家庭から宇宙まで、エコチェンジ

Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security

Yusuke Naito

Mitsubishi Electric Corporation, Japan

FSE 2018

March 6, 2018

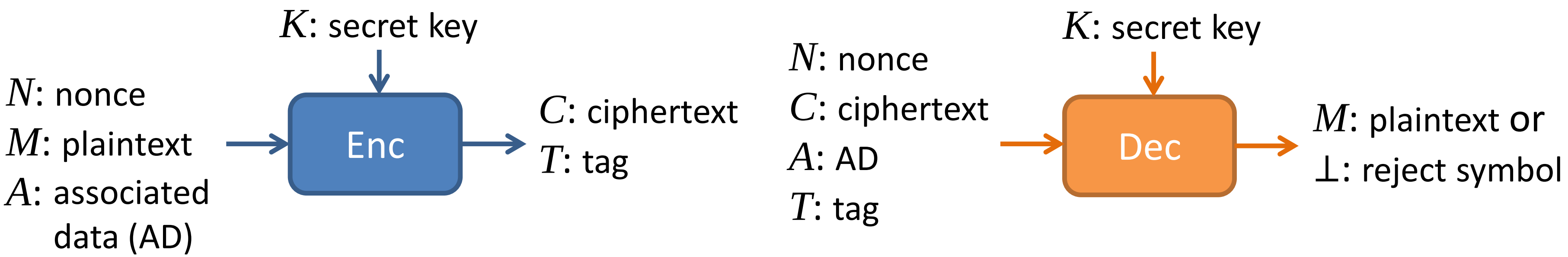
Summary

- Goal: design blockcipher-based AEAD schemes (authenticated encryption with associated data)
  - highly efficient: a blockcipher is called once for each data block.
  - highly secure: beyond-birthday-bound (BBB) security.
- XKX
  - a tweakable blockcipher (TBC) from a (classical) blockcipher.
  - offers highly efficient and BBB-secure AEAD schemes.
- Comparison

AEAD Schemes	Highly Efficient	BBB Security
OCB1, OCB2, OCB3 (Rogaway et al.) OTR (Minematsu)	Yes	No
XKX-based AEAD schemes	Yes	Yes

Authenticated Encryption with Associated Data (AEAD)

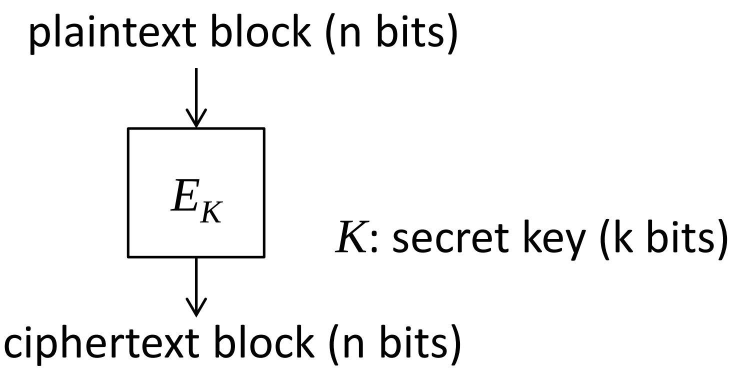
- AEAD (Nonce-based)
  - ensures jointly privacy and authenticity,
  - consists of encryption and decryption algorithms.



- Nonce-respecting scenario.
  - Enc: the same nonce is not repeated.
  - Dec: the same nonce can be repeated.

Blockcipher-based AEAD

- Primitives of AEAD schemes:
  blockcipher, tweakable blockcipher, permutation, etc.
- Blockcipher

