# ZOCB and ZOTR: Tweakable Blockcipher Modes for Authenticated Encryption with Full Absorption

Zhenzhen Bao, NTU, Singapore
Jian Guo, NTU, Singapore
Tetsu Iwata, Nagoya University, Japan
Kazuhiko Minematsu, NEC corporation, Japan

FSE 2020
November 9–13, 2020, Virtual

# Overview: ZOCB and ZOTR

- nonce-based authenticated encryption with associated data (AEAD)
- use a tweakable blockcipher (TBC) as the underlying primitive
- fully utilize the input of the TBC to process a plaintext and associated data (AD)
  - full absorption
  - reduce the number of TBC calls of ΘCB3 and $\mathbb{OTR}$
- have a unique design feature that an authentication tag is independent of a part of AD

# Outline

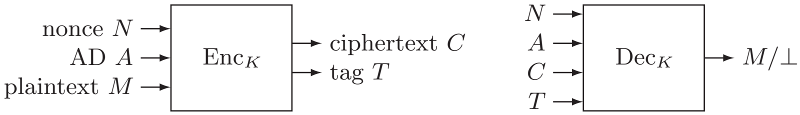
- Background
- ZOCB and ZOTR
- Instantiation and implementation
  - TAES, a TBC based on AES-256
- Conclusions

# Outline

- ▷ Background
- ZOCB and ZOTR
- Instantiation and implementation
  - TAES, a TBC based on AES-256
- Conclusions

# AEAD

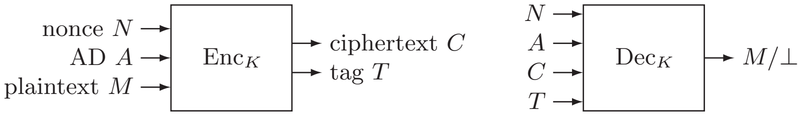
- nonce-based authenticated encryption with associated data (AEAD)
  - privacy and authenticity of plaintexts
  - authenticity of associated data (AD)




- various design approaches
  - dedicated design
  - blockcipher
  - tweakable blockcipher (TBC)
  - cryptographic permutation
  - pseudorandom function

# AEAD

- nonce-based authenticated encryption with associated data (AEAD)
  - privacy and authenticity of plaintexts
  - authenticity of associated data (AD)



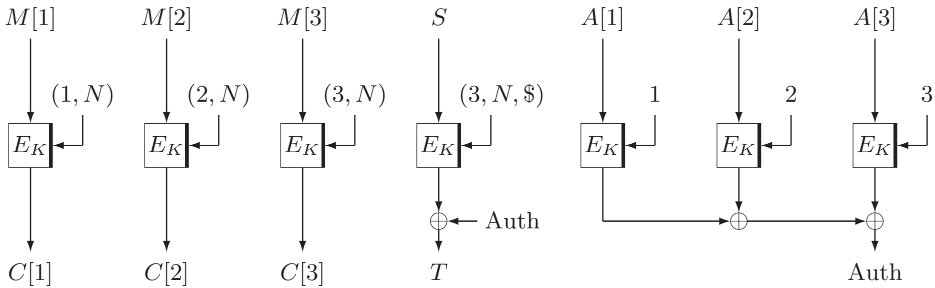

- various design approaches
  - dedicated design
  - blockcipher
  - ▷ tweakable blockcipher (TBC)
  - cryptographic permutation
  - pseudorandom function

# ΘCB3

- AEAD scheme based on a TBC [KR11]
- was not proposed as a standalone AEAD mode of TBCs, but was introduced as an abstraction of OCB3 for a security proof
- employed in many proposals for its strong features
  - strong provable security result
  - fully parallelizable

[KR11] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated- Encryption Modes. FSE 2011

