MITSUBISHI ELECTRIC
Changes for the Better

家庭から宇宙まで、エコチェンジ。

SAEB: A Lightweight Blockcipher-Based AEAD Mode of Operation

Authenticated Encryption with Associated Data

Yusuke Naito[1], Mitsuru Matsui[1],
Takeshi Sugawara[2], Daisuke Suzuki[1]

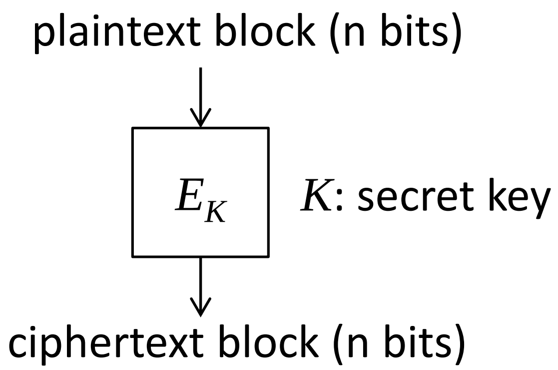
1. Mitsubishi Electric Corporation, Japan
2. The University of Electro-Communications, Japan

CHES 2018, September 11

Motivation

- Resource-constrained devices
  - such as RFID, sensor nodes, IoT devices, ...,
  - have access to insecure networks,
  - require lightweight cryptographic algorithms
    for secure communication & authentication.
- Lightweight blockciphers (fixed input length primitives) have actively designed, e.g.,
  - PRESENT (ISO/IEC 29192-2)
  - LED, Piccolo, TWINE, PRINCE, Midori, SKINNY, GIFT, ...
- We need not only a lightweight blockcipher
  - but also a lightweight mode of operation
    that offers a variable input length cryptographic primitive.

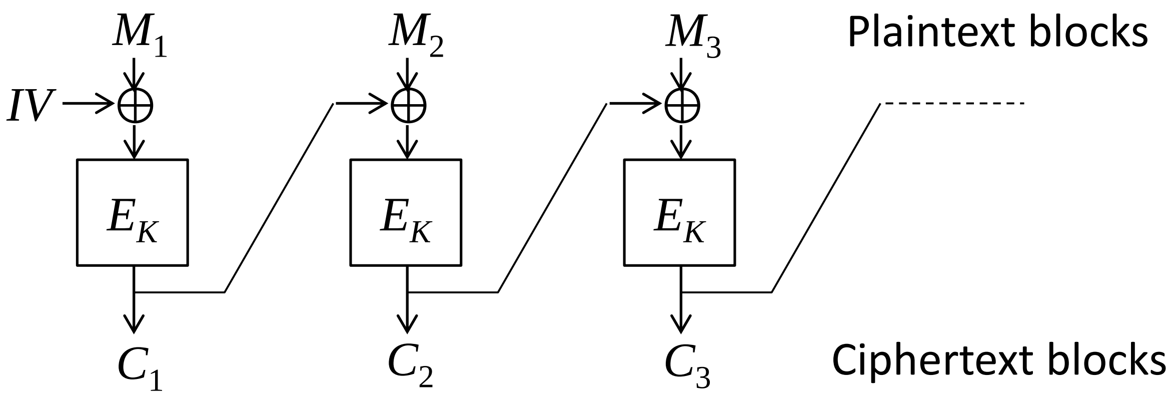
Blockcipher



- Family of permutations indexed by a key.
- A blockcipher key is randomly drawn.
- Security: Pseudo-Random Permutation.

