Key Committing Security of AEZ and More

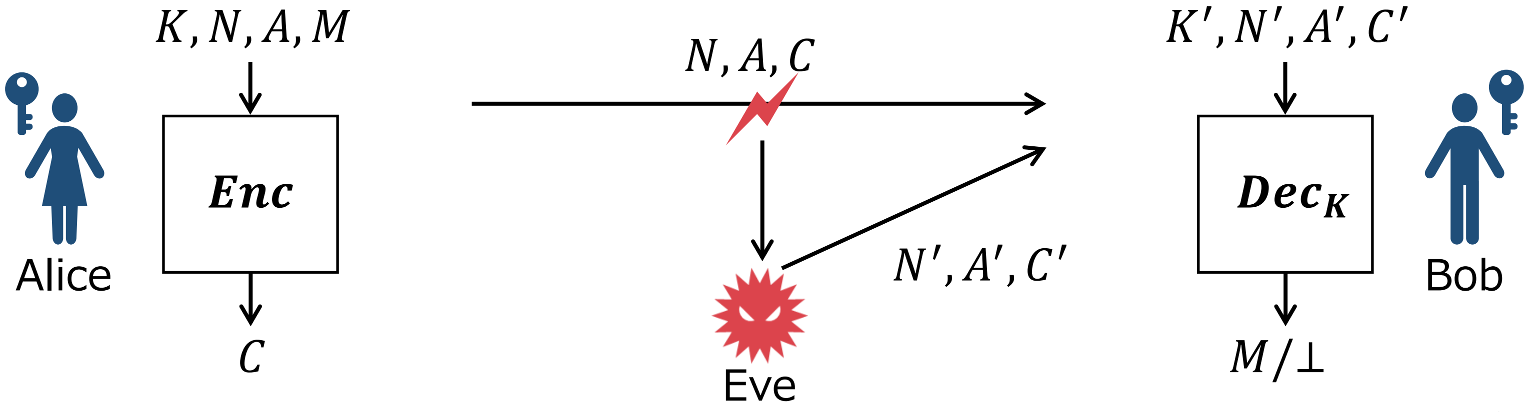
Yu Long Chen[*1], Antonio Flórez-Gutiérrez[*2], **Akiko Inoue**[*3], Ryoma Ito[*4], Tetsu Iwata[*5], Kazuhiko Minematsu[*3], Nicky Mouha[*6], Yusuke Naito[*7], Ferdinand Sibleyras[*2], Yosuke Todo[*2]

*1: imec-COSIC, KU Leuven, *2: NTT Social Informatics Laboratories, *3: NEC Corporation,
*4: National Institute of Information and Communications Technology, *5: Nagoya University,
*6: Strativia, *7: Mitsubishi Electric Corporation

FSE 2024 Leuven Belgium, 25 March 2024

AEAD: Authenticated Encryption with Associated Data

- Symmetric key cryptosystem to provide privacy & authenticity [Rog02]
  - K: key, N: nonce, M: plaintext, A: associated data (AD), C: ciphertext (including tag)
  - Encryption: $Enc(K, N, A, M) = C$
  - Decryption: $Dec(K, N, A, C) = M$ when inputs are authentic, otherwise returns $\perp$
- Security
  - Basic: privacy & authenticity
  - Advanced: nonce-misuse/decryption-misuse resistant, **Key Committing Security**



Key committing security (KCS) for AEAD

- KCS: guarantee that ciphertext is a commitment of K
  - Evaluated by collision resistance of Enc
  - Adversary chooses K
  - Standard security notions (PRIV/AUTH) do not capture KCS

- Increased demand by attacks exploiting non-KC-secure AEAD
  - Attack on message franking [DGRW18]:
    message receiver cannot report delivered picture as abuse
  - Partitioning oracle attack [LGR21]:
    narrowing down the range of the passwords stored in servers
  - Other attacks: SFrame [IIM21], Subscribe with Google [ADG+22], ⋯
  - Ongoing NIST accordion cipher project includes KCS as one example of desired security

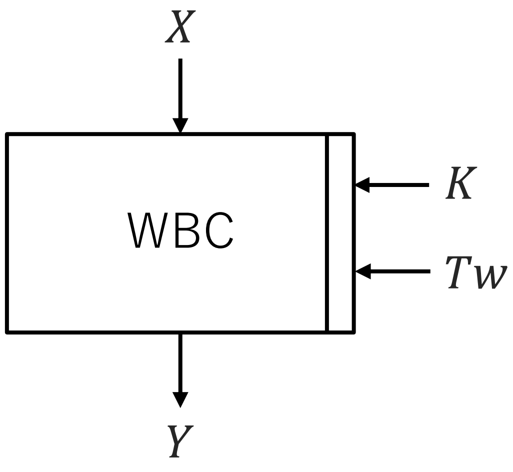
Definitions for KCS

- We follow the definitions by Bellare and Hoang [BH22]
  - Other related definitions: Complete Robustness [FOR17], sender/receiver binding [GLR17], Context discovery [MLGR23], ⋯

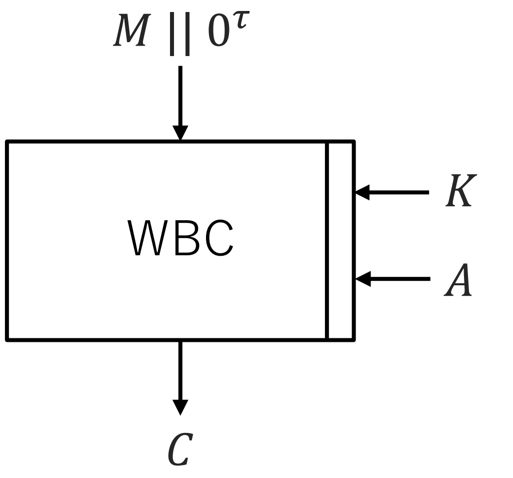
- An adversary is computationally hard to find two inputs of Enc that have the same ciphertext under:
  - CMT-1: different keys
  - CMT-3: different (K, N, A) pairs
  - CMT-4: different (K, N, A, M) pairs
  - CMT-3 is equivalent to CMT-4 [BH22]

Encode-then-Encipher via Wide-block cipher

- (Tweakable) Wide block cipher (WBC)
  - IN: secret key, plaintext w/ variable length, and tweak w/ variable length
  - OUT: ciphertext w/ same length as plaintext
  - WBC itself is not AEAD, but it can be converted to AEAD by Encode-then-Encipher

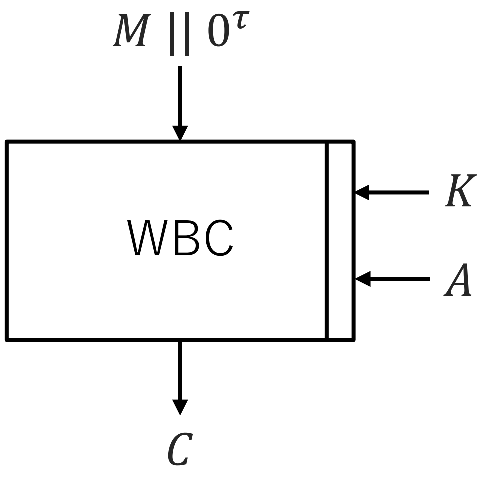


- Encode-then-Encipher (EtE) [BR00]
  - underlying primitive: WBC
  - Enc: encode an input message (ex. append/prepend 0^τ) and encipher with a WBC
  - Dec: decipher ciphertext and check whether deciphered string follows the encoding rule → If it is OK, return decoded string



Security of EtE

- EtE is Robust AE; resists nonce misuse and decryption misuse
- No KCS analysis on concrete EtE schemes
  - Existing studies focus on NAE and MRAE
    - GCM, CCM, ChaCha20-Poly1305, SIV, GCM-SIV, ⋯
- Ideal: τ-bit KCS when assuming WBC is an ideal cipher (IC) and C is long enough [GLR17]
  - Generic CMT-1/4 attack: $O(2^{\tau})$
  - Try decryption with fixed C and distinct (K, A) until the decrypted value has 0^{τ}
- **In practice: WBC is not behaving as IC (built on smaller primitives)**



Our results

- We study key committing security of
  - **AEZ [HKR15]** ··· Popular AEAD with lots of cryptanalysis, and CAESAR 3rd round candidate
    - Zero-appending is specified
  - **EtE-Adiantum [CB18]** ··· Adiantum: Designed by Google, widely deployed in actual devices
    - Prepend and append with zeros
  - **EtE-HCTR2 [CHB21]** ··· HCTR2: deployed in Android file-based encryption
    - Prepend and append with zeros

