XOCB: Beyond-Birthday-Bound Secure Authenticated Encryption Mode with Rate-One Computation

Zhenzhen Bao[1,4], **Seongha Hwang[2]**, Akiko Inoue[3], Byeonghak Lee[2], Jooyoung Lee[2], and Kazuhiko Minematsu[3]

[1]Institute for Network Sciences and Cyberspace, BNRist, Tsinghua University, Beijing, China

[2]KAIST, Daejeon, Korea

[3]NEC, Kawasaki, Japan

[4]Zhongguancun Laboratory, Beijing, China

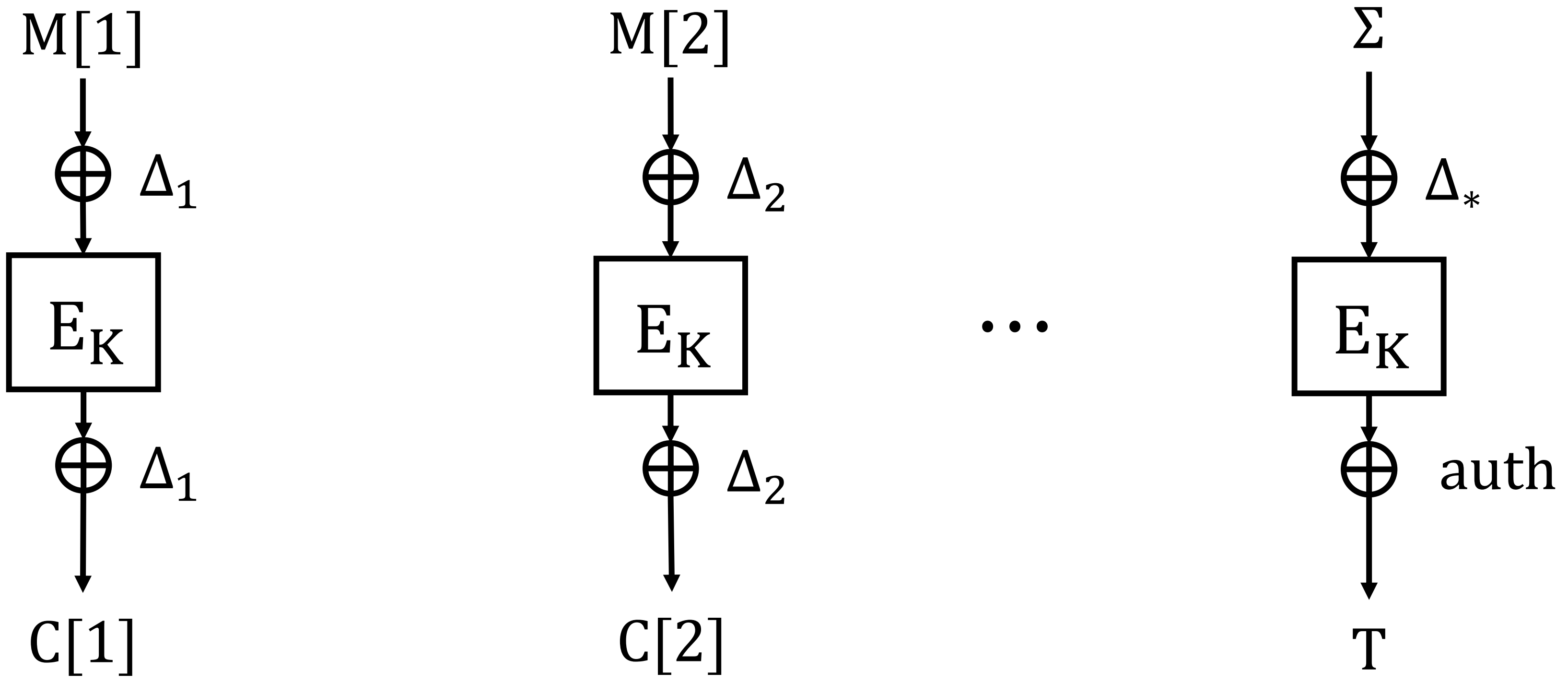
Eurocrypt 2023

Overview

- We present **XOCB**, a new block cipher mode of operation for nonce-based authenticated encryption.
- XOCB has the following features:
    1. **mostly follows the structure of OCB,**
    2. **has beyond-birthday-bound security,**
    3. **is parallelizable with rate-1 computation.**