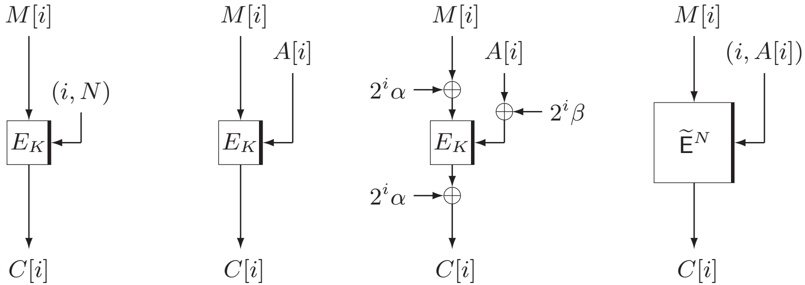
# ΘCB3




- $E_K$ is a TBC, and $S$ is the checksum of $M$
- The process for $M$ and that for $A$ are separated. Can we efficiently integrate these processes?
  - explored for sponge-based [SY15, MRV15] and PRF-based AEAD schemes [RVV15]

[SY15] Yu Sasaki and Kan Yasuda. How to Incorporate Associated Data in Sponge- Based Authenticated Encryption. CT-RSA 2015
[MRV15] Bart Mennink, Reza Reyhanitabar, and Damian Vizár. Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption. ASIACRYPT 2015
[RVV15] Reza Reyhanitabar, Serge Vaudenay, and Damian Vizár. Boosting OMD for Almost Free Authentication of Associated Data. FSE 2015

# Idea



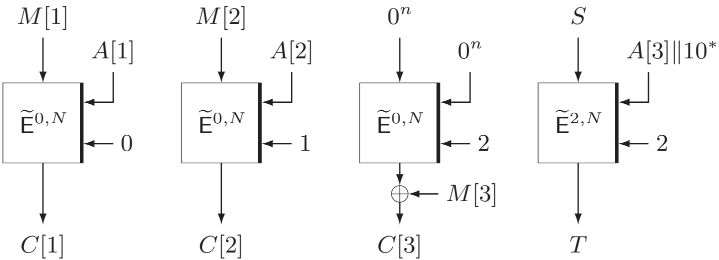

- use the tweak input to process $A[i]$ to fully utilize the input, "full absorption"
- rely on masks for the counter and nonce [Rog04, MI15, IMPS17], $\alpha = E_K^{3,0}(N), \beta = E_K^{3,1}(N)$


[Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. ASIACRYPT 2004

[MI15] Kazuhiko Minematsu and Tetsu Iwata. Tweak-Length Extension for Tweakable Blockciphers. IMACC 2015

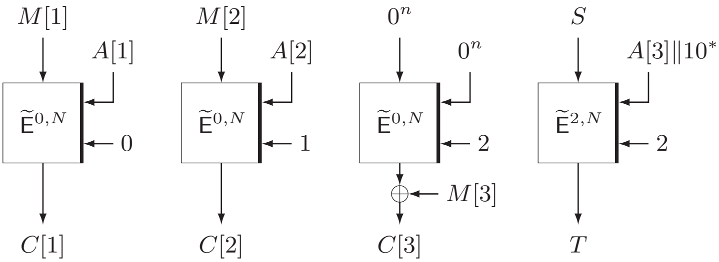
[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. CRYPTO 2017

# From ΘCB3 to iZOCB



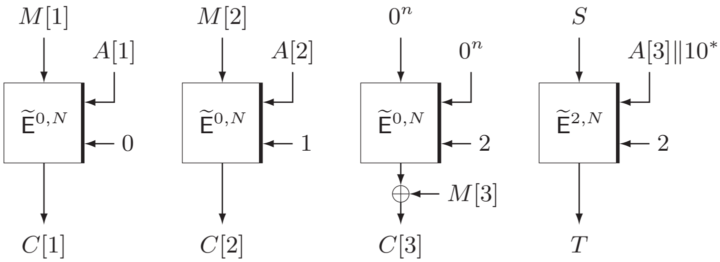

- $|M| = 3n, |M[i]| = n, 2n < |A| < 3n, |A[1]| = |A[2]| = n$
- $S = M[1] \oplus M[2] \oplus M[3]$
- (many details are omitted)