Blockcipher-based Mode of Operation

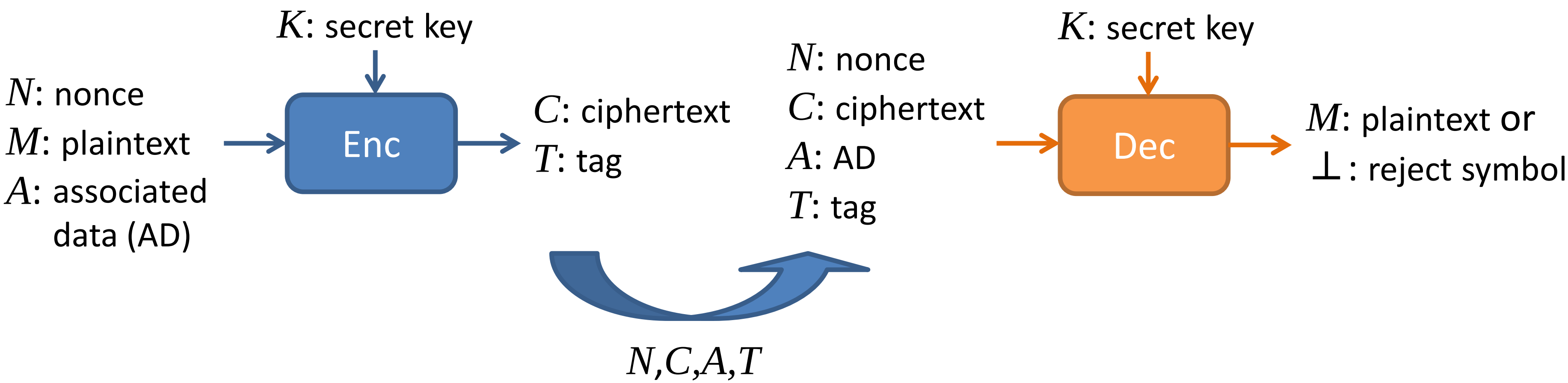
- A procedure to realize the desired algorithm, where a blockcipher is used as a component,
  - e.g., CBC encryption mode:



- Types of Mode of Operation
  - Authenticated Encryption with Associated Data (AEAD)
  - Encryption of Variable-Length Plaintexts
  - Message Authentication Code
  - Pseudorandom Function
  - ....

Blockcipher-based AEAD

- Blockcipher-based AEAD mode:
  - a procedure to ensures jointly privacy and authenticity.
- Nonce-based AEAD consists of encryption and decryption algorithms.



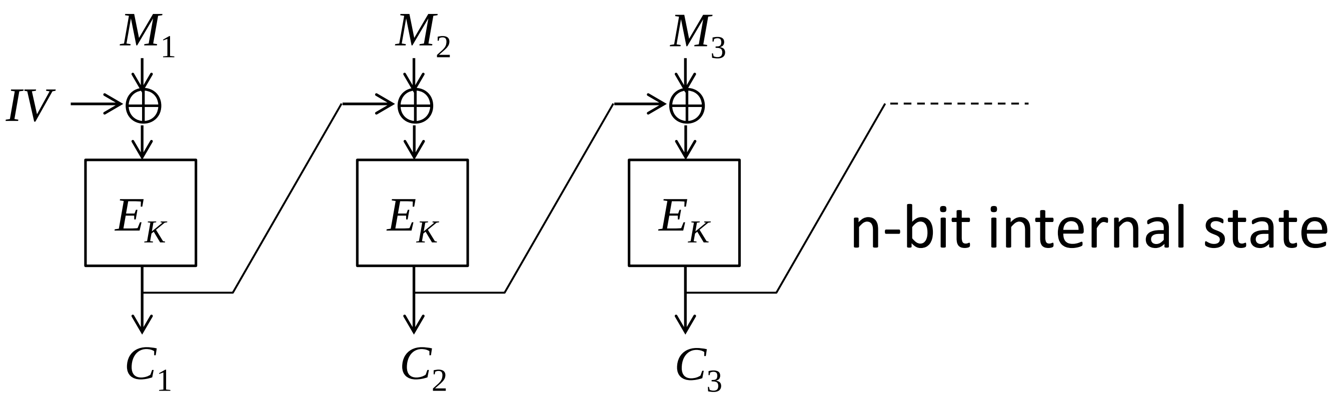
  - Nonce N is changed for every encryption.
  - Plaintext M is authenticated and encrypted.
  - AD A is authenticated but not encrypted.

Lightweight AEAD Mode of Operation

- "Lightweight" usually refers to a primitive that allows a compact implementation in a target platform.
  - Small program/RAM footprint in SW.
  - Compact circuit/resister area in HW.
- Blockcipher-based AEAD:
  - internal state, plain/ciphertext block -> RAM/resister.
  - blockcipher, mode of operation -> program/circuit.
- In order to design a lightweight blockcipher-based AEAD mode, we consider the following requirements.
  1. Minimum state size.
  2. Online.
  3. Inverse-free.
  4. XOR Only.