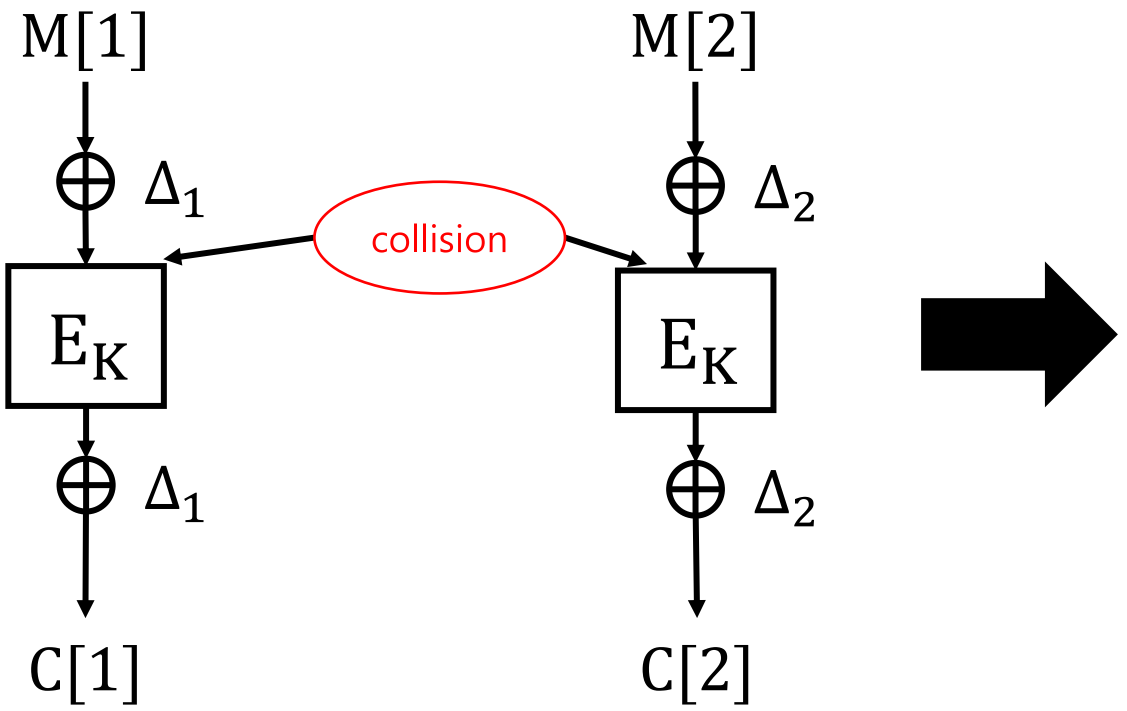
OCB mode

- OCB3 (Offset CodeBook)



OCB mode

- OCB3 (Offset CodeBook) : Δ_i is the masking generated from the scheme - all the maskings are distinct.



$$M[1] \oplus M[2] = C[1] \oplus C[2]$$

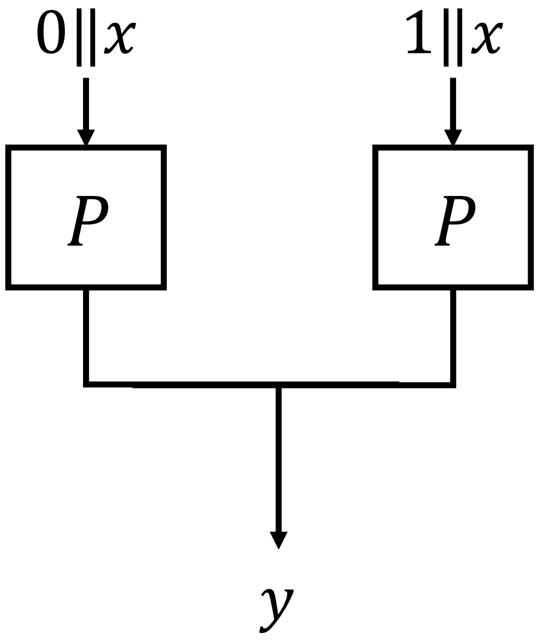
Distinguish Attack!

Beyond-Birthday-Bound Security Requirement

- The security of OCB is up to the birthday bound.
- The computational power and the amount of data have been increased recently.
- In particular, exabyte (10^{18}) data is already in use and zettabyte (10^{21}) is in near future.
- Therefore, a higher level of security is desirable.