Scheme	CMT-1 A	CMT-1 P	CMT-4 (A & P)	Proof
general AEZ	$O(2^{n/2})$	(not specified)	$O(1)$	$n/2$ (Sect. 7.1)
full-spec AEZ	2^{27}	(not specified)	$O(1)$	—
EtE-Adiantum	$O(2^{n/2})$	$O(2^{n/2})$	$O(1)$	$n/2$ (Sect. 7.2)
EtE-HCTR2	$O(2^{n/2})$	$O(2^{n/2})$	$O(1)$	—

$n = \tau$, n is input/output size of underlying BC

Our results

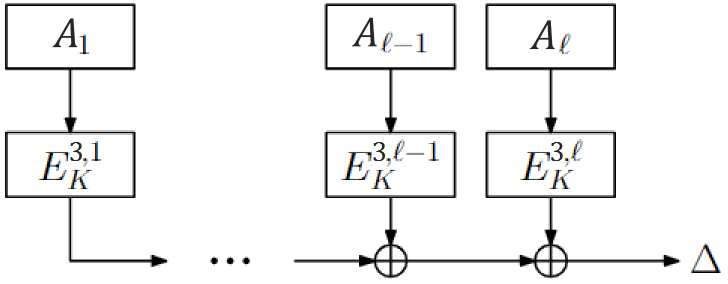
- We study key committing security of
  - **AEZ [HKR15]** ··· Popular AEAD with lots of cryptanalysis, and CAESAR 3rd round candidate
    - Zero-appending is specified
  - **EtE-Adiantum [CB18]** ··· Adiantum: Designed by Google, widely deployed in actual devices
    - Prepend and append with zeros
  - **EtE-HCTR2 [CHB21]** ··· HCTR2: deployed in Android file-based encryption
    - Prepend and append with zeros

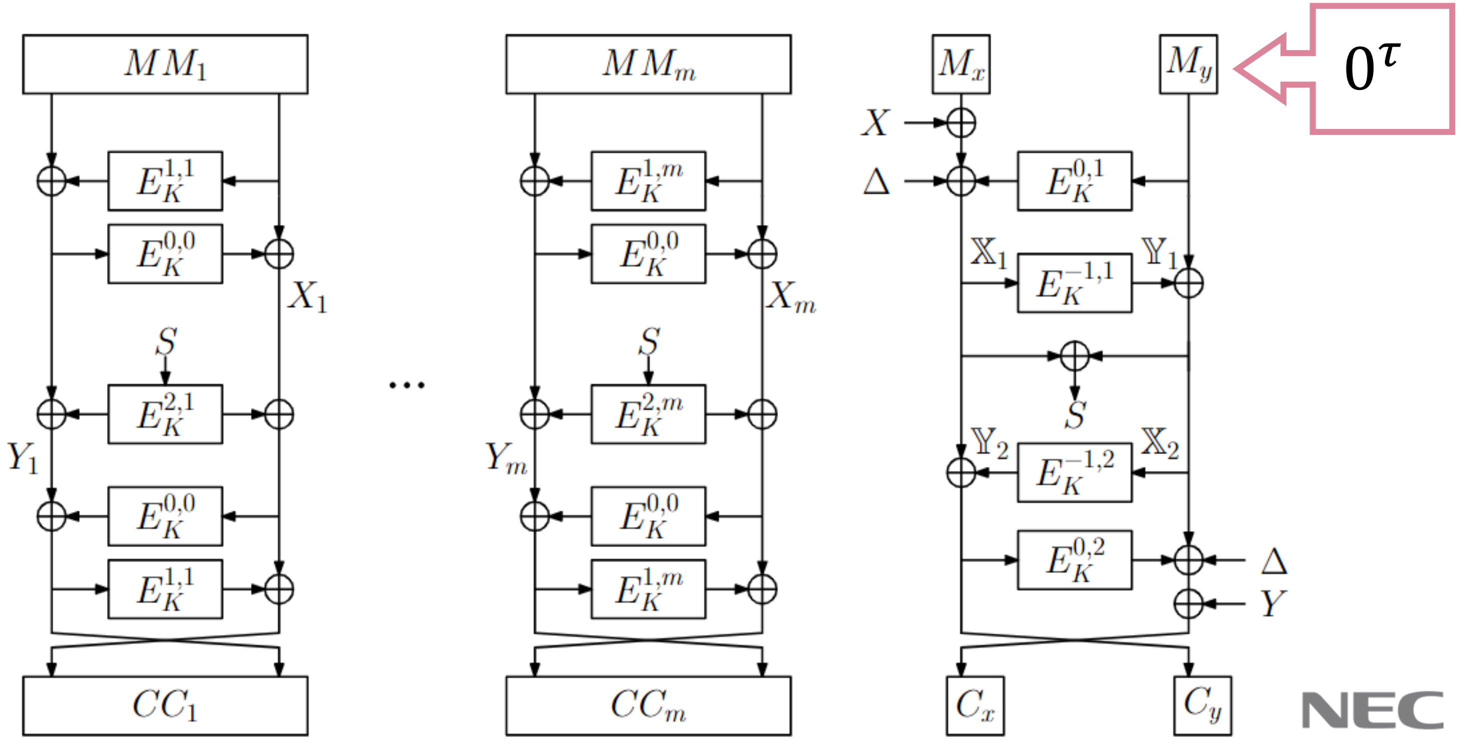
	Scheme	CMT-1 A	CMT-1 P	CMT-4 (A & P)	Proof
This talk	general AEZ	$O(2^{n/2})$	(not specified)	$O(1)$	$n/2$ (Sect. 7.1)
This talk	full-spec AEZ	2^{27}	(not specified)	$O(1)$	—
	EtE-Adiantum	$O(2^{n/2})$	$O(2^{n/2})$	$O(1)$	$n/2$ (Sect. 7.2)
	EtE-HCTR2	$O(2^{n/2})$	$O(2^{n/2})$	$O(1)$	—

$n = \tau$, n is input/output size of underlying BC

AEZ [Hoang, Krovetz, Rogaway@EC15]

- EtE using n-bit TBC $E_K^{i,j}$
  - Encodes M by concatenating 0^τ at the end of M ($\tau \leq n$, M_y includes 0^τ)
  - Enciphering way changes depending on input length (including 0^τ)
  - Input length ≥ 256 bits: AEZ-core (Fig.; our target), otherwise: AEZ-tiny (out of scope)
  - AEZ-core: 4 or 5-round Feistel with PHASH-like AD processing
- Proof-then-prune strategy: proving its security assuming TBC is TPRP then pruning TBC cost
  - Reducing # rounds of TBC
  - Using simpler key schedule