1. Minimum State Size

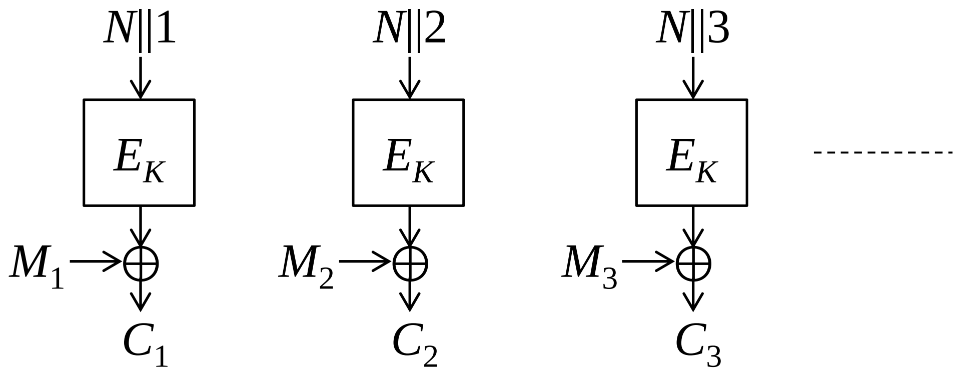
- A memory to keep an internal state is considered.
- E.g., CBC encryption mode requires an n-bit memory.



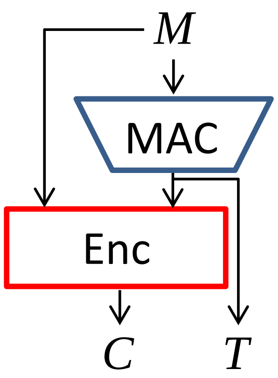
- A memory to keep an internal state impacts on RAM/resister sizes.
- The internal state size should be small as much as possible.
- Using an n-bit blockcipher, any AEAD mode requires at least n-bit memory.
- The minimum state size is n bits.

2. Online

- Two types of mode regarding memory to keep plaintext blocks.
  - Online: each plaintext block is processed only once
    - e.g., CTR mode.



  - Offline: all plaintext blocks are processed twice or more,
    - e.g., Deterministic AEAD: SIV, GCM-SIV.
    - require a memory to keep all plaintext blocks.



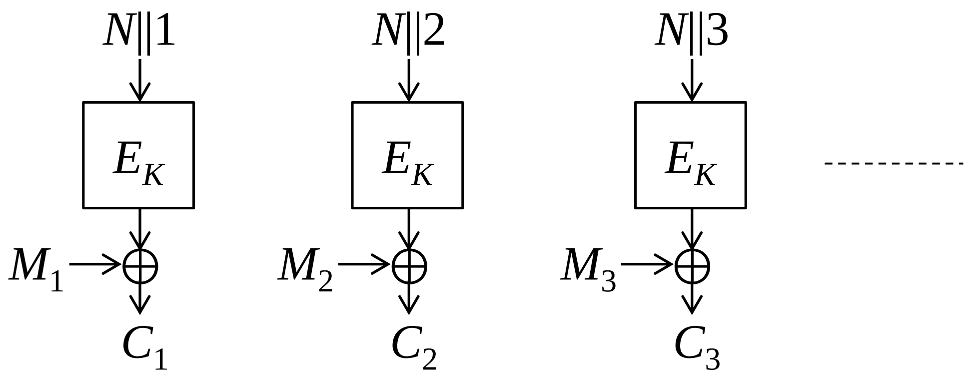
- A memory to keep plaintext bocks impacts on RAM/resister sizes.
- A lightweight AEAD mode should be online.

3. Inverse-free

- Two types of mode regarding blockcipher implementation:
  - both forward E_K and inverse E_K^{-1} are used, e.g., OCB1,2,3,
  - only forward E_K is used, e.g., OTR, COFB,...
- The latter (inverse-free) modes do not require the inverse E_K^{-1},
  ⇒ more compact than the former modes for program/circuit.
- An implementation size of a blockcipher impacts on program/circuit sizes.
- A lightweight mode should be inverse-free.