Design Principle to Enhance Security

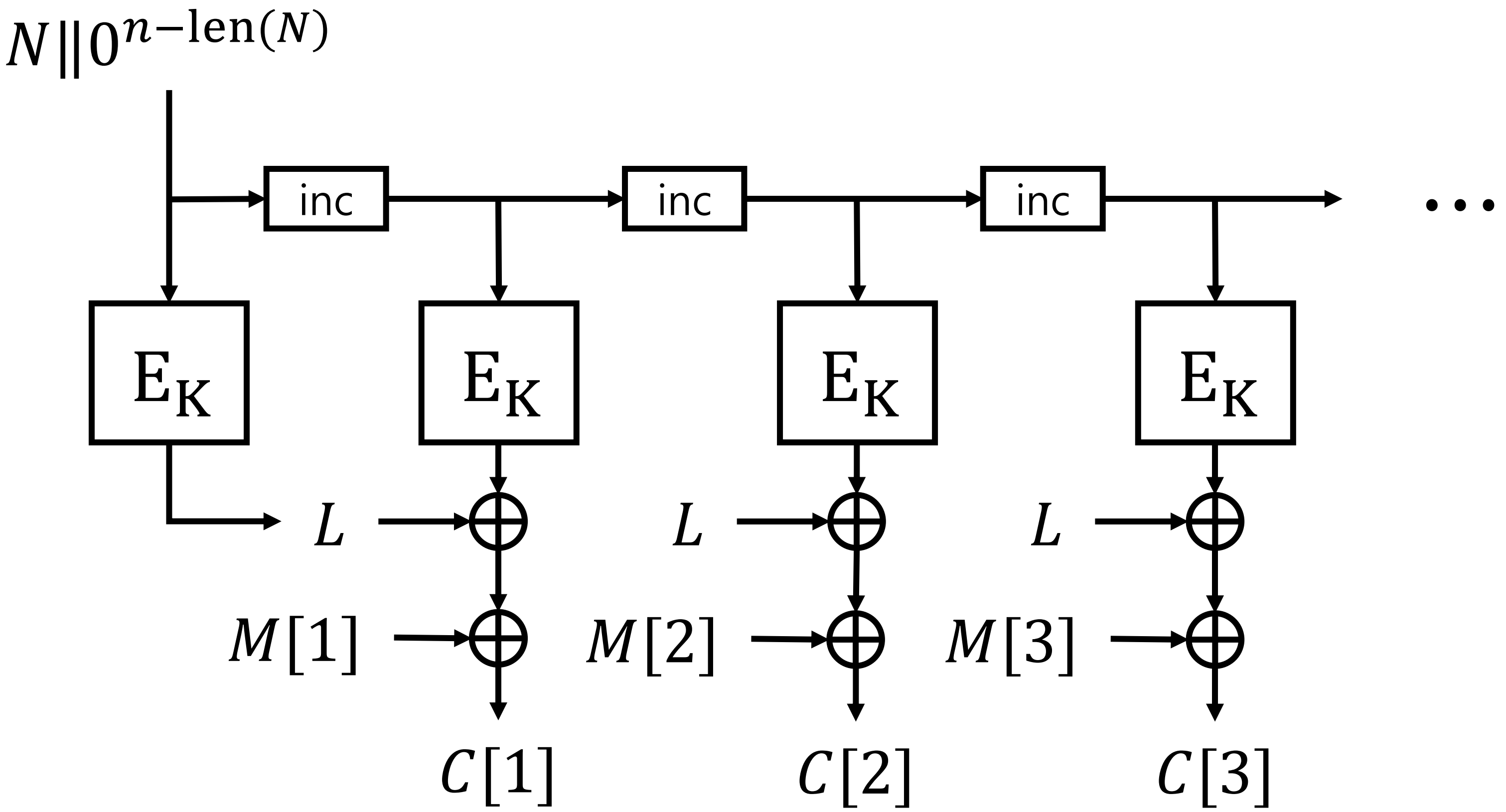
- XORP
  - XORing two outputs of the permutation.
  - XORP is secure PRF up to $\boldsymbol{O(2^n)}$ queries.[1]



(1) W. Dai, V. T. Hoang, and S. Tessaro. Information-Theoretic Indistinguishability via the Chi-Squared Method. CRYPTO 2018

Design Principle to Enhance Security

- CENC [1]



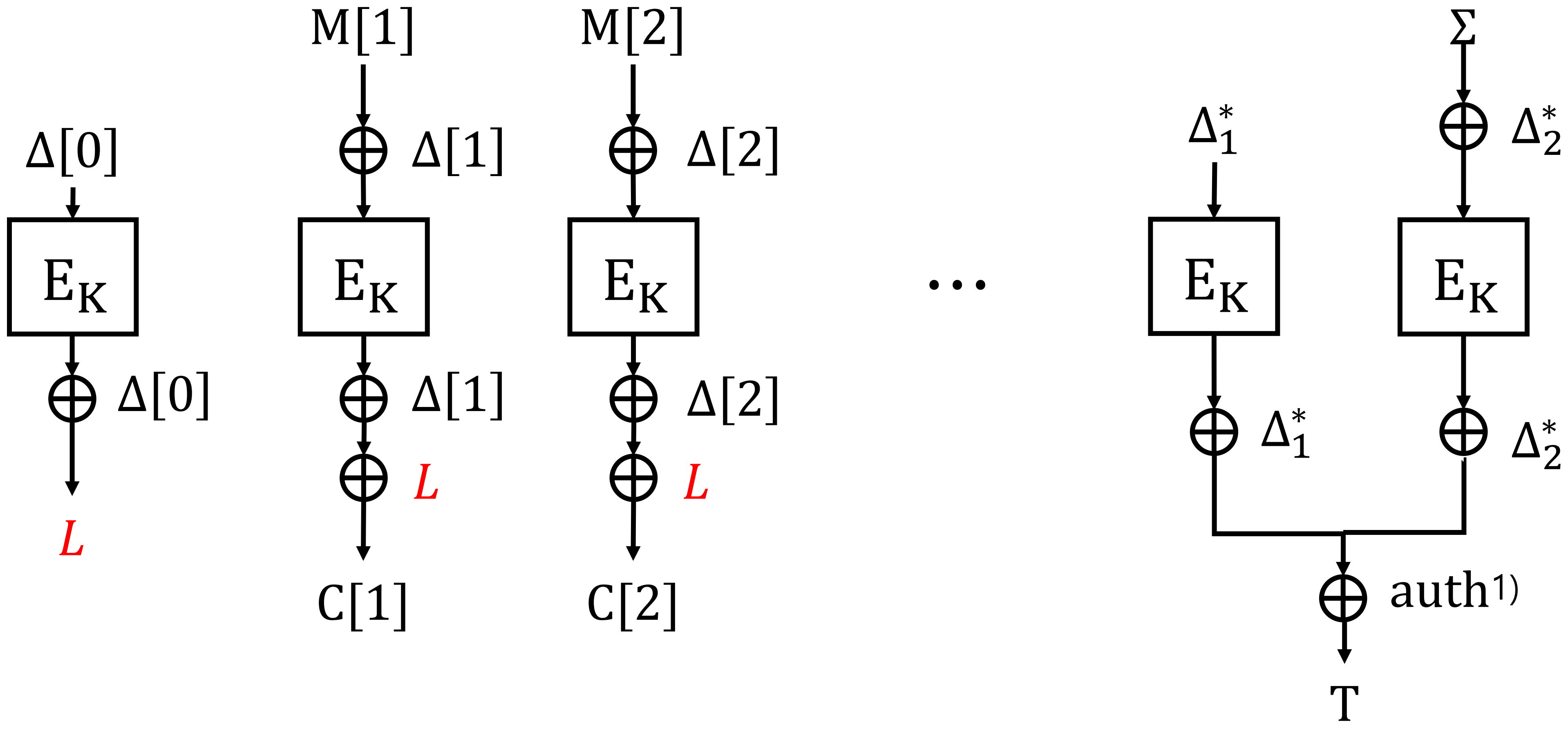
(1) Tetsu Iwata. New blockcipher modes of operation with beyond the birthday bound security. FSE 2006