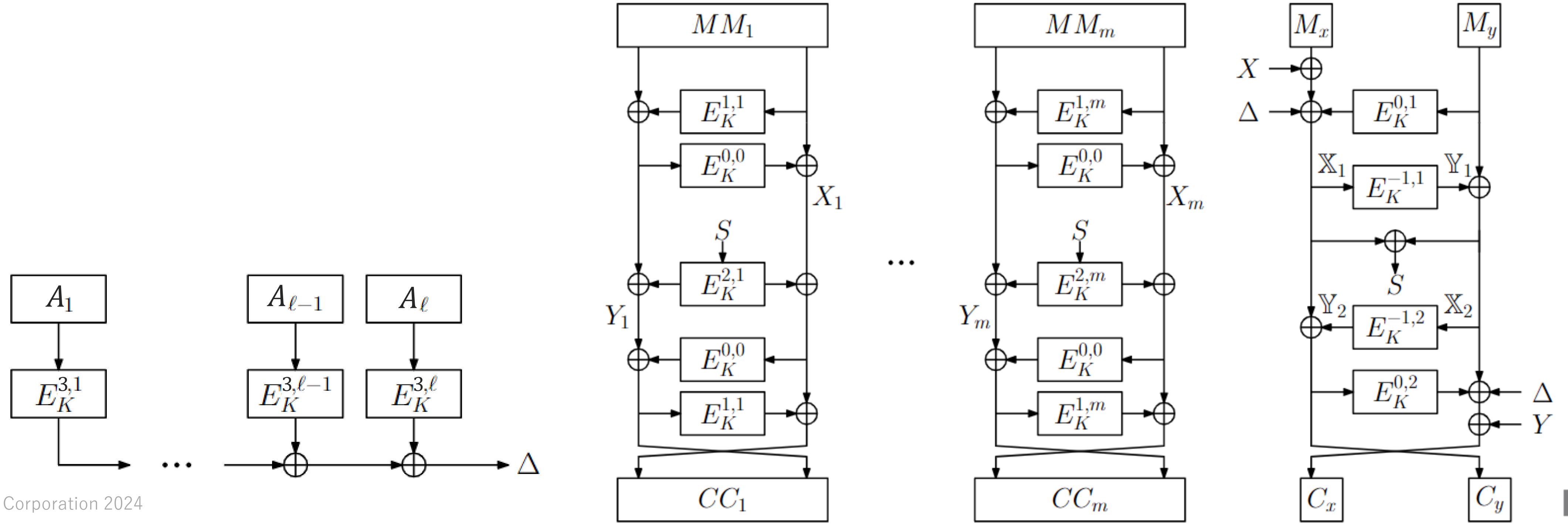




NEC

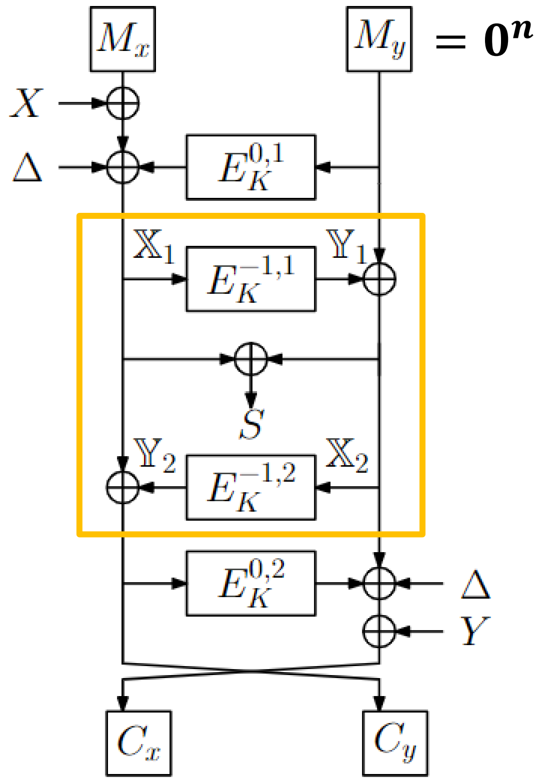
CMT-4 attack on AEZ

- Recall: CMT-4 adv. tries to find distinct $(K, N, A, M), (K', N', A', M')$ s.t. $Enc(K, N, A, M) = Enc(K', N', A', M')$
  - Assuming $(K, N, M) = (K', N', M')$
  - Adv. wins if it invokes a collision of Δ for distinct A, A'
  - It is easy since adv. knows K, K', and it can invert TBC $\Rightarrow O(1)$ CMT-4 attack



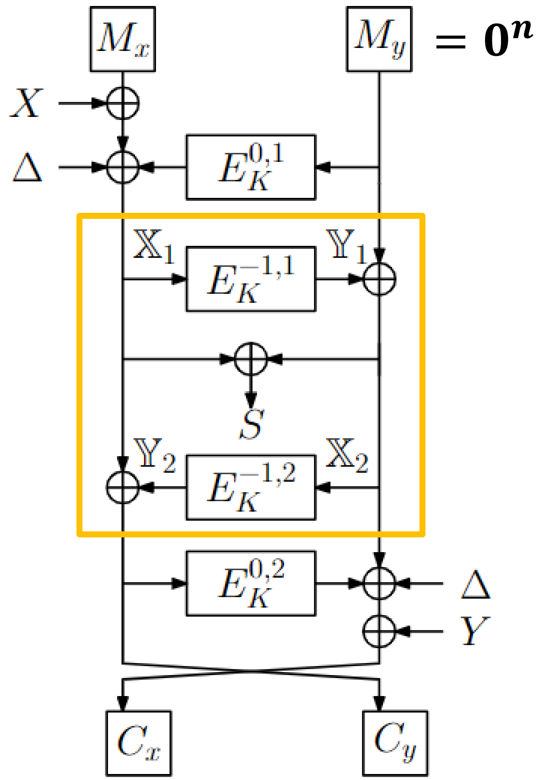
CMT-1 attack & proof on general AEZ ($\tau = n$)

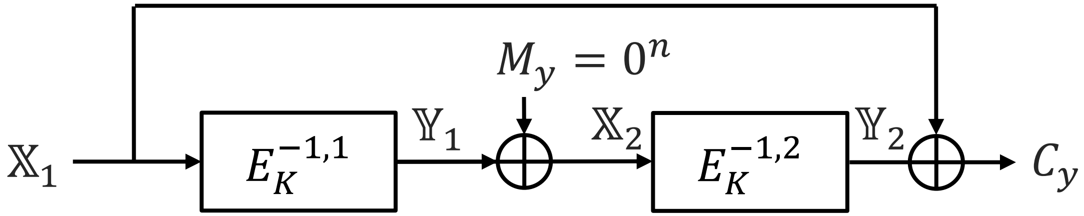
- General AEZ: assuming the ideal TBC
- Strategy: focusing on ▭ in the last Feistel i.e., C_y collision
  - Once getting C_y collision, it is easy to get collisions on other ciphertexts (omit the details)



CMT-1 attack & proof on general AEZ ($\tau = n$)

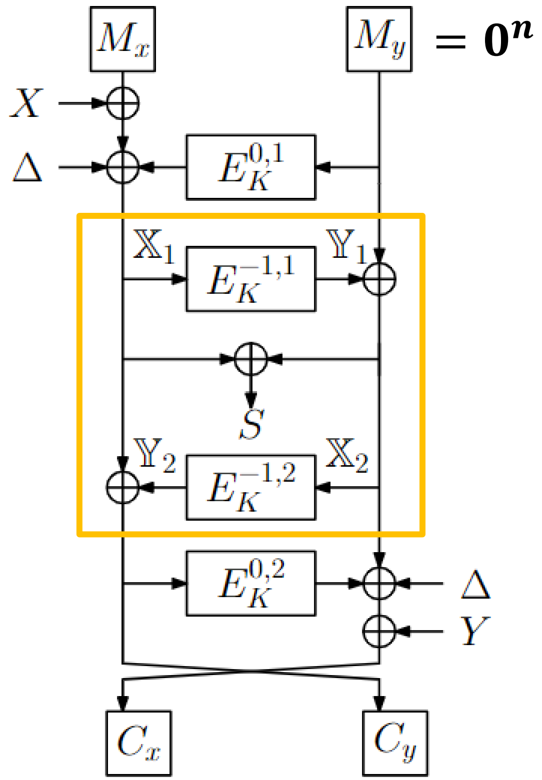
- General AEZ: assuming the ideal TBC
- Strategy: focusing on □ in the last Feistel i.e., C_y collision
  - Once getting C_y collision, it is easy to get collisions on other ciphertexts (omit the details)
- Assume $\tau = n \Rightarrow M_y = 0^n$
  - □ can be viewed as Davies-Meyer (DM) construction

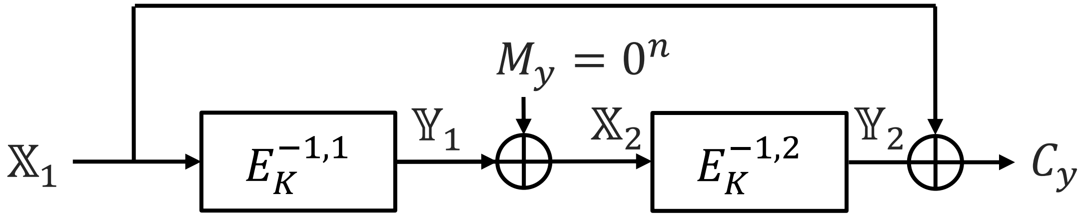




CMT-1 attack & proof on general AEZ ($\tau = n$)

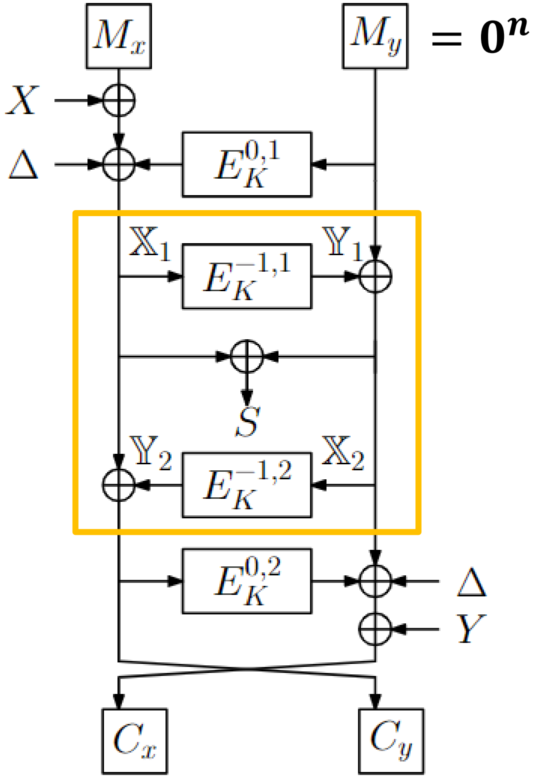
- General AEZ: assuming the ideal TBC
- Strategy: focusing on [ ] in the last Feistel i.e., C_y collision
  - Once getting C_y collision, it is easy to get collisions on other ciphertexts (omit the details)
- Assume $\tau = n \Rightarrow M_y = 0^n$
  - [ ] can be viewed as Davies-Meyer (DM) construction
  - As in the usual DM, a coll. Attack works in $O(2^{n/2})$
    - Search $(\mathbb{X}_1, \mathbb{Y}_2)$ and $(\mathbb{X}_1', \mathbb{Y}_2')$ s.t. $\mathbb{X}_1 \oplus \mathbb{X}_1' = \mathbb{Y}_2 \oplus \mathbb{Y}_2'$