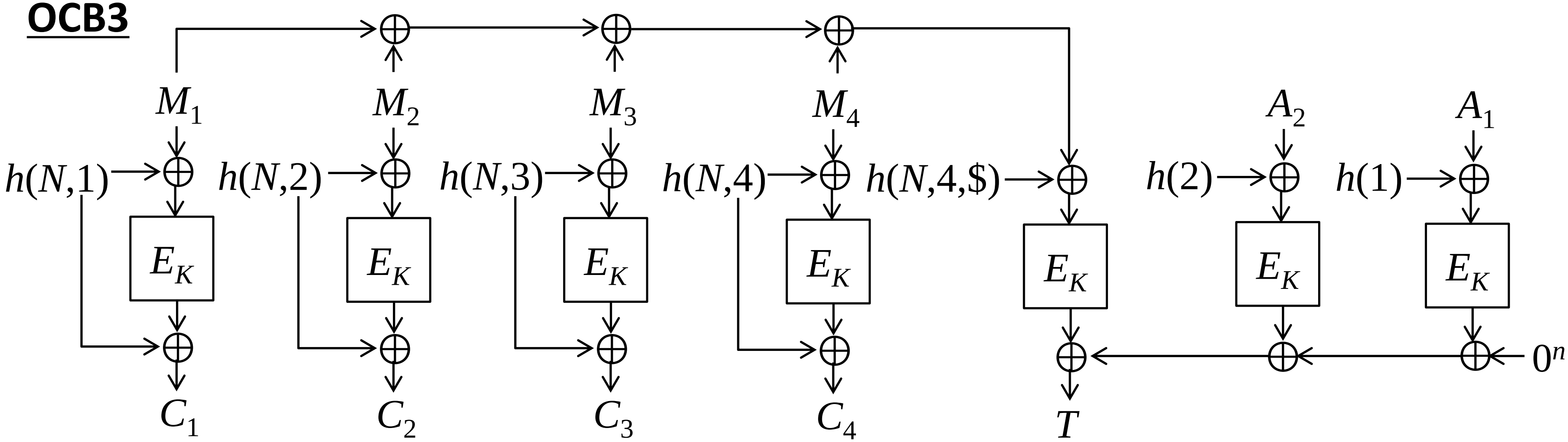


  - Family of permutations indexed by a key.
  - A blockcipher key is randomly drawn.
  - Security: strong pseudo-random permutation (SPRP).
- Research topic of blockcipher-based AEAD:
  - Designing a highly efficient AEAD scheme.

Highly Efficient AEAD Schemes

- Highly efficient:
  for each data block, a blockcipher is called once.
- Existing schemes:
  OCB1, OCB2, OCB3, OTR, etc.

OCB3

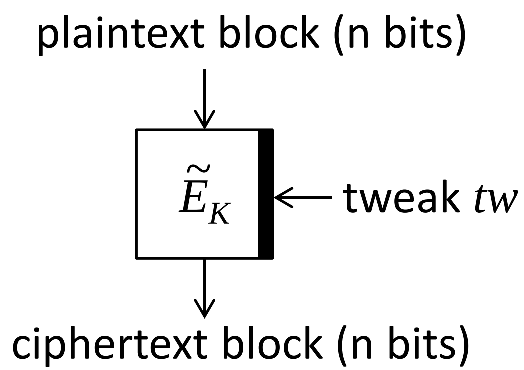


h: almost XOR universal hash function

- Design methodology:
  Tweakable blockcipher-based design.

Tweakable Blockcipher (TBC) [Liskov, Rivest, Wagner 02]

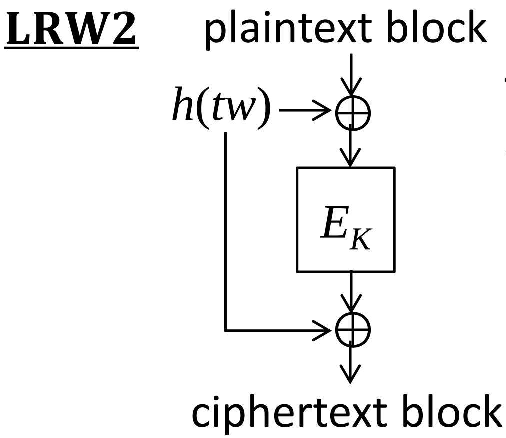
- Generalization of blockciphers.



- Take an input tweak tw.
  - ✓ Role: Changing tw = Rekeying
  - ✓ Cost: Changing $tw \ll$ Rekeying
- Security: Tweakable Strong Pseudo-Random Permutation (TSPRP).