# Secure?



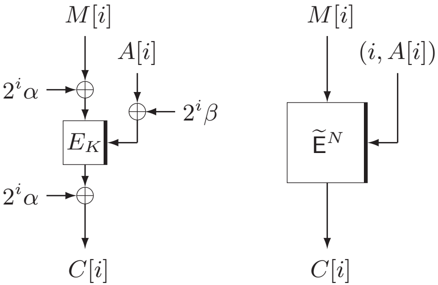

- Privacy is fine, from the uniqueness of the nonce and counter
- For authenticity, $S = M[1] \oplus M[2] \oplus M[3]$, $T$ is independent of $A[1]$ and $A[2]$
  - does not seem to provide authenticity...

# Secure?



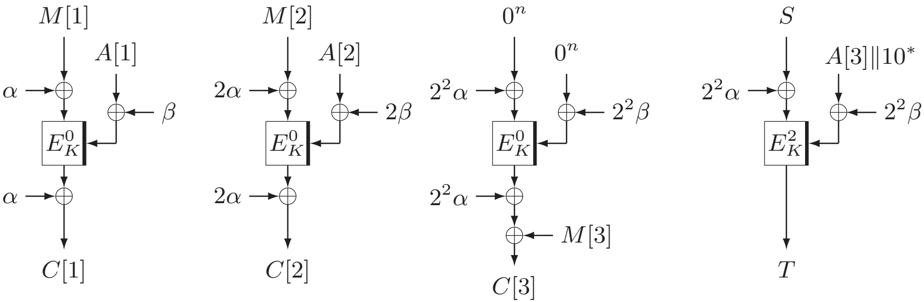

- Privacy is fine, from the uniqueness of the nonce and counter
- For authenticity, $S = M[1] \oplus M[2] \oplus M[3]$, $T$ is independent of $A[1]$ and $A[2]$
  - does not seem to provide authenticity...
  - when we decrypt $(N, A, C, T)$, the computed tag from $(N, A, C)$ that is compared with $T$, depends on the entire AD
  - works!

# From iZOCB to ZOCB




- ZOCB is obtained from iZOCB by instantiating $\widetilde{\mathsf{E}}$ with a TBC $E$

# From iZOCB to ZOCB




- $|M| = 3n, |M[i]| = n, 2n < |A| < 3n, |A[1]| = |A[2]| = n$
- $\alpha = E_K^{3,0}(N), \beta = E_K^{3,1}(N), S = M[1] \oplus M[2] \oplus M[3]$
- If AD is not long, there is no separate process for AD, and the process of AD is fully integrated into the process of a plaintext
- If AD is long, there is a separate process for it

# Provable Security Results

- standard security notions of nonce-based AEAD schemes [Rog02]
  - privacy: indistinguishability from random bits under CPA
  - authenticity: unforgeability under CCA
  - nonce-respecting adversaries
  - $E_K : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$
- $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{ZOCB}[\mathrm{Perm}(\mathcal{W},n)]}(\mathcal{A}) \leq 4\sigma^2_{\mathrm{priv}}/2^{n+\min\{n,t\}}$
- $\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{ZOCB}[\mathrm{Perm}(\mathcal{W},n)]}(\mathcal{A}) \leq 4\sigma^2_{\mathrm{auth}}/2^{n+\min\{n,t\}} + 4q'/2^n$
- ZOCB has the full $n$-bit security when $t \geq n$

