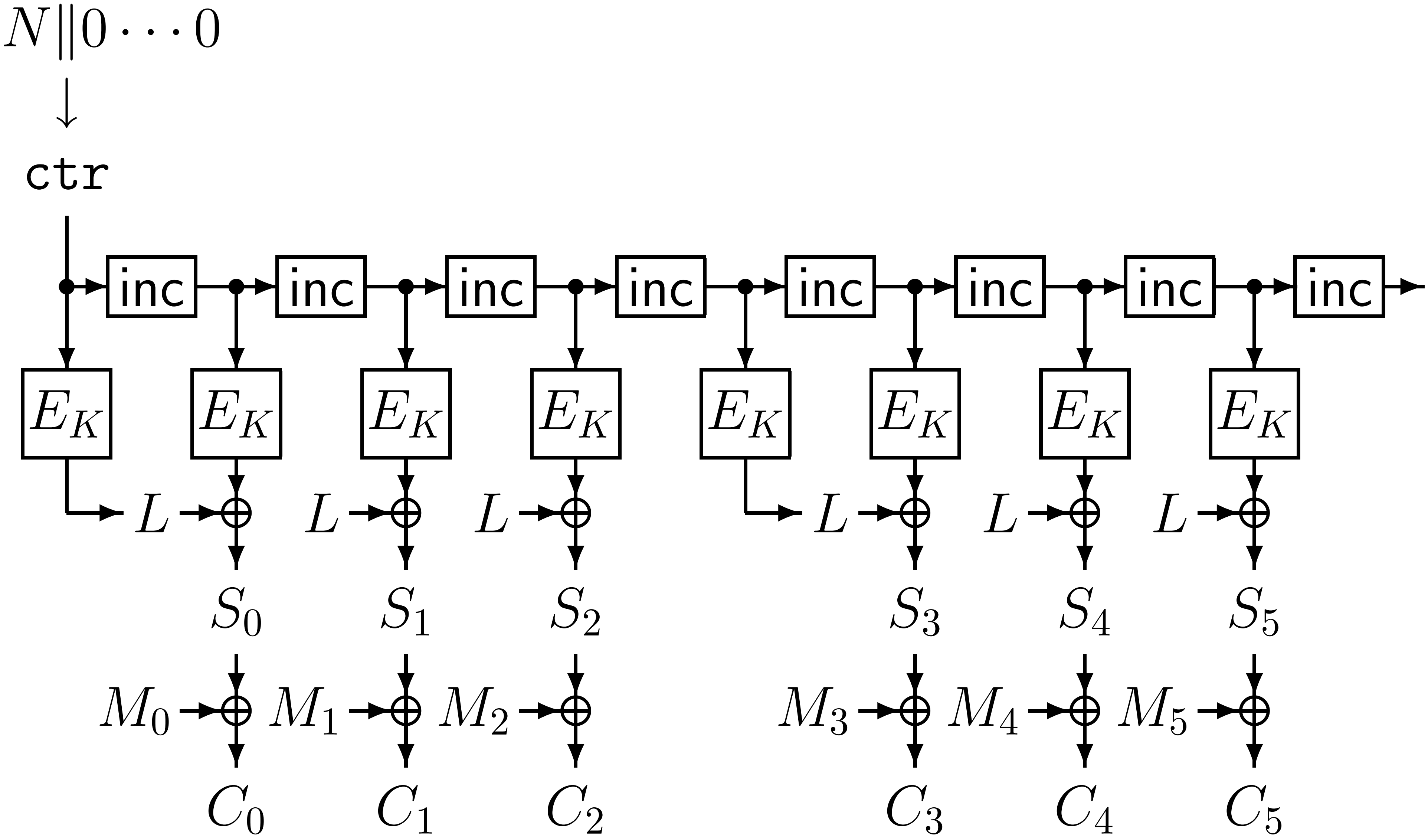


Keystream Generation Part of CENC



- N: Nonce, $\texttt{ctr} \leftarrow N \| 0 \cdots 0$
- default: $|N| = \ell_{\text{nonce}} = n/2$