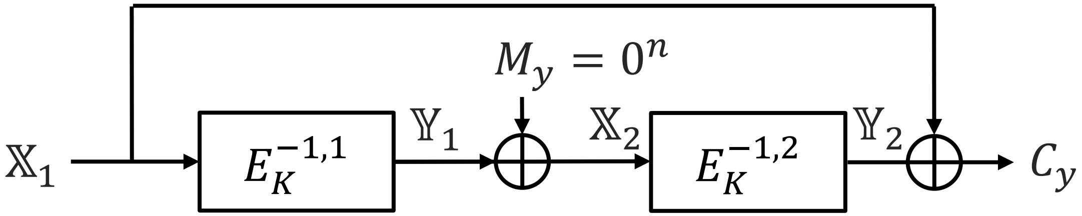




CMT-1 attack & proof on general AEZ ($\tau = n$)

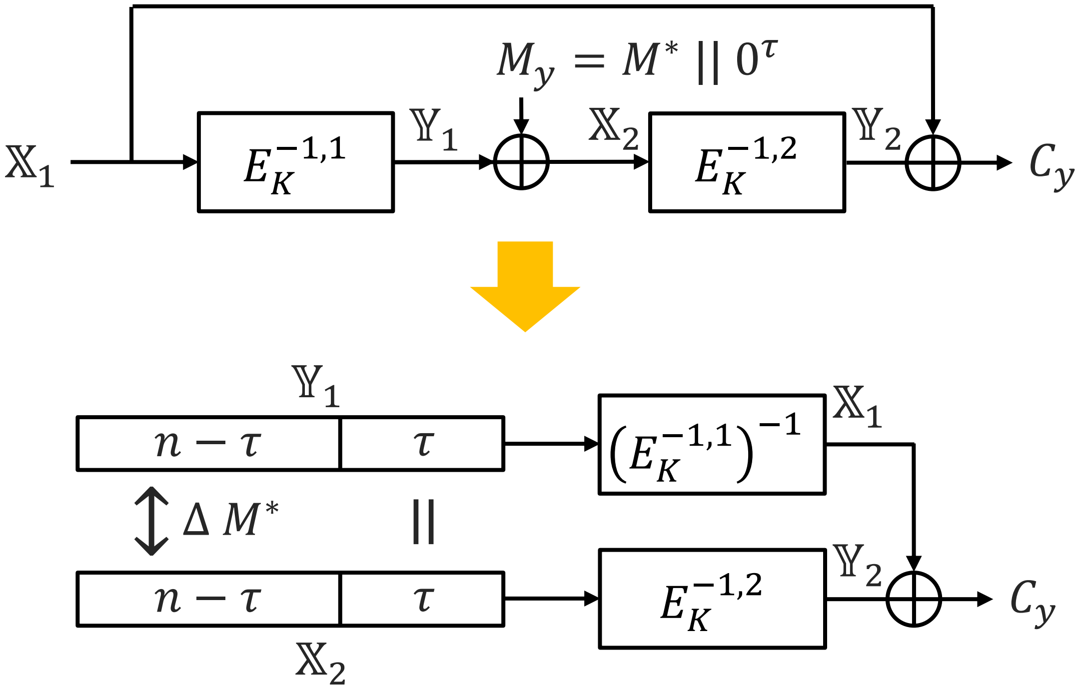
- General AEZ: assuming the ideal TBC
- Strategy: focusing on [ ] in the last Feistel i.e., C_y collision
  - Once getting C_y collision, it is easy to get collisions on other ciphertexts (omit the details)
- Assume $\tau = n \Rightarrow M_y = 0^n$
  - [ ] can be viewed as Davies-Meyer (DM) construction
  - As in the usual DM, a coll. Attack works in $O(2^{n/2})$
    - Search $(\mathbb{X}_1, \mathbb{Y}_2)$ and $(\mathbb{X}'_1, \mathbb{Y}'_2)$ s.t. $\mathbb{X}_1 \oplus \mathbb{X}'_1 = \mathbb{Y}_2 \oplus \mathbb{Y}'_2$
  - Also, we can prove that it is tight
    - Bellare and Hoang prove DM's collision resistance in IC model. Ours is almost the same. [BH22]
    - We have two consecutive TBCs, but it is not a problem.





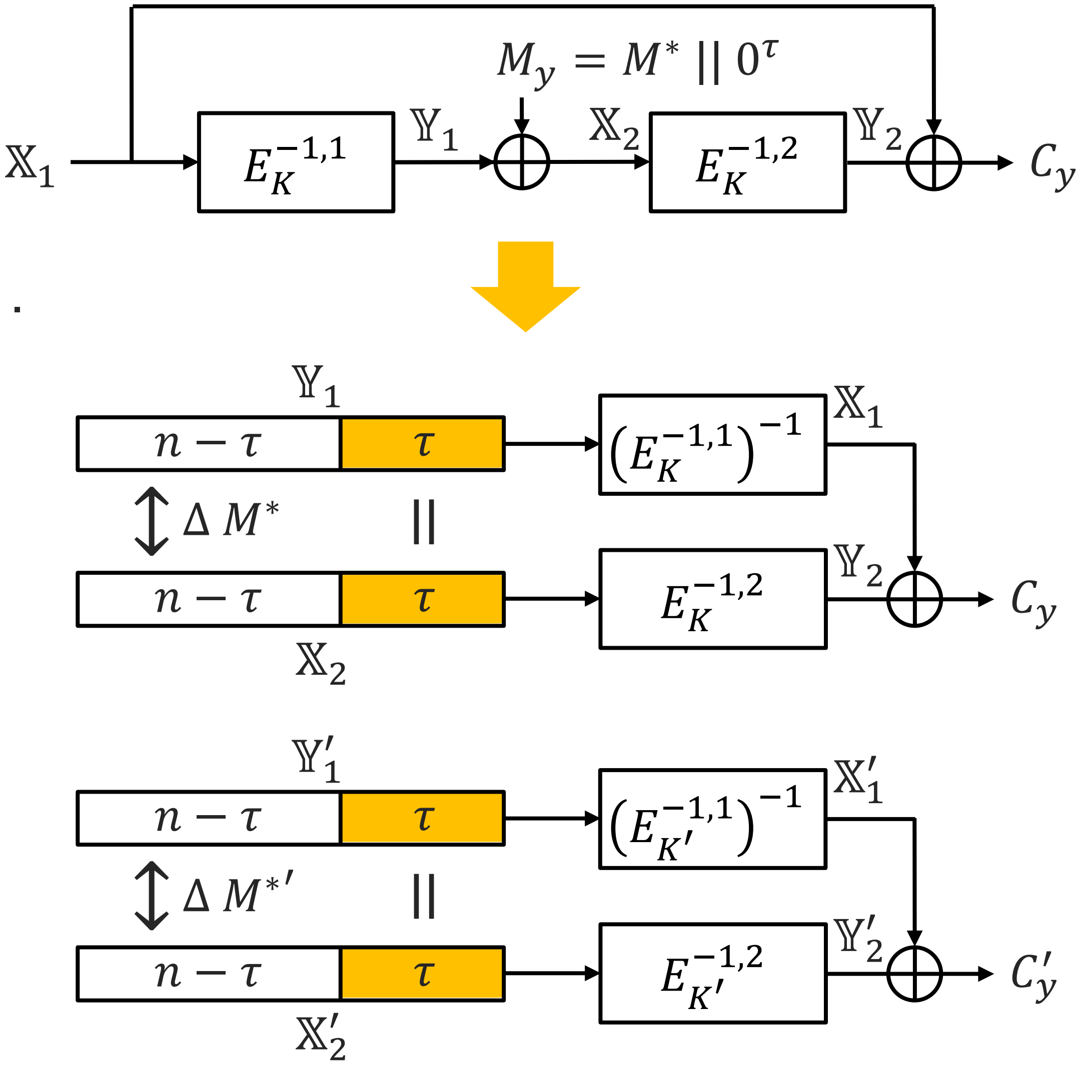
CMT-1 attack on general AEZ ($\tau < n$)