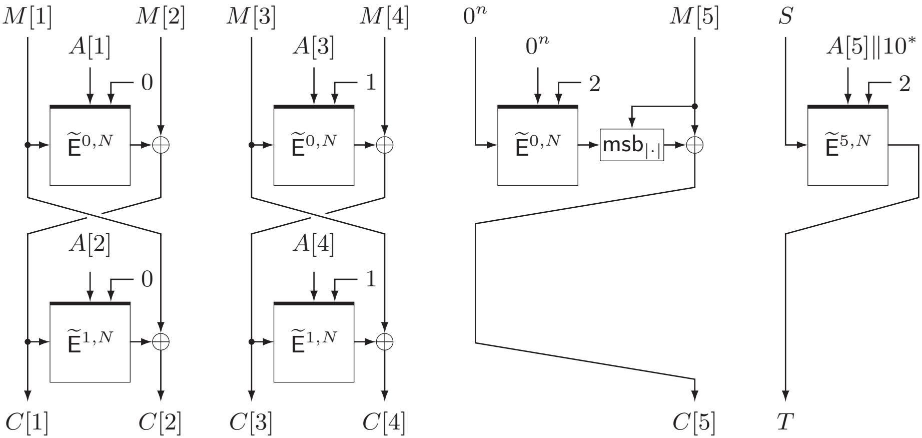
[Rog02] Phillip Rogaway. Authenticated-Encryption with Associated-Data. ACM CCS 2002

# ZOTR

- OTR is an AEAD scheme based on a blockcipher with all the features of OCB3, without using decryption of the blockcipher [Min14]
  - provable security, full parallelizability
- makes use of two round Feistel network
- $\mathbb{OTR}$ is the TBC-based counterpart
  - has a separate process of AD
  - makes the same number of TBC calls as ΘCB3
  - we can integrate the process of AD into that of a plaintext

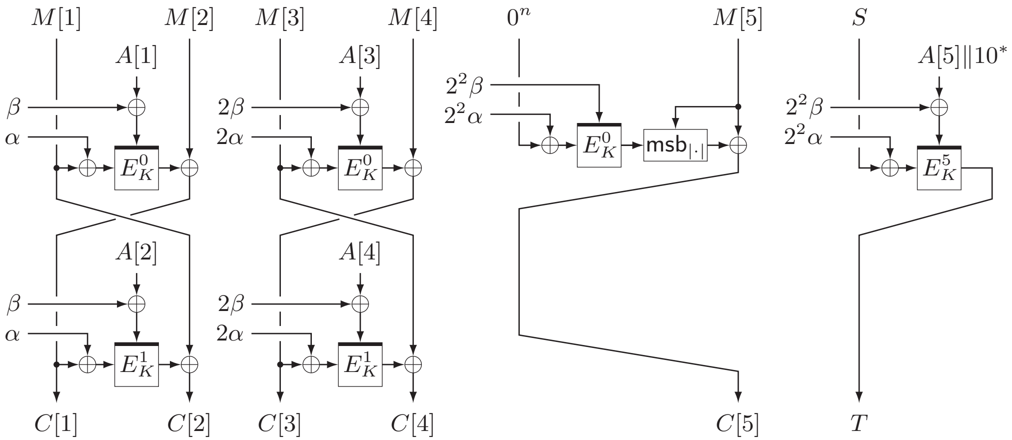
[Min14] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. EUROCRYPT 2014

# From $\mathbb{OTR}$ to iZOTR




- The process of AD is integrated into the process of a plaintext

# From iZOTR to ZOTR




- ZOTR is obtained from iZOTR by instantiating $\widetilde{\mathrm{E}}$ with $E$
  - slightly simpler than the case of ZOCB, since the decryption of $E$ is not involved

# Provable Security Results

- standard security notions of nonce-based AEAD schemes [Rog02]
  - $E_K : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$
- $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{ZOTR}[\mathrm{Perm}(\mathcal{W},n)]}(\mathcal{A}) \leq 4\sigma^2_{\mathrm{priv}}/2^{n+\min\{n,t\}}$
- $\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{ZOTR}[\mathrm{Perm}(\mathcal{W},n)]}(\mathcal{A}) \leq 4\sigma^2_{\mathrm{auth}}/2^{n+\min\{n,t\}} + 6q'/2^n$
- ZOTR also has the full $n$-bit security when $t \geq n$