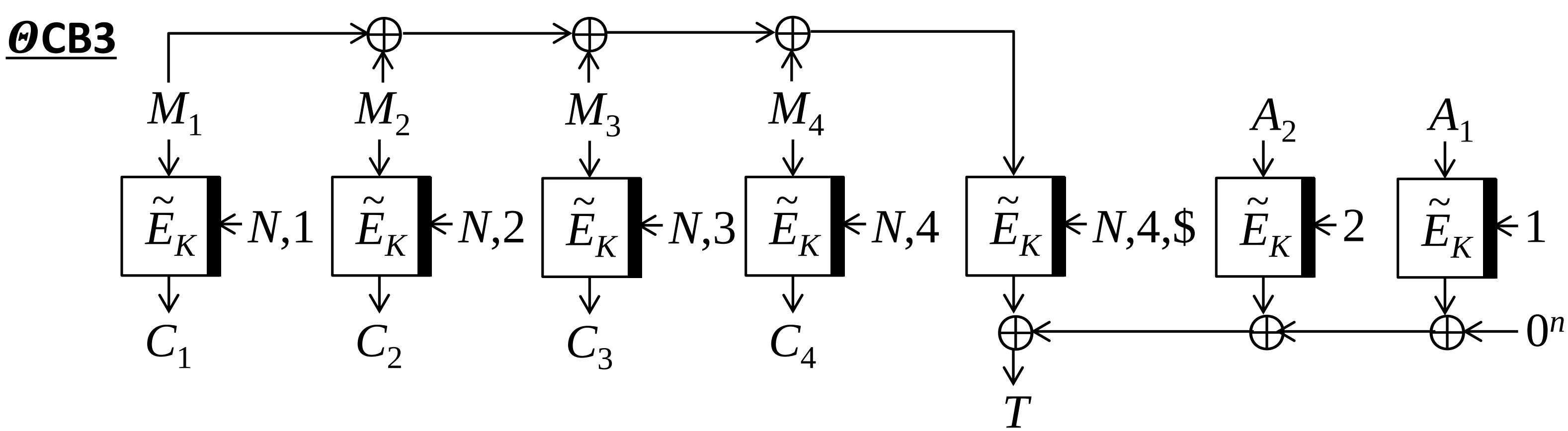
TBC-based Design Methodology

1. Design a highly efficient TBC from a blockcipher: a blockcipher is called once for each query.

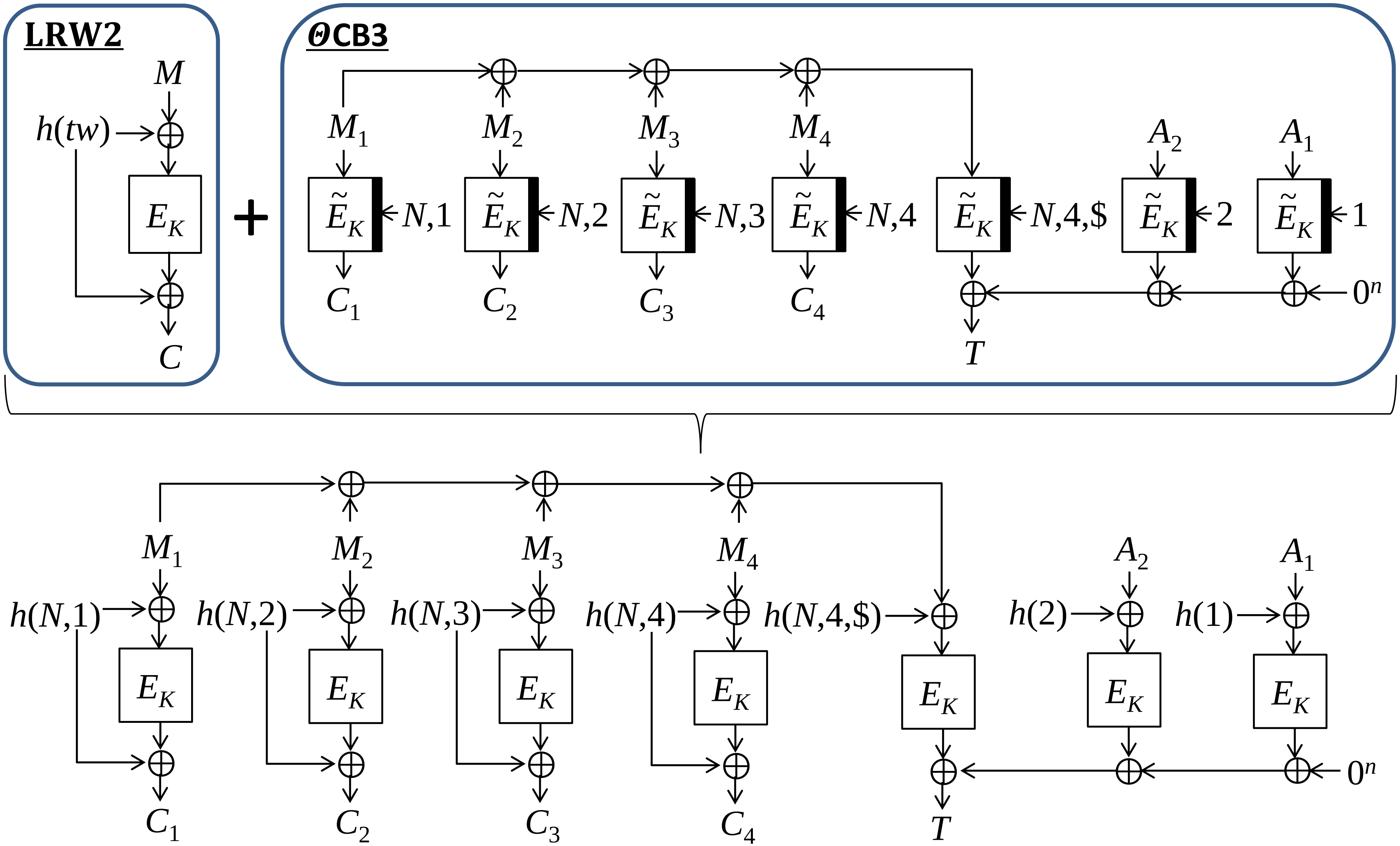


The TSPRP-advantage $\le \sigma^2/2^n$ (birthday bound), where σ is # blockcipher calls by all queries.