Design Principle to Enhance Security

- The main point of enhancing security is XORing two outputs of a block cipher.

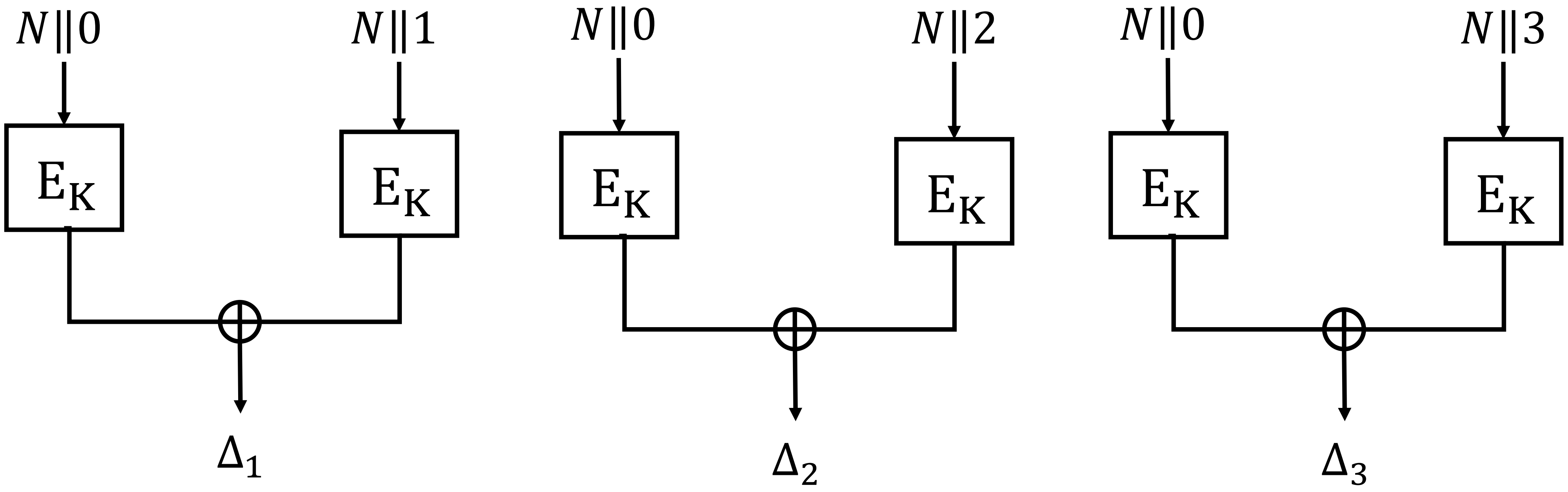
- To obtain a BBB authenticated encryption, the message should be fed to the input of the block cipher.

Structure of XOCB



1) auth is the hash value of the associated data.

Masking Generation



Masking Generation

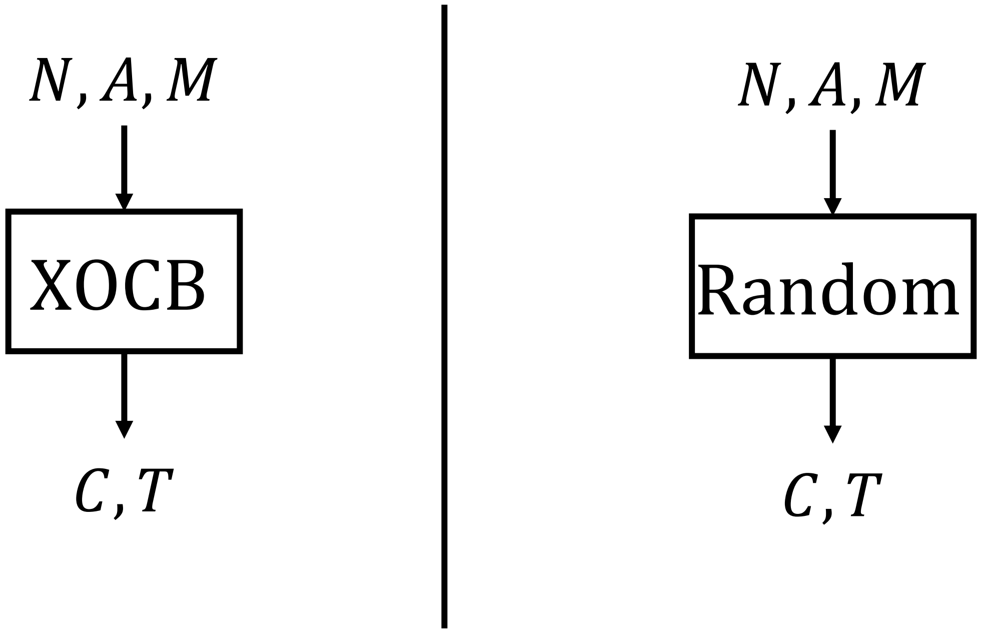
- To ensure the randomness of the inputs of the block cipher, we constructed each masking as follows:
  - For the i-th message block : $2^i\Delta_1 \oplus \Delta_2$
  - For a partial message block : $2^i\Delta_1$
  - For the i-th associated data block : $2^i\Delta_2$
  - For tag generation blocks : $2^m\Delta_1 \oplus \Delta_3, 2^m\Delta_1 \oplus \Delta_3$