Encryption Algorithm of CENC



Advantages of CENC

▷ provable security — beyond the birthday bound

• security proofs with the standard PRP assumption

▷ highly efficient — small cost

• single blockcipher key

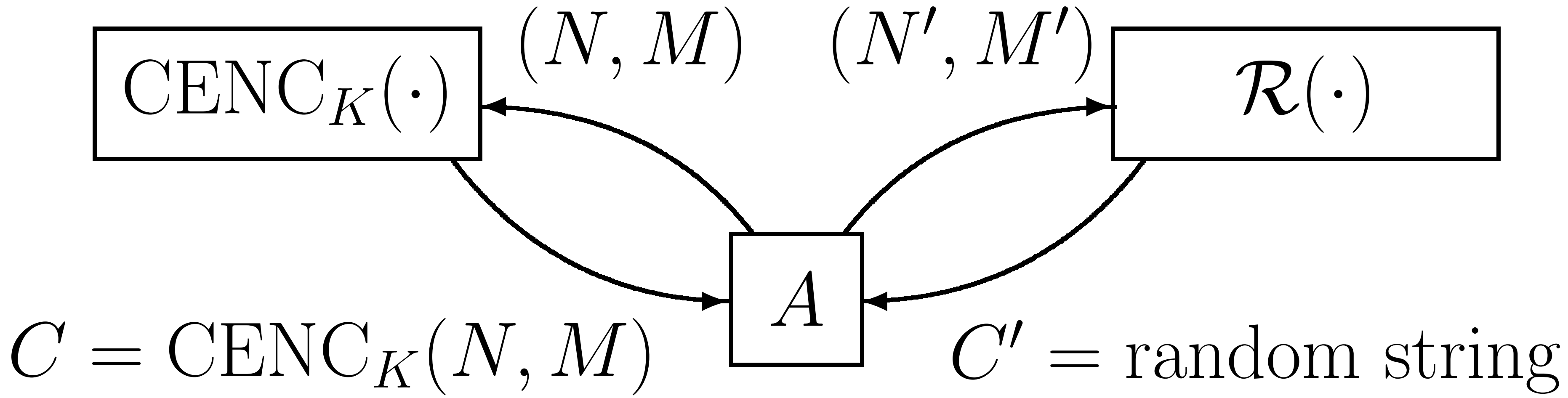
• fully parallelizable

• allows precomputation of keystream

• allows random access

Indistinguishability from Random Strings

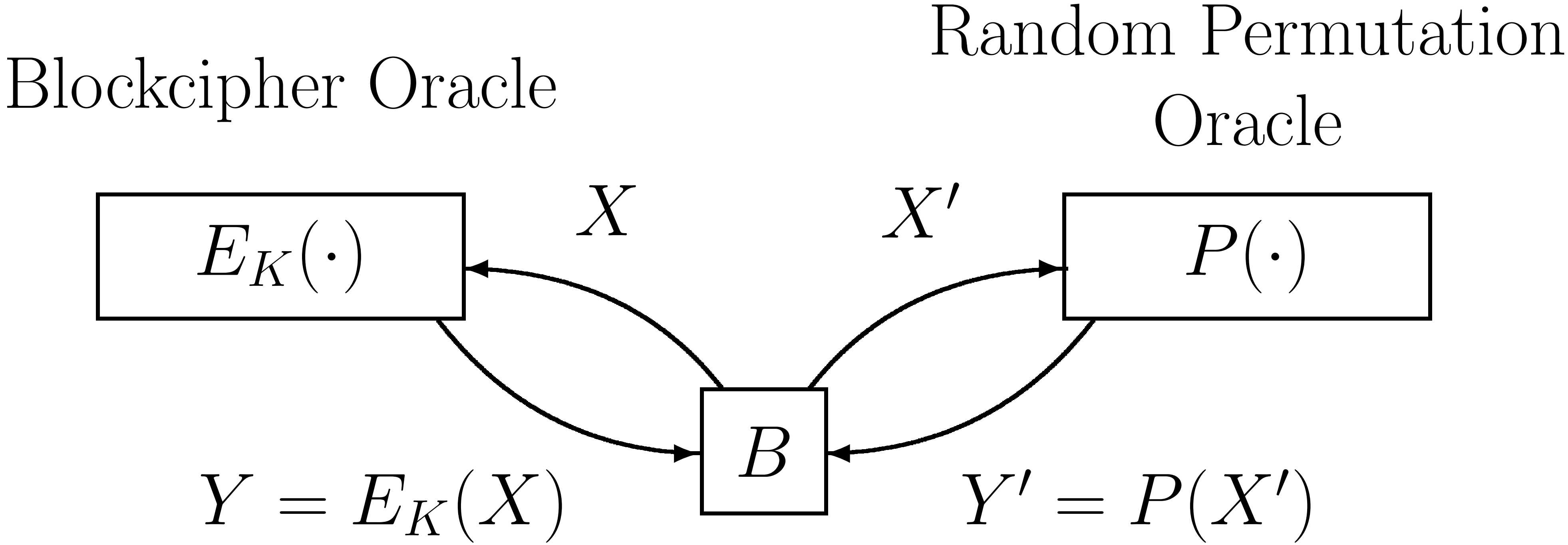
Encryption Oracle | Random String Oracle