4. XOR Only

- A mode consists of only XOR operations except for a blockcipher.
- An XOR operation is essential for encrypting a plaintext block,
  - e.g., CTR mode.



- An implementation size from a mode impacts on program/circuit sizes.
- A lightweight mode should be XOR only.

Open Problem

- Previous AEAD modes do not satisfy some of the four requirements.

	Minimum State Size	Inverse Free	Online	XOR Only
GCM	— (4n bits)	✓	✓	—
OCB	— (3n bits)	—	✓	—
OTR	— (4n bits)	✓	✓	✓
CLOC	— (2n bits)	✓	✓	✓
JAMBU	— (1.5n bits)	✓	✓	—
COFB	— (1.5n bits)	✓	✓	✓

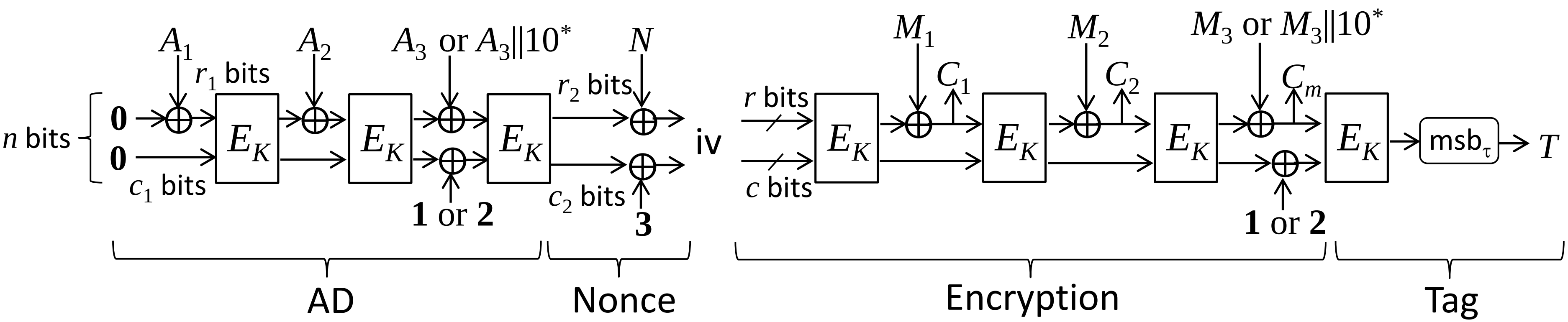
- Open problem: design a blockcipher-based AEAD mode with the four requirements.

Efficient Handling of Static AD

- In addition to the four requirements for lightweight AEAD modes, efficient handling of static AD is an important requirement.
- Static AD:
  - the same AD is used for every encryption procedure, e.g., packet header.
- Efficient handling of static AD:
  - if AD is not changed, so is the result of handling AD, i.e., the procedure can be skipped.
- Important AEAD modes were designed so that this requirement is satisfied,
  - e.g., GCM, OCB, OTR, …

Our Result

- Design a blockcipher-based AEAD mode, SAEB
  - based on the sponge-style design methodology.