Proof Sketch : Overview

- We use H-coefficient technique.
- For the probability to get good transcripts in the ideal world, we use extended Mirror theory
  - first, for evaluations in the mask generations and message encryptions,
  - second, for evaluations in the tag generations.

Proof Technique : H-coefficient Technique

- H-coefficient Technique upper bounds the adversarial distinguishing advantage between a **real construction** and its **ideal counterpart.**



Proof Technique : H-coefficient Technique

- After the adversary finishes the queries, the adversary gets a "**transcript**", which consists of all the information the adversary has obtained during the attack.
- The oracle also gives the evaluations determined in the query phase. (This information is also added to the transcript.)
  - In the real world, the oracle gives the real evaluations.
  - In the ideal world, the oracle gives the evaluations by a certain process.

Jacques Patarin. The “coefficients H” technique. SAC 2008

Proof Technique : H-coefficient Technique

- We can divide the set of all possible transcripts into two subsets, say "**Good**" transcripts (Γ_{Good}) and "**Bad**" transcripts (Γ_{Bad}).
- If there exists non-negative numbers ε_1 and ε_2 such that

$$\frac{\Pr[\mathrm{T_{re}}=\tau]}{\Pr[\mathrm{T_{id}}=\tau]} \geq 1-\varepsilon_1 \text{ for any } \tau \in \Gamma_{\mathrm{Good}},$$

$$\Pr[\mathrm{T_{id}} \in \Gamma_{\mathrm{bad}}] \leq \varepsilon_2,$$

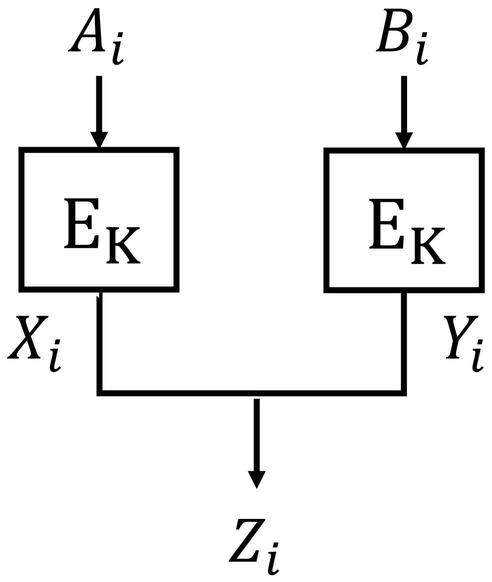
then for any adversary $\mathcal{D}$, one has

$$\left|\Pr\left[\mathcal{D}^{\mathcal{O}_{real}}=1\right]-\Pr\left[\mathcal{D}^{\mathcal{O}_{ideal}}=1\right]\right| \leq \varepsilon_1+\varepsilon_2.$$

Jacques Patarin. The “coefficients H” technique. SAC 2008

Proof Technique : Mirror Theory

- Mirror theory is a very powerful tool to estimate the number of solutions to a certain type of system of equations.

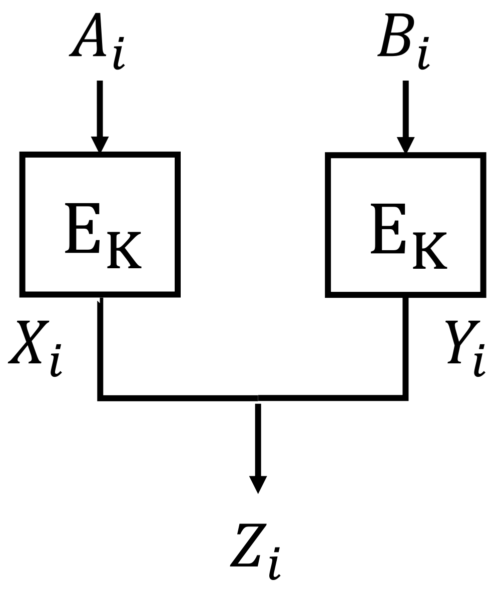


$$X_1 \oplus Y_1 = Z_1$$
$$X_2 \oplus Y_2 = Z_2$$
$$\dots$$
$$X_n \oplus Y_n = Z_n$$

Patarin, Jacques. Mirror theory and cryptography. Applicable Algebra in Engineering, Communication and Computing 28 (2017): 321-338.