[Rog02] Phillip Rogaway. Authenticated-Encryption with Associated-Data. ACM CCS 2002

# Comparison

| Scheme | Prim. | # of calls | | Inv. | Para. | Security | Ref. |
|---|---|---|---|---|---|---|---|
| | | $a < m$ | $a \geq m$ | | | | |
| OCB3 | $n$-BC | $a + m$ | | N | Y | $n/2$ | [KR11] |
| OTR | $n$-BC | $a + m$ | | Y | Y | $n/2$ | [Min14] |
| $\Theta$CB3 | $(n, t)$-TBC | $a + m$ | | N | Y | $n$ | [KR11] |
| $\mathbb{OTR}$ | $(n, t)$-TBC | $a + m$ | | Y | Y | $n$ | [Min14] |
| ZOCB | $(n, t)$-TBC | $m$ | $(a + m)/2$ | N | Y | $\min\{n, (n + t)/2\}$ | Ours |
| ZOTR | $(n, t)$-TBC | $m$ | $(a + m)/2$ | Y | Y | $\min\{n, (n + t)/2\}$ | Ours |

- $n$-BC is a blockcipher, $(n, t)$-TBC is a TBC with $t$-bit tweaks
- # of calls is for $at$-bit AD and $mn$-bit plaintexts ($n = t$), neglecting constant number

[KR11] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated- Encryption Modes. FSE 2011
[Min14] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. EUROCRYPT 2014

# Cost

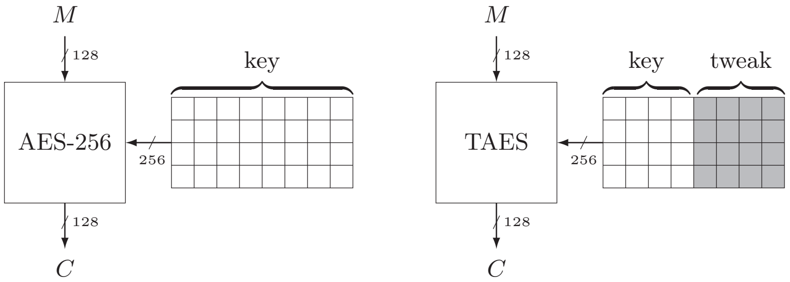
- The use of a mask requires a doubling operation
- The tweak does not behave like a counter, and updating the tweak can add a computational cost
- If AD is short, then ZOCB/ZOTR can be slower if the cost for doubling is larger than the efficiency gain
- In order to see the practical efficiency gain, we instantiated and implemented ZOCB and ZOTR

# Outline

- Background
- ZOCB and ZOTR
- ▷ Instantiation and implementation
  - TAES, a TBC based on AES-256
- Conclusions

# Instantiation

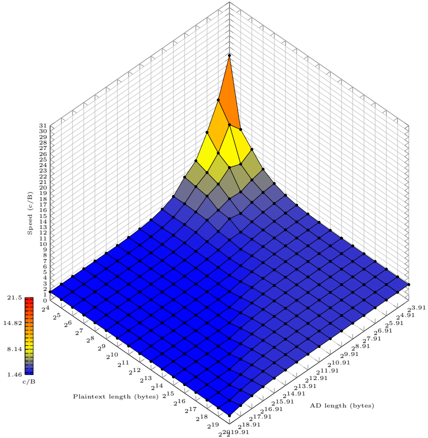
- Tweakable AES, TAES, a 128-bit block, 128-bit key, 128-bit tweak TBC
- obtained from AES-256, where key||tweak is used as the AES-256 key
  - The TAES key is placed in the first part of the AES-256 key (used as the whitening key)
  - We claim 128-bit security of TAES, in the single key setting
    - Related-key attacks in [BK09] cannot be directly applied