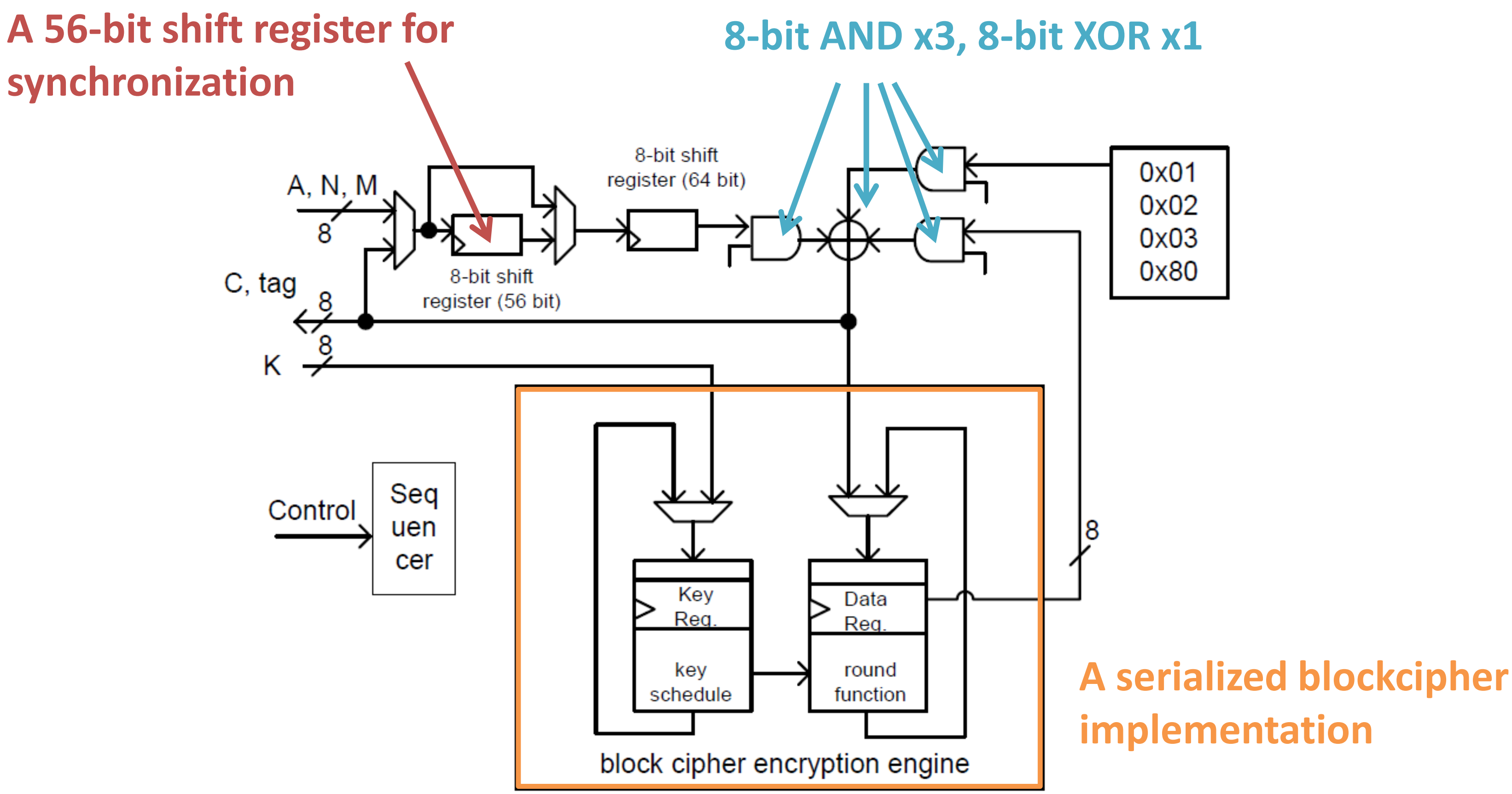


- Security: security up to $O(2^{n/2})$ query complexity when c=n/2 i.e., birthday-bound security.
- Five Requirements:

	Minimum State Size	Online	XOR Only	Inverse Free	Efficient Handling Static AD
SAEB	✓ (n bits)	✓	✓	✓	✓

Hardware Implementation

- The extra cost from the SAEB mode is very small.



HW/SW Performances

Circuit area in hardware implementations

ASIC impl. on NanGate 45-nm CMOS

	Area [GE]
AES	2679
mode	**823**
Total	3502

FPGA impl. on Xilinx Virtex-7

	#LUTs	#FFs
AES	304	218
mode	**44**	**24**
Total	348	242

Software costs

Renesas 16-bit microcontroller RL78

	ROM	RAM
AES	926	20
mode	**200**	**26**
Total	1126	46

Hardware Performance Comparisons

Table 5: Performance of SAEB in ASIC.

	Standard Cell Library	Target	Circuit Area [GE]	Max. Freq. [MHz]	Latency [Cycles]
[BBM16]	*STMicroelectronics* 90-nm CMOS	CLOC	4,310	—	—
		SILC	4,220	—	—
		AES-OTR	6,770	—	—
This work	*NanGate* 45-nm CMOS	SAEB	3,502	122.0	231
		• AES	2,679	126.4	231
		• diff	823	—	—

Table 6: Performance of SAEB in FPGA.