- Reduce C_y coll. to a generalized birthday problem
  - $\tau < n \Rightarrow M_y = M^* \,||\, 0^\tau$
  - DM-like const. becomes the sum of 2 TBCs, where $\mathrm{lsb}_\tau(\mathbb{Y}_1) = \mathrm{lsb}_\tau(\mathbb{X}_2)$ must hold



CMT-1 attack on general AEZ ($\tau < n$)

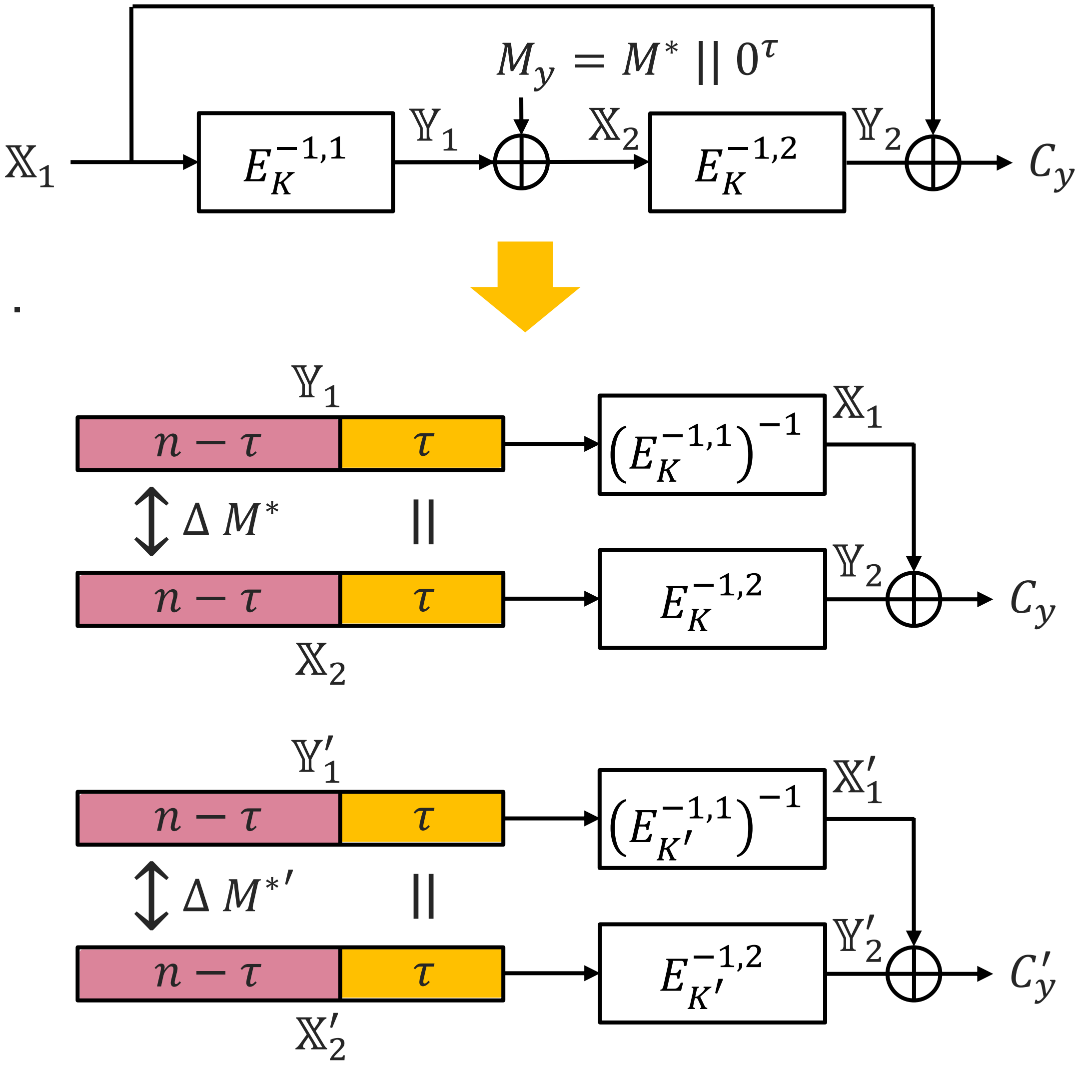
- Reduce C_y coll. to a generalized birthday problem
  - $\tau < n \Rightarrow M_y = M^* \,||\, 0^\tau$
  - DM-like const. becomes the sum of 2 TBCs, where $\mathrm{lsb}_\tau(\mathbb{Y}_1) = \mathrm{lsb}_\tau(\mathbb{X}_2)$ must hold
  - Pick up any distinct keys K, K' and fix values in [yellow box].



CMT-1 attack on general AEZ ($\tau < n$)

- Reduce C_y coll. to a generalized birthday problem
  - $\tau < n \Rightarrow M_y = M^* \,||\, 0^\tau$
  - DM-like const. becomes the sum of 2 TBCs, where $\mathrm{lsb}_\tau(\mathbb{Y}_1) = \mathrm{lsb}_\tau(\mathbb{X}_2)$ must hold
  - Pick up any distinct keys K, K' and fix values in .
  - Search $\mathbb{X}_1, \mathbb{Y}_2, \mathbb{X}'_1, \mathbb{Y}'_2$ s.t. $\mathbb{X}_1 \oplus \mathbb{Y}_2 \oplus \mathbb{X}'_1 \oplus \mathbb{Y}'_2 = 0$ by changing values in .
    - Diff. can be canceled by M^*

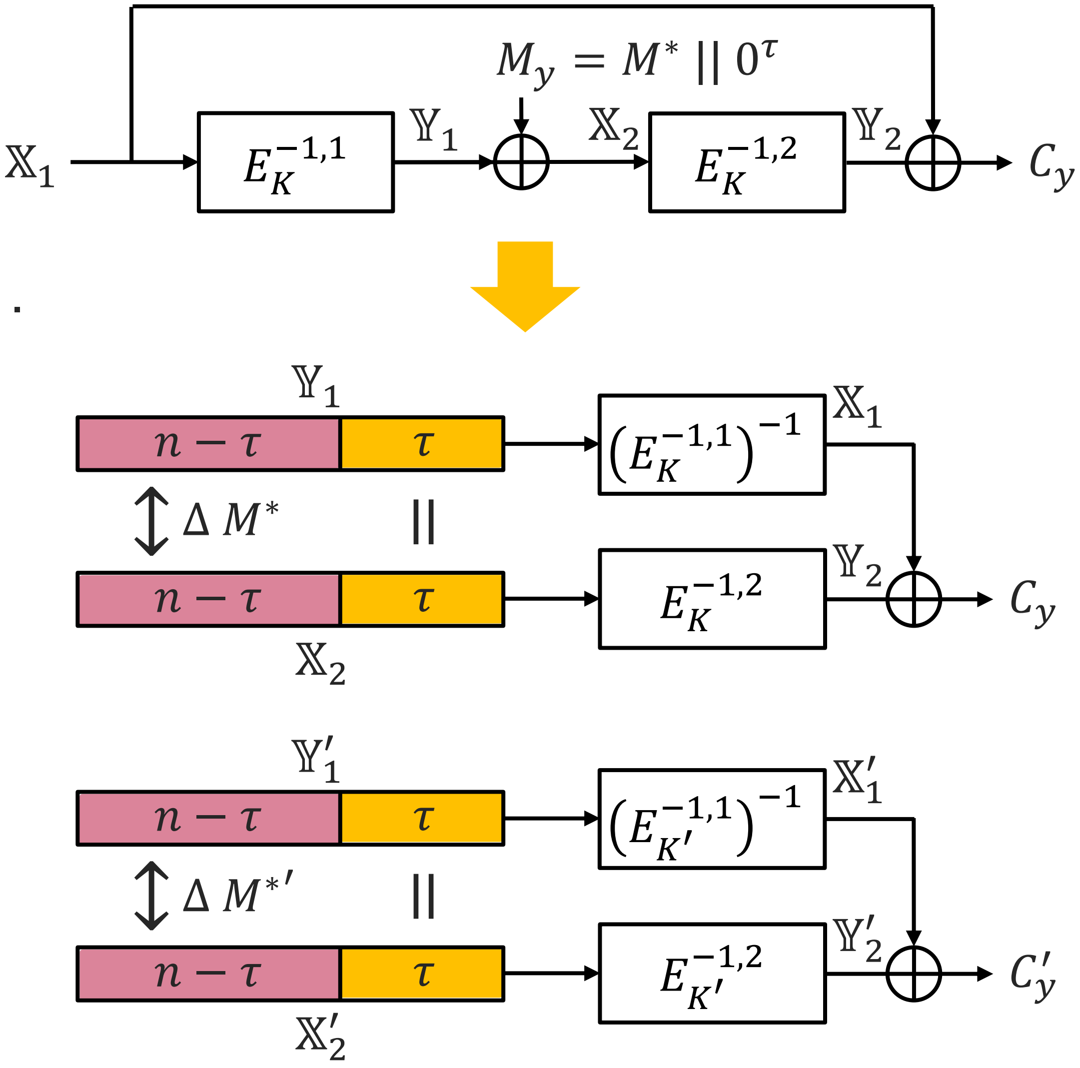
$\Rightarrow$ Generalized birthday problem with 4 lists