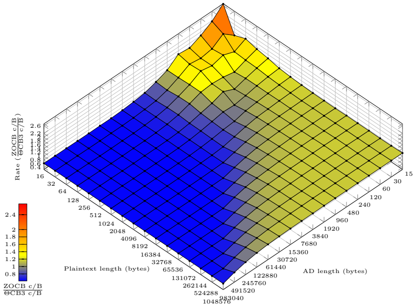



[BK09] Alex Biryukov and Dmitry Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. ASIACRYPT 2009

# Implementation

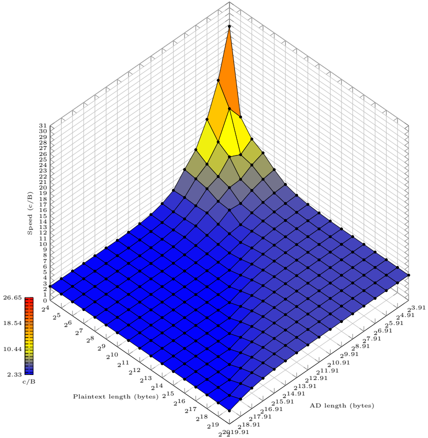
- TAES-$\{\Theta CB3, ZOCB\}$, Intel(R) Core(R) i5-6500 CPU, 3.20 GHz (Skylake family)

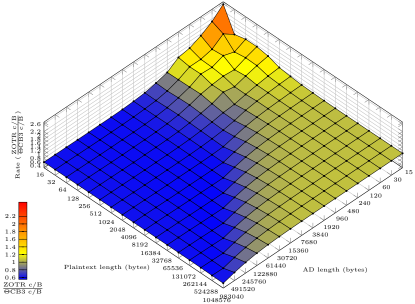


# Implementation

- TAES-$\{\Theta CB3, ZOTR\}$, Intel(R) Xeon(R) E5-2603 v3 CPU, 1.60 GHz (Haswell family)



# Implementation

- We also implemented SKINNY-ZOCB/ZOTR/ΘCB3, where SKINNY-128-256 [BJK+16] is used
- Source code, raw data, and the graphs are available at `https://github.com/zocbzotr`

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. CRYPTO 2016

# Implementation

- For short input data ($|A| \lesssim 480$ bytes or $|A|/|M| \lesssim 0.12$), TAES-ZOCB and TAES-ZOTR are not (always) as fast as TAES-ΘCB3
- For long input data ($|A| \gtrsim 480$ bytes and $|A|/|M| \gtrsim 0.12$), TAES-ZOCB and TAES-ZOTR perform better than TAES-ΘCB3
- Asymptotically with long data ($|A|/|M| \gtrsim 0.12$), the performance gain of TAES-ZOCB/ZOTR is about 40%, they are about $1.7\times$ faster than TAES-ΘCB3
- Similar observations hold for SKINNY-ZOCB/ZOTR/ΘCB3

# Outline

- Background
- ZOCB and ZOTR
- Instantiation and implementation
  - TAES, a TBC based on AES-256
- ▷ Conclusions

# Conclusions

- We designed ZOCB and ZOTR
  - reduce the number of TBC calls of ΘCB3 and $\mathbb{OTR}$
- provable security results
- software implementation results
- Future directions/open questions
  - designing a TBC with large tweak space with efficient tweak update
  - detailed security analysis of TAES
  - apply the design approach of ZOCB/ZOTR to other TBC-based constructions
    - tweakable enciphering schemes
    - robust AE schemes
    - online AE schemes

# Conclusions

- We designed ZOCB and ZOTR
  - reduce the number of TBC calls of ΘCB3 and $\mathbb{OTR}$
- provable security results
- software implementation results
- Future directions/open questions
  - designing a TBC with large tweak space with efficient tweak update
  - detailed security analysis of TAES
  - apply the design approach of ZOCB/ZOTR to other TBC-based constructions
    - tweakable enciphering schemes
    - robust AE schemes
    - online AE schemes

Thank you!