A must not repeat 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 Definition for E (PRP, LR '88)



$$\mathbf{Adv}_E^{\mathrm{prp}}(B) \stackrel{\mathrm{def}}{=} \left| \Pr_K(B^{E_K(\cdot)} = 1) - \Pr_P(B^{P(\cdot)} = 1) \right|$$

Theorem. If there exists A against CENC such that:

- at most q queries, and
- at most σ blocks,

then there exists B against E such that:

- $\mathit{time}(B) = \mathit{time}(A) + O(n\hat{\sigma}w)$,
- at most $(w+1)\hat{\sigma}/w$ queries, and
- $\mathbf{Adv}_E^{\mathrm{prp}}(B) \geq \mathbf{Adv}_{\mathrm{CENC}}^{\mathrm{priv}}(A) - \dfrac{w\hat{\sigma}^3}{2^{2n-3}} - \dfrac{w\hat{\sigma}}{2^n}$,

where $\hat{\sigma} = \sigma + qw$.

Interpretation

- CENC is secure up to 2^{82} blocks (AES, $w = 2^8$).

▷ CTR is secure up to 2^{64} blocks.

If we encrypt $\sigma \le 2^{n/2}$ blocks,

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

▷ $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CTR}}(A) \le \dfrac{0.5\sigma^2}{2^n}$ (w: constant, $\hat{\sigma} \approx \sigma$)

Cost for the Security Improvement

$w + 1$ blockcipher calls for w blocks of keystream

- 257 calls to encrypt 256 blocks (Default: $w = 2^8$)
  - ▷ The cost is $1/257 = 0.4\%$ compared to CTR.
- 1 frame is w blocks, which is 4KBytes.
  - ▷ 99.9% of the Internet traffic is less than 1.5KBytes.
  - ▷ The cost is *one* blockcipher call compared to CTR.

New Authenticated-Encryption Mode

CHM $\cdots$ **C**ENC with **H**ash-based **M**AC

- CENC for privacy.
- Hash-based MAC (Wegman-Carter MAC) for authenticity.
- Beyond the birthday bound security.
- Similar to GCM by McGrew & Viega.

Open Question

▷ The security bound of CTR is tight.

- $\forall A$, $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CTR}}(A) \le 0.5\sigma(\sigma-1)/2^n$
- $\exists A$, $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CTR}}(A) > 0.3\sigma(\sigma-1)/2^n$

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

▷ Improve the security bound

▷ Attack with $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CENC}}(A) > \Omega(w\hat{\sigma}^3/2^{2n-3} + w\hat{\sigma}/2^n)$

Conjecture

The security bound can be improved.

$$\forall A,\ \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{CENC}}(A) \le O(w\hat{\sigma}/2^n)$$

Conclusion

- New encryption mode, CENC
- New AE mode, CHM
- beyond the birthday bound security

Questions?

Tetsu Iwata

iwata@cis.ibaraki.ac.jp