Proof Technique : Mirror Theory

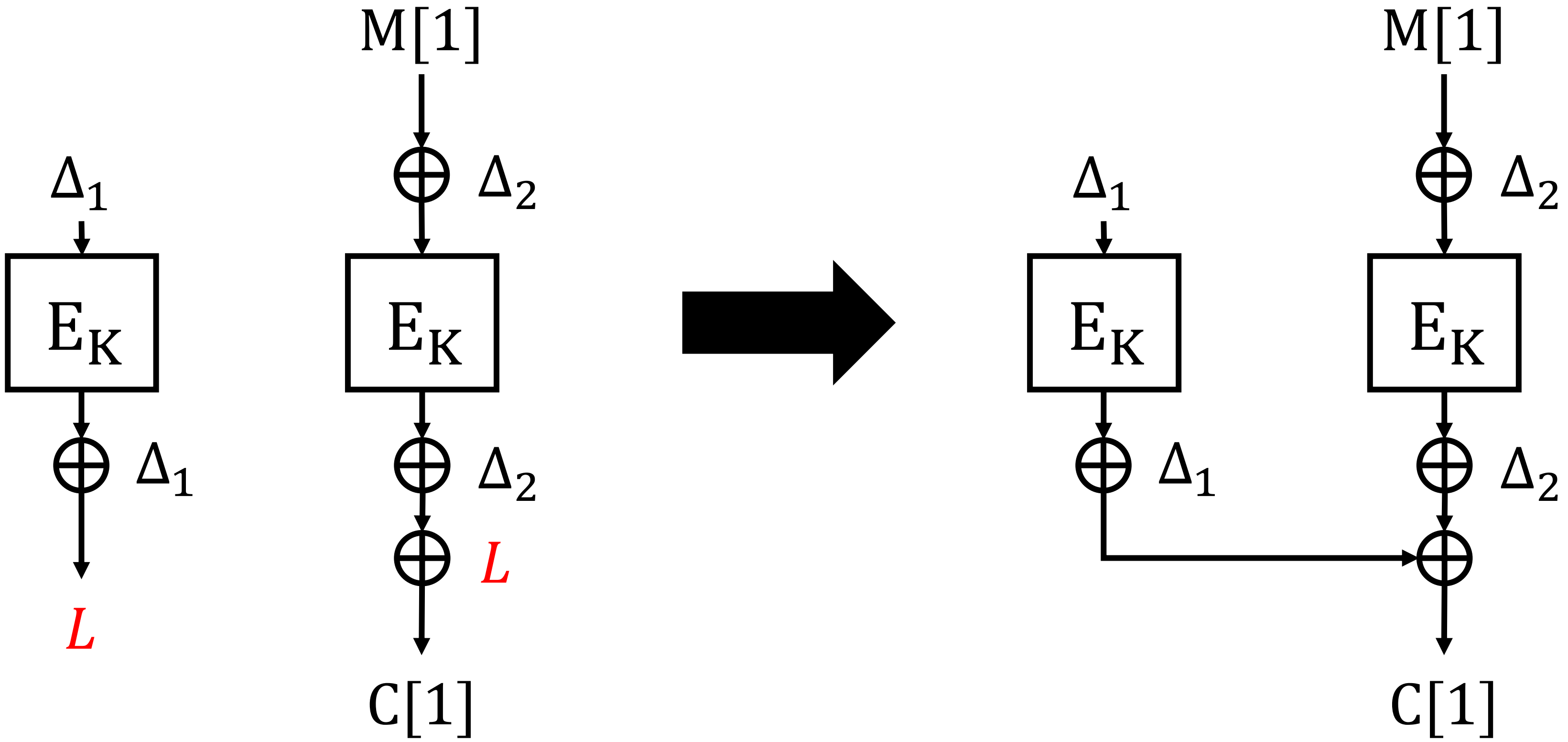
- We use the **extended Mirror theory**, which estimates the number of solutions to **a system of equations** as well as **non-equations**.



$$\begin{aligned} X_1 \oplus Y_1 &= Z_1 \\ X_2 \oplus Y_2 &= Z_2 \\ &\cdots \\ X_n \oplus Y_n &= Z_n \end{aligned} \qquad \begin{aligned} X'_1 \oplus Y'_1 &\neq Z'_1 \\ X'_2 \oplus Y'_2 &\neq Z'_2 \\ &\cdots \\ X'_m \oplus Y'_m &\neq Z'_m \end{aligned}$$