CMT-1 attack on general AEZ ($\tau < n$)

- Reduce C_y coll. to a generalized birthday problem
  - $\tau < n \Rightarrow M_y = M^* \,||\, 0^\tau$
  - DM-like const. becomes the sum of 2 TBCs, where $\mathrm{lsb}_\tau(\mathbb{Y}_1) = \mathrm{lsb}_\tau(\mathbb{X}_2)$ must hold
  - Pick up any distinct keys K, K' and fix values in [yellow].
  - Search $\mathbb{X}_1, \mathbb{Y}_2, \mathbb{X}_1', \mathbb{Y}_2'$ s.t. $\mathbb{X}_1 \oplus \mathbb{Y}_2 \oplus \mathbb{X}_1' \oplus \mathbb{Y}_2' = 0$ by changing values in [pink].
    - Diff. can be canceled by M^*

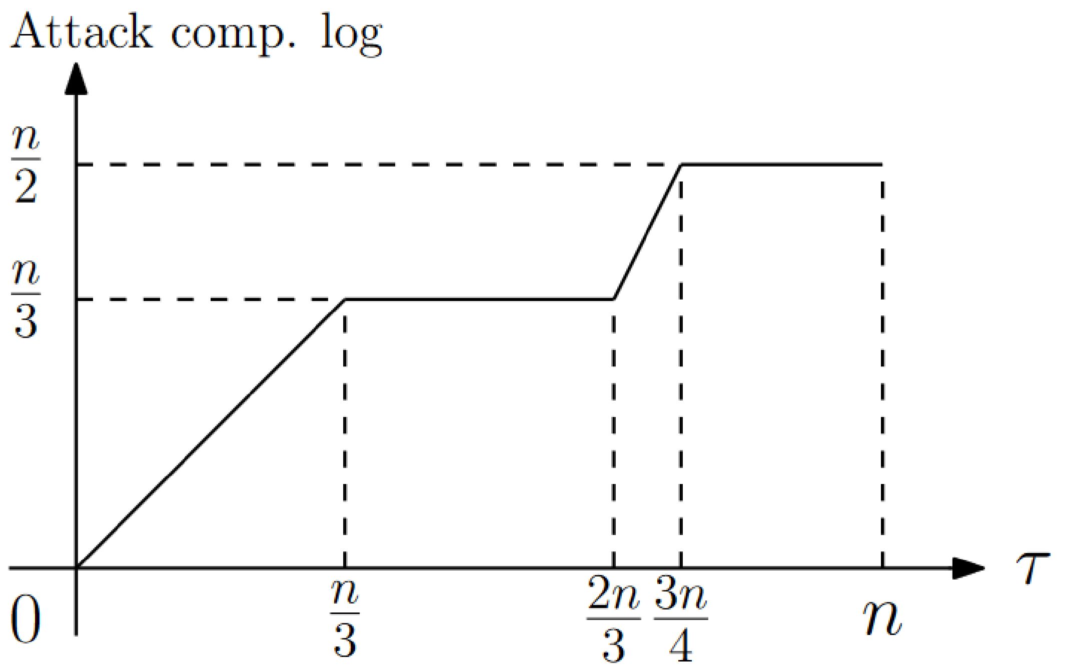
  $\Rightarrow$ Generalized birthday problem with 4 lists
- Solution: k-tree algorithm ($k = 4$)
  - Comp. : $O(2^{n/3})$ but each list needs $\mathbf{2^{n/3}}$ elements
  - Possible when $\tau \leq 2n/3$



CMT-1 attack on general AEZ ($2n/3 < \tau < n$)

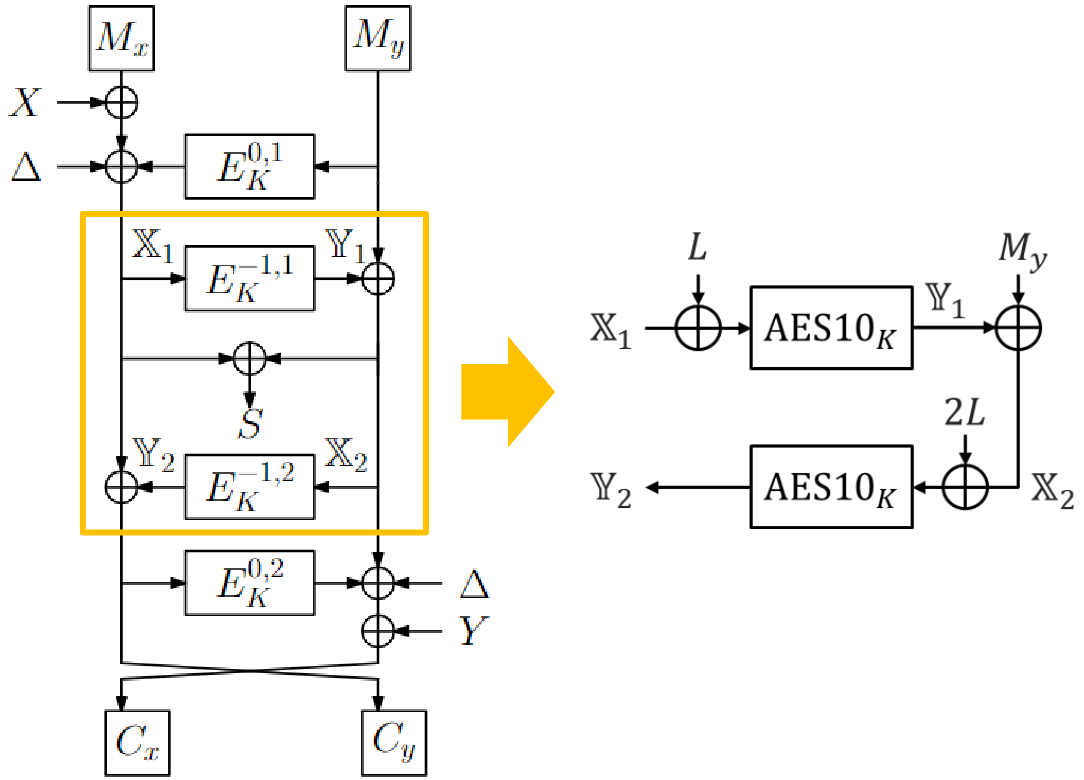
- When we cannot prepare enough values for $\mathbb{X}_1, \mathbb{Y}_2, \mathbb{X}_1', \mathbb{Y}_2'$, the success of 4-tree alg. becomes probabilistic.
  - Repeat 4-tree alg. with less elements of each list until success
  - 4-tree alg. with $O(2^{n-\tau})$ elements: success prob. is $O(2^{2n-3\tau})$
  - Comp.: $O(2^{n-\tau}) \times O(2^{3\tau-2n}) = O(2^{2\tau-n})$

- Summary of general AEZ
  - $0 \leq \tau \leq n/3$: Generic attack $\cdots$ $O(2^{\tau})$
  - $n/3 \leq \tau \leq 2n/3$: 4-tree alg. $\cdots$ $O\left(2^{n/3}\right)$
  - $2n/3 \leq \tau \leq 3n/4$: Repeated 4-tree alg. $\cdots$ $O(2^{2\tau-n})$
  - $3n/4 \leq \tau \leq n$: Attack on DM $\cdots$ $O\left(2^{n/2}\right)$
  - Tight when $\tau = n$