2. Design a highly efficient AEAD scheme from a TBC: a TBC is called once for each data block.



Efficient Blockcipher-based AEAD Scheme

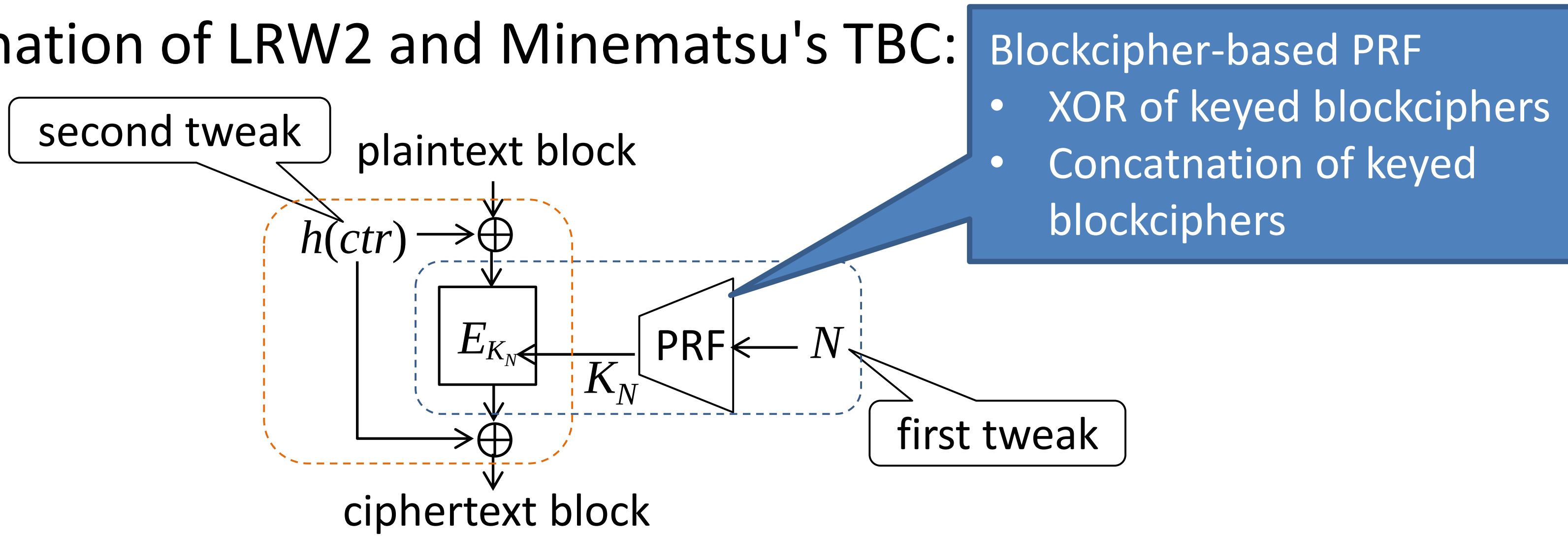


Security of Efficient AEAD Schemes

- Existing highly efficient AEAD schemes use LRW2-type TBCs.
- LRW2-based AEAD schemes are secure up to the birthday bound, where the security bound is $\sigma^2/2^n$.
- The security bound defines a term of rekeying: A key is changed when the bound reaches a threshold, e.g., $1/2^{20}$, $1/2^{32}$.