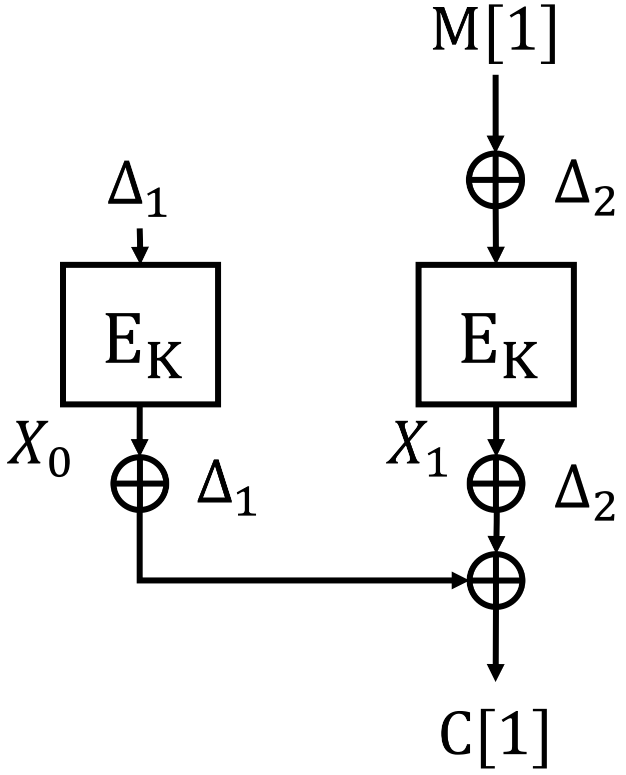
Proof Technique : Mirror Theory

- In our proof, we applied Mirror theory to compute the upper bound of the number of solutions for the equations.



Proof Technique : Mirror Theory

- In our proof, we applied Mirror theory to compute the upper bound of the number of solutions for the equations.



$$X_0 \oplus X_1 = \mathrm{C}[1] \oplus \Delta_1 \oplus \Delta_2$$

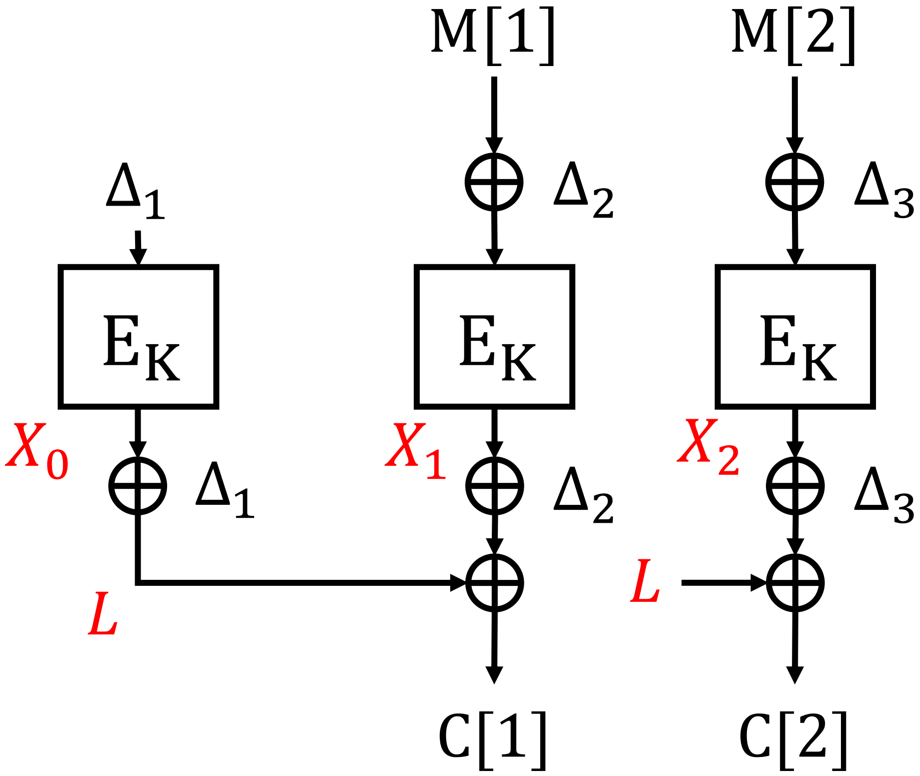
$$\vdots$$

We can collect those equations for all the ciphertext blocks.

Let $H(G)$ be the number of solutions.

Proof Technique : Mirror Theory

- Then the probability that those evaluations (related to the ciphertexts) are determined is the inverse of the number of the solutions.



The probability that $X_0, X_1, X_2, X_3, X_4, \ldots$ are determined is $1/H(G)$.

Result

- As a result, XOCB has the following security.

$$\mathrm{Adv}^{\mathrm{nAE}}_{\mathrm{XOCB}}(\mathcal{D}) \leq \frac{28q + 2\sigma + 1.5ql + 1.5l\sigma}{2^n} + \frac{4q\sigma^2 + (30q^2 + 10q)\sigma + 93q^3 + 44q^2}{2^{2n}} + \frac{(8\sigma^2 q + 45\sigma q^2 + 6q^3)l + \sigma^3 l}{2^{2n+1}}.$$

q : total number of queries.

σ : total number of queried blocks of n bits

l : maximum query length in n-bit blocks.

Lead term : $\frac{1.5l\sigma}{2^n} + \frac{\sigma^3 l}{2^{2n+1}}$

Result

- We can conclude that XOCB has BBB security when $l < 2^{\frac{n}{2}}$, and has $\frac{2}{3}n$-bit security when $l = O(1)$.
- This might not be a practical problem in real-world applications since many practical communication protocols specify a maximum packet length (MTU, Maximum transmission unit).