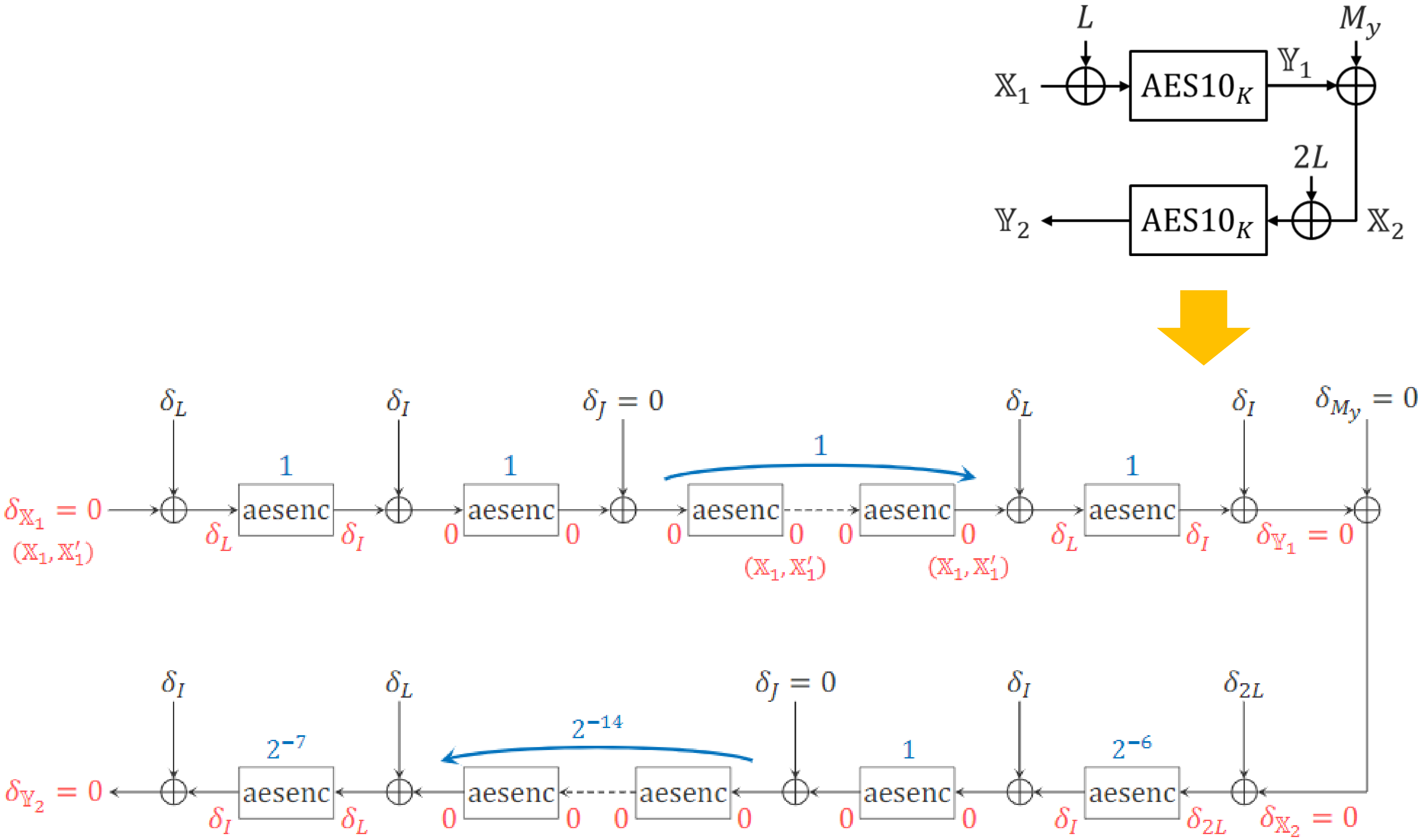
CMT-1 attack on full-spec AEZ

- Full-spec AEZ: TBC follows the full specification of AEZ
- Same strategy as the general AEZ attack: focusing on ☐ i.e., C_y collision
- TBC: XE-style TBC using $\mathbf{AES10}$
  - Assuming $|K| = 384$ (default), and $L \,||\, I \,||\, J \overset{128}{\longleftarrow} K$
  - $E_K^{-1,i}(X) = \mathrm{AES10}_K(X \oplus i \cdot L)$
  - $\mathrm{AES10}$: 10-round AES, but ..
  - **Last round has MixColumns, unlike usual AES**
  - **Round subkeys:** $(\boldsymbol{I, J,\ L, I, J,\ L, I, J,\ L, I})$



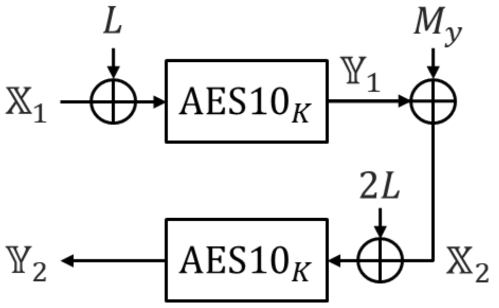
Attack detail

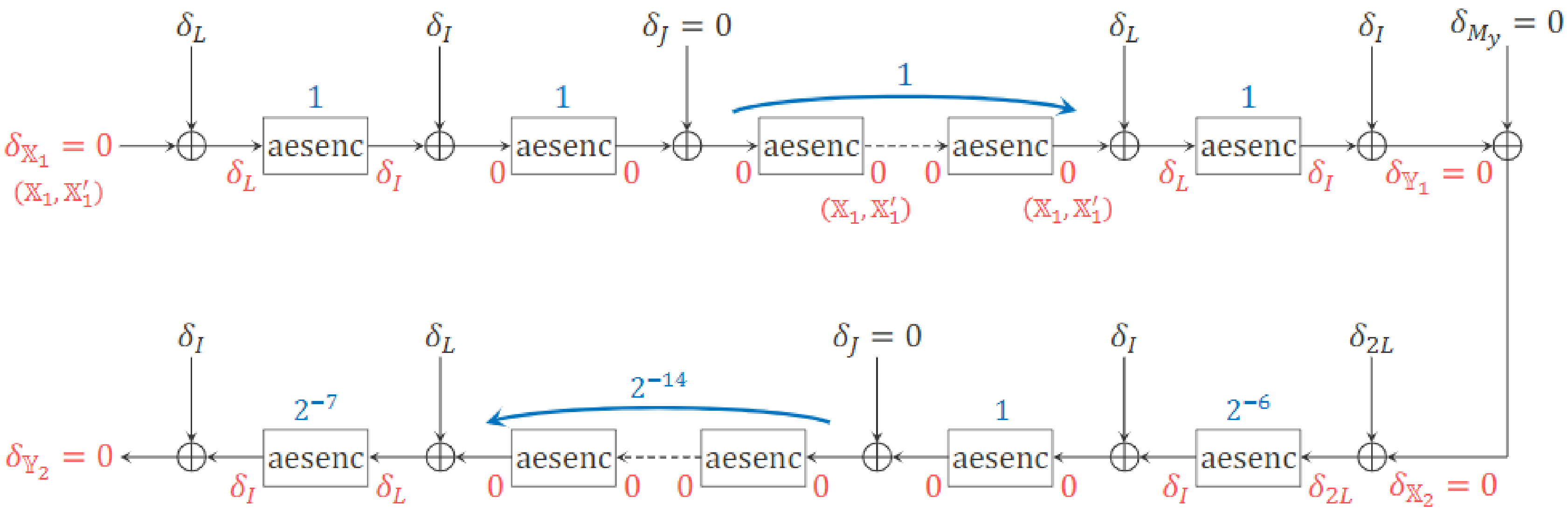
- Find $K = I \,||\, J \,||\, L,\ K' = I' \,||\, J' \,||\, L'$, s.t. $(\delta_{\mathbb{X}_1}, \delta_{\mathbb{Y}_1}, \delta_{\mathbb{X}_2}, \delta_{\mathbb{Y}_2}) = (0,0,0,0)$ $(\delta_{\mathbb{X}_1} = \mathbb{X}_1 \oplus \mathbb{X}'_1)$



Attack detail

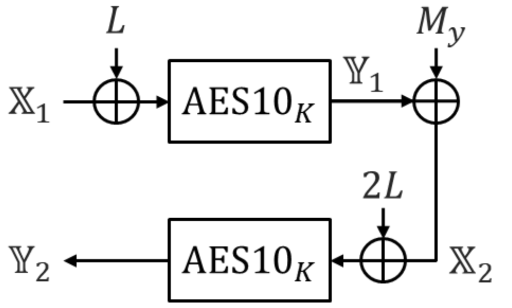
- Find $K = I \,||\, J \,||\, L,\ K' = I' \,||\, J' \,||\, L'$, s.t. $(\delta_{\mathbb{X}_1}, \delta_{\mathbb{Y}_1}, \delta_{\mathbb{X}_2}, \delta_{\mathbb{Y}_2}) = (0,0,0,0)$ $(\delta_{\mathbb{X}_1} = \mathbb{X}_1 \oplus \mathbb{X}'_1)$
  - Set $\delta_{\mathbb{X}_1} = 0$, and set δ_L so that δ_L and δ_{2L} have only 1 active S-box
  - Set δ_I to cancel out diff. propagation caused by δ_L and δ_{2L}