- For example, when n=64 and the threshold=$1/2^{20}$, a key is changed when # data blocks $\sigma = 2^{22}$ (34 Mbyte).
- The birthday bound might be unreliable, e.g.,
  - when the block size n is small, (n=64)
  - when large amounts of data are processed, or
  - when large number of connections need to be kept secure.
- Designing highly efficient AEAD schemes with BBB-security is an important research topic.

Our Result: XKX (Xor-Key-Xor)

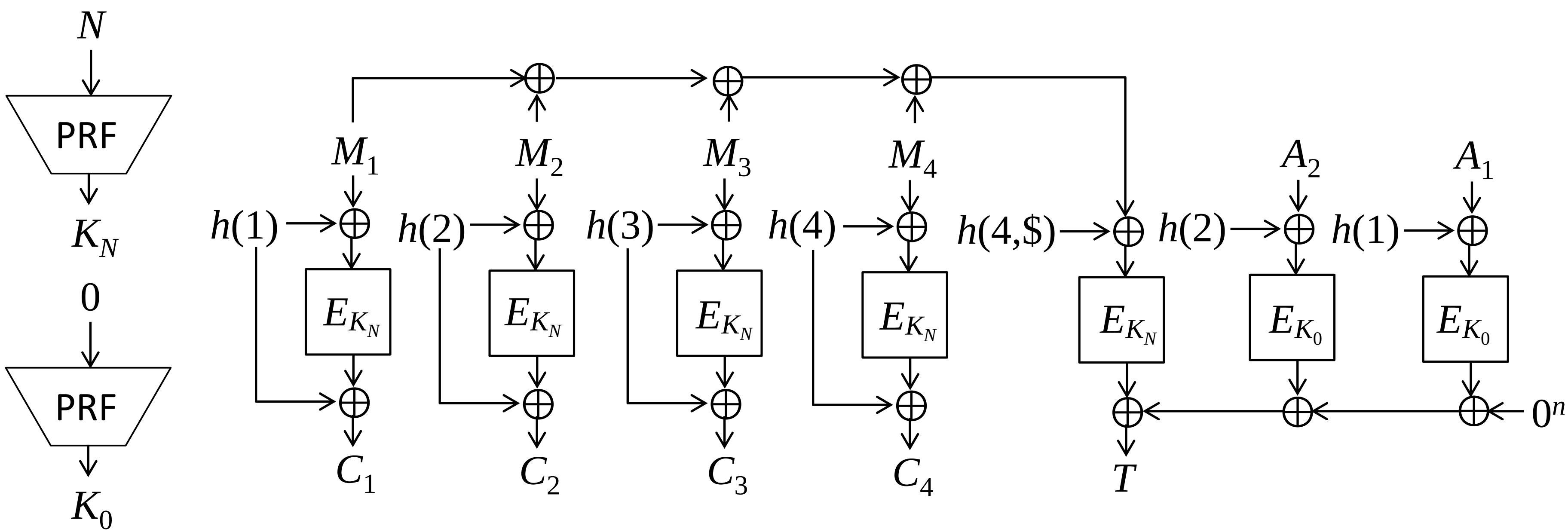
- Blockcipher-based TBC.
- Combination of LRW2 and Minematsu's TBC:



  - Accept two tweaks: first tweak N, second tweak ctr.
  - The first tweak N is input to the PRF and the output is used as a blockcipher key (Mienmatsu's TBC).
  - The second tweak ctr is input to h (LRW2).
- Offer highly efficient AEAD schemes with BBB-security, by combining with efficient TBC-based AEAD schemes.

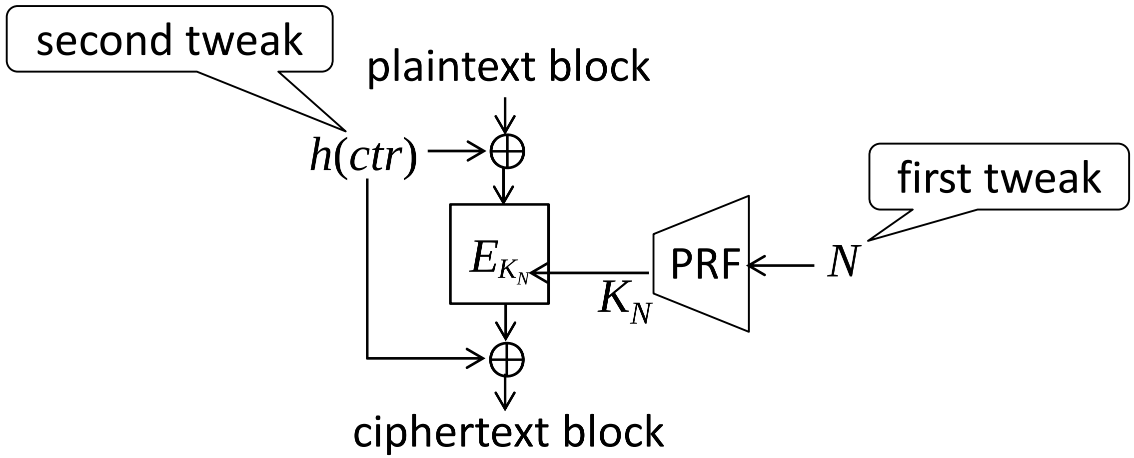
XKX-based AEAD Scheme

ΘCB3 with XKX



- N and 0 are used as first tweaks.
- At the precomp., N and 0 are input to the PRF, then the N-dependent key K_N and the 0-key K_0 are defined.
- After the precomp., a blockcipher is called once for each data block.