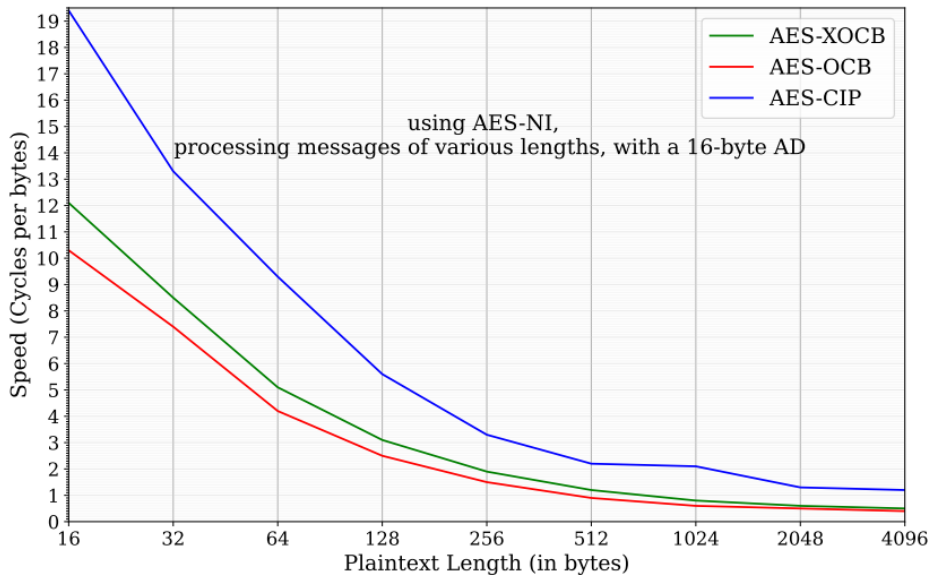
Comparison

Scheme	Primitive	Rate	Security	Lead Terms*
OCB	SPRP	1	$n/2$	$\frac{\sigma^2 + q}{2^n}$
GCM	PRP, MUL	1/2	$n/2$	$\frac{\sigma^2 + q}{2^n}$
CHM, CIP	PRP, MUL	1/2	$2n/3$	$\frac{\sigma^3}{2^{2n}} + \frac{\sigma}{2^n}$
XOCB	SPRP	1	$2n/3$	$\frac{l\sigma^3}{2^{2n}} + \frac{l\sigma}{2^n}$

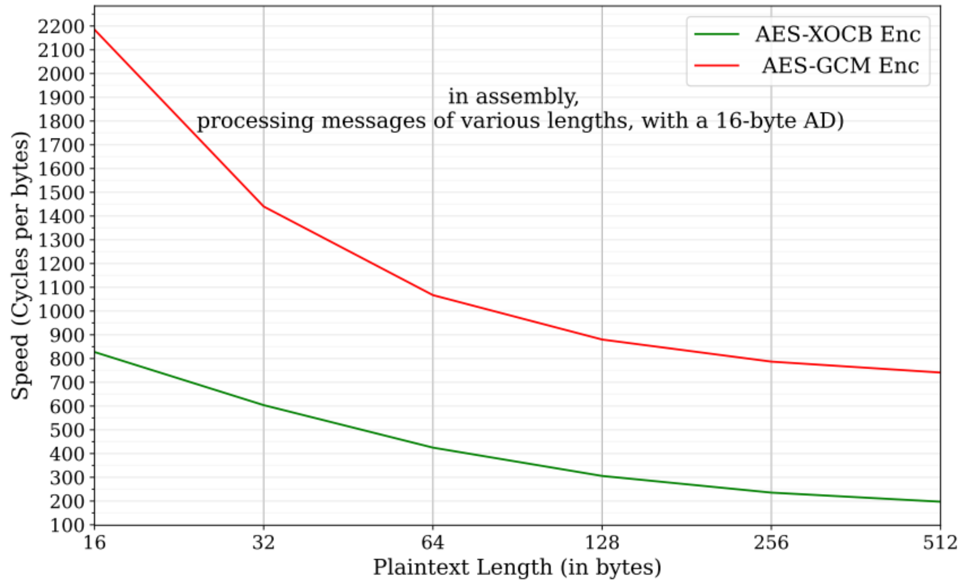
* σ : total queried blocks in n-bit blocks, q : total number of queries, and l : the maximum block length of a query. (We assume $O(1)$ AD blocks.)

Implementation

- The performance of XOCB is quite close to OCB and faster than CIP for x64 platforms with AES-NI.
- For 8-bit AVR, the initialization cost is not negligible and affects the total performance.



Speeds on an x86-64 CPU



Speeds on an 8-bit AVR

Conclusion

- **XOCB** is a new authenticated encryption mode which **mostly follows the structure of OCB.**
  - It has a quantitatively stronger security than the seminal OCB while inheriting most of the efficiency advantages.
- Further reseach topics:
  - Optimizing the scheme to reduce computational overhead
  - Reducing the length contribution to the bound
  - More comprehensive benchmarks

Thank you

Reference

1. W. Dai, V. T. Hoang, and S. Tessaro. Information-Theoretic Indistinguishability via the Chi-Squared Method. In J. Katz and H. Shacham, editos, Advances in Cryptology - CRYPTO 2018 (Proceedings, Part III), volume 10403 of LNCS, pages 497-523. Springer, 2017.

2. Iwata, Tetsu. New blockcipher modes of operation with beyond the birthday bound security. Fast Software Encryption: 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers 13. Springer Berlin Heidelberg, 2006.

3. Patarin, Jacques. Mirror theory and cryptography. Applicable Algebra in Engineering, Communication and Computing 28 (2017): 321-338.

4. Patarin, Jacques. The “coefficients H” technique. Selected Areas in Cryptography: 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers 15. Springer Berlin Heidelberg, 2009.