	Platform	Target	Look-up Table [LUTs/ALMs]	Flip-flop [FFs]	Max. Freq. [MHz]	Latency [Cycles]
[CIMN17]	*Xilinx Virtex-7* xc7vx330t	COFB	1,456	722	264.2	—
[GMU]	*Xilinx Virtex-7* xc7vx485t ffg1761-3	ACORN	566	—	466.0	—
		JAMBU	1,051	—	491.0	—
		ASCON	1,557	—	444.0	—
This work	*Xilinx Virtex-7* xc7vx330t ffg1157-1	SAEB	348	242	145.9	231
		• AES	304	218	144.2	231
		• diff	44	24	—	—

Conclusion

- Define the five requirements for lightweight AEAD modes
  - Minimum State Size, XOR Only, Inverse-free, Online, Efficient handling of static AD.
- Previous blockcipher-based AEAD modes do not satisfy some of the five requirements.
- Present SAEB
  - lightweight blockcipher-based AEAD mode,
  - achieves birthday bound security when c=n/2,
  - satisfies the five requirements,
  - offers compact HW/SW implementations.

Thank you for your attention!

Changes for the Better

Software Performance Comparison

Table 4: Performance comparison with existing AEAD schemes.

	Mode of operation	Underlying blockcipher	ROM bytes	RAM bytes	Cycles/byte for x-byte data					
					16	32	64	128	256	∞
[IMGM14]	CLOC	AES	2980	362	875	612	480	414	381	-
[IMGM14]	OCB-E	AES	5010	971	1527	891	573	414	334	-
[IMGM14]	OCB-D	AES	5010	971	1562	928	611	453	374	-
This work	SAEB	AES_fast	1126	46	1166	813	626	538	493	449

Mode: 200 byte
AES: 926 byte

- CLOC, OCB are implemented on ATmega128.
- SAEB is implemented on RL78.

	ROM	RAM
AES	926	20
mode	200	26
Total	1126	46

Security Bound

- nAE-Security: Ind. between SAEB and an ideal AE ($,⊥)
- For any adversary A and free parameter ρ,

$$\mathrm{Adv}^{\mathrm{nAE}}_{\mathrm{SAEB}}(\mathrm{A}) \leq \frac{2\sigma^2}{2^n} + \frac{(\rho-1)(\sigma_A+\sigma_D)}{2^c} + 2^r\left(\frac{e\sigma_\varepsilon}{\rho 2^r}\right)^\rho + \frac{q_D}{2^\tau}$$

where σ is # of blockcipher calls by all queries,
$\sigma_\varepsilon, \sigma_D$ are # of blockcipher calls by all enc., dec. queries,
σ_A is # of blockcipher calls hangling AD by all enc. queries.

- Putting c=r=n/2, ρ=n/2, τ=n/2, the bound becomes

$$\mathrm{Adv}^{\mathrm{nAE}}_{\mathrm{SAEB}}(\mathrm{A}) \leq \frac{2\sigma^2}{2^n} + \frac{n(\sigma_A+\sigma_D)}{2^{\frac{n}{2}+1}} + \left(\frac{4e}{n}\cdot\frac{\sigma_\varepsilon}{2^{n/2}}\right)^{n/2}$$

If $\sigma_A + \sigma_D$ << $2^{n/2}$, SAEB is secure AEAD up to $O(2^{n/2})$ query complexity.

Comparison for the Five Requirements

	Minimum State Size	Inverse Free	XOR Only	Online	Efficient Handling Static AD	Security
GCM	— (4n bits)	✓	—	✓	✓	Birthday Security
OCB	— (3n bits)	—	—	✓	✓	Birthday Security
OTR	— (4n bits)	✓	✓	✓	✓	Birthday Security
CLOC	— (2n bits)	✓	✓	✓	✓	Birthday Security
JAMBU	— (1.5n bits)	✓	—	✓	—	—
COFB	— (1.5n bits)	✓	✓	✓	—	Birthday Security
SAEB	✓ (n bits)	✓	✓	✓	✓	Birthday Security