Security of XKX



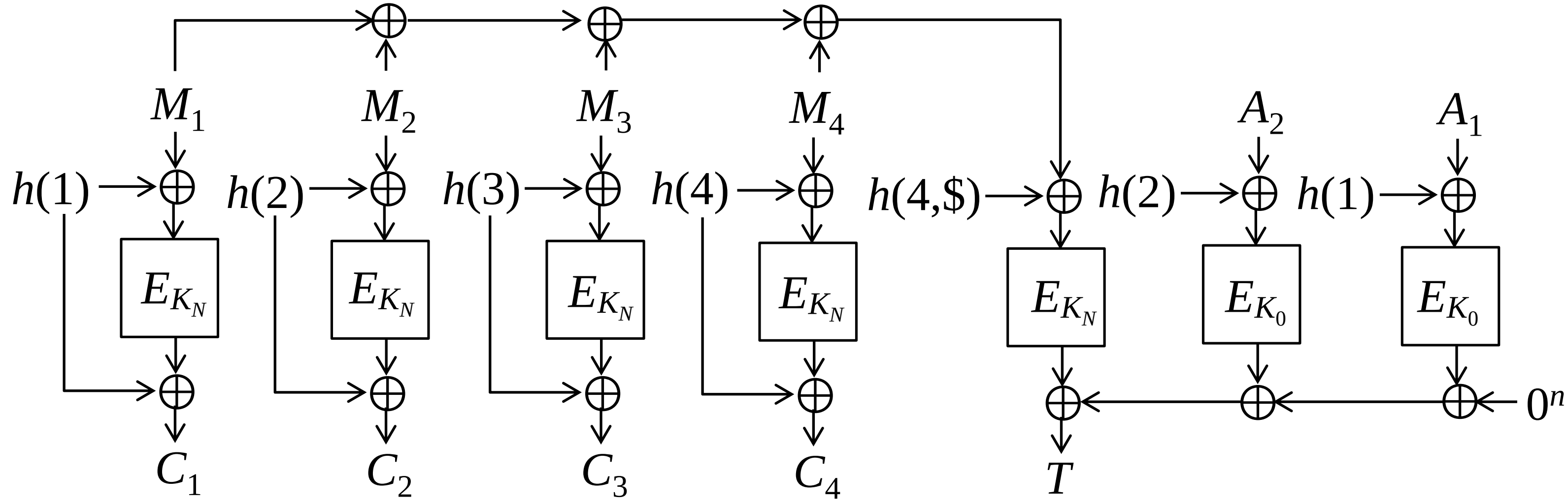
- When # queries with the same first tweak is $\leq R$ and
  # distinct first tweaks N is Q,

  $Q \cdot \left(\frac{R^2}{2^n} + \text{(SPRP advantage for } E\text{)} \right)$ is introduced.
- Since in XKX the PRF is used, (PRF advantage) is introduced.
- TSPRP-advantage of XKX

  $$\leq \frac{Q \cdot R^2}{2^n} + \underbrace{Q \cdot \text{(SPRP advantage for } E\text{)} + \text{(PRF advantage)}}_{\text{can be negligible when } E \text{ and PRF are secure.}}.$$

Security of ΘCB3 with XKX

K_N=PRF(N)
K_0=PRF(0)



- From the XKX's bound $QR^2/2^n$,
  - Privacy-advantage $\leq \frac{q_E \cdot \ell^2}{2^n} + \frac{\sigma_A^2}{2^n}$,
  - Authenticity-advantage $\leq \frac{q_E \cdot \ell^2}{2^n} + \frac{\sigma_A^2}{2^n} + \frac{\sigma_D^2}{2^n}$,

  where q_E is # Enc-queries,
  ℓ is # E-calls by an Enc query ,
  σ_A is # all E-calls handling AD blocks by enc-queries,
  σ_D is # all E-calls by dec-queries.

Usually, AD is not frequently changed. Then, the term is negl.

When # forgeries is limited (a key is changed when # forgeries reaches some threshold), the term is negl.

Conclusion

	Priv	Auth
OCB1, 2, 3, OTR	$\sigma_E^2/2^n$	$\sigma^2/2^n$
XKX-based AEAD schemes	$q_E\ell^2/2^n + \cancel{\sigma_A^2/2^n}$	$q_E\ell^2/2^n + \cancel{\sigma_A^2/2^n} + \cancel{\sigma_D^2/2^n}$

- Existing highly efficient AEAD schemes such as OCB1, 2, 3, OTR are not BBB secure.
- This paper
  - XKX, a blockcipher-based TBC.
  - highly efficient and BBB secure AEAD schemes if $\sigma_A, \sigma_D << 2^{n/2}$.
- Improvement (Latincrypt 2017)
  - By proving the security of XKX-based AEAD schemes from scratch, the terms $\sigma_A^2/2^n$, $\sigma_D^2/2^n$ can be eliminated.

Thank you for your attention!