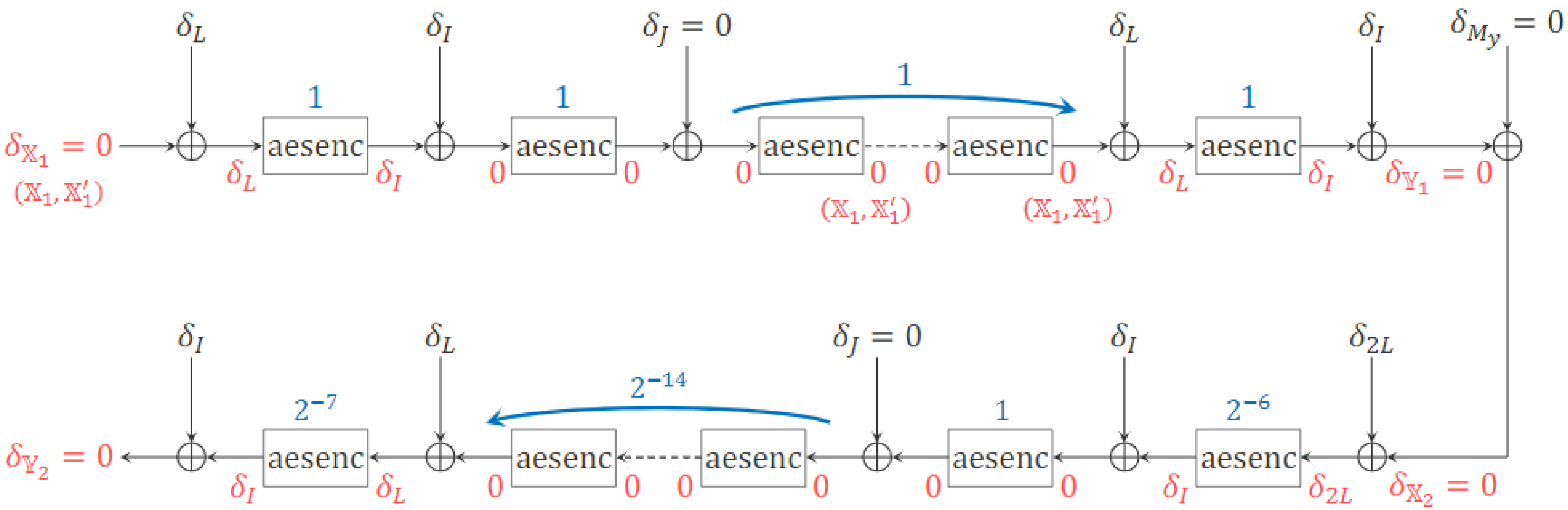




Attack detail

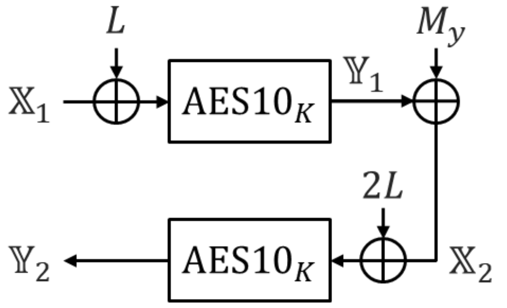
- Find $K = I \,||\, J \,||\, L,\ K' = I' \,||\, J' \,||\, L'$, s.t. $(\delta_{\mathbb{X}_1}, \delta_{\mathbb{Y}_1}, \delta_{\mathbb{X}_2}, \delta_{\mathbb{Y}_2}) = (0, 0, 0, 0)$ $(\delta_{\mathbb{X}_1} = \mathbb{X}_1 \oplus \mathbb{X}_1')$
  - Set $\delta_{\mathbb{X}_1} = 0$, and set δ_L so that δ_L and δ_{2L} have only 1 active S-box
  - Set δ_I to cancel out diff. propagation caused by δ_L and δ_{2L}
  - Set J, J' so that **3rd aesenc outputs go back to $\mathbb{X}_1, \mathbb{X}_1'$** (here, $\delta_J = 0$)

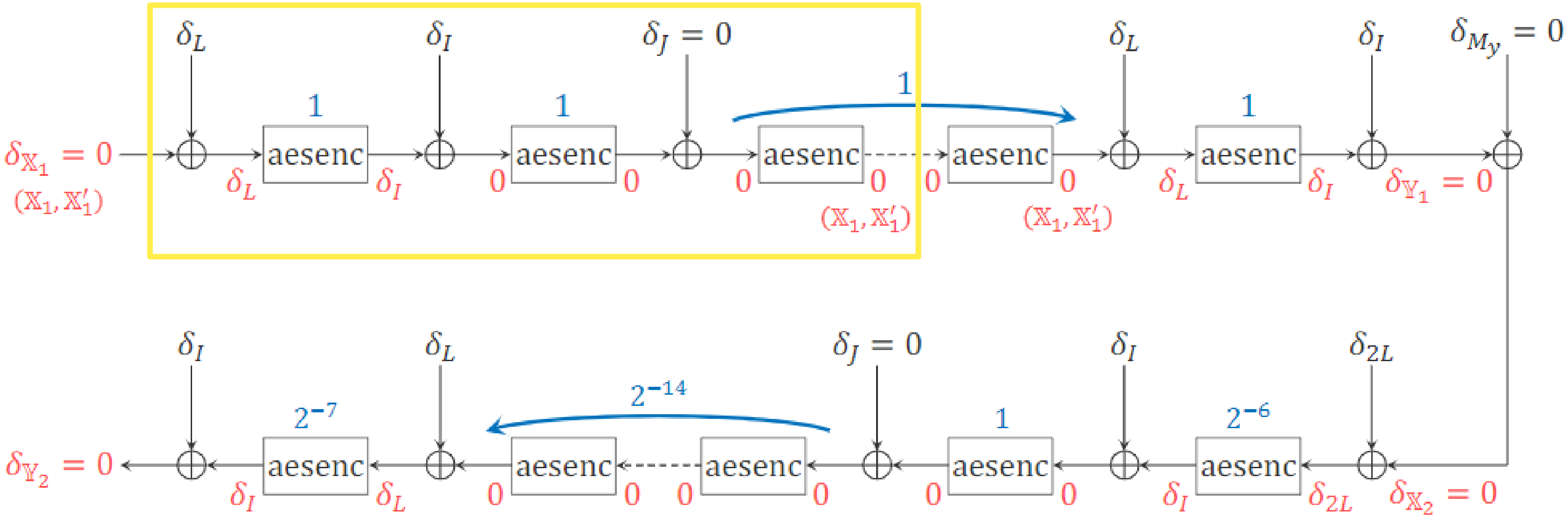




Attack detail

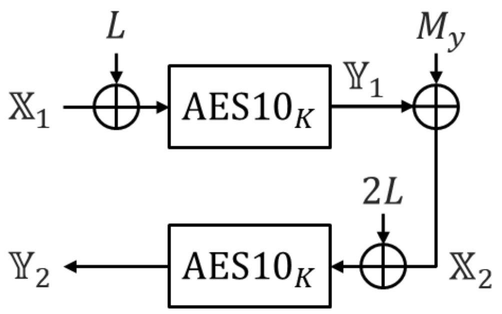
- Find $K = I \,||\, J \,||\, L,\ K' = I' \,||\, J' \,||\, L'$, s.t. $(\delta_{\mathbb{X}_1}, \delta_{\mathbb{Y}_1}, \delta_{\mathbb{X}_2}, \delta_{\mathbb{Y}_2}) = (0,0,0,0)$ $(\delta_{\mathbb{X}_1} = \mathbb{X}_1 \oplus \mathbb{X}_1')$
  - Set $\delta_{\mathbb{X}_1} = 0$, and set δ_L so that δ_L and δ_{2L} have only 1 active S-box
  - Set δ_I to cancel out diff. propagation caused by δ_L and δ_{2L}
  - Set J, J' so that **3rd aesenc outputs go back to $\mathbb{X}_1, \mathbb{X}_1'$** (here, $\delta_J = 0$)
  - 3 aesenc with (L, I, J) and (L', I', J') maps $\mathbb{X}_1$ to $\mathbb{X}_1$ $\Rightarrow$ **$\delta_{\mathbb{Y}_1} = 0$ w/ prob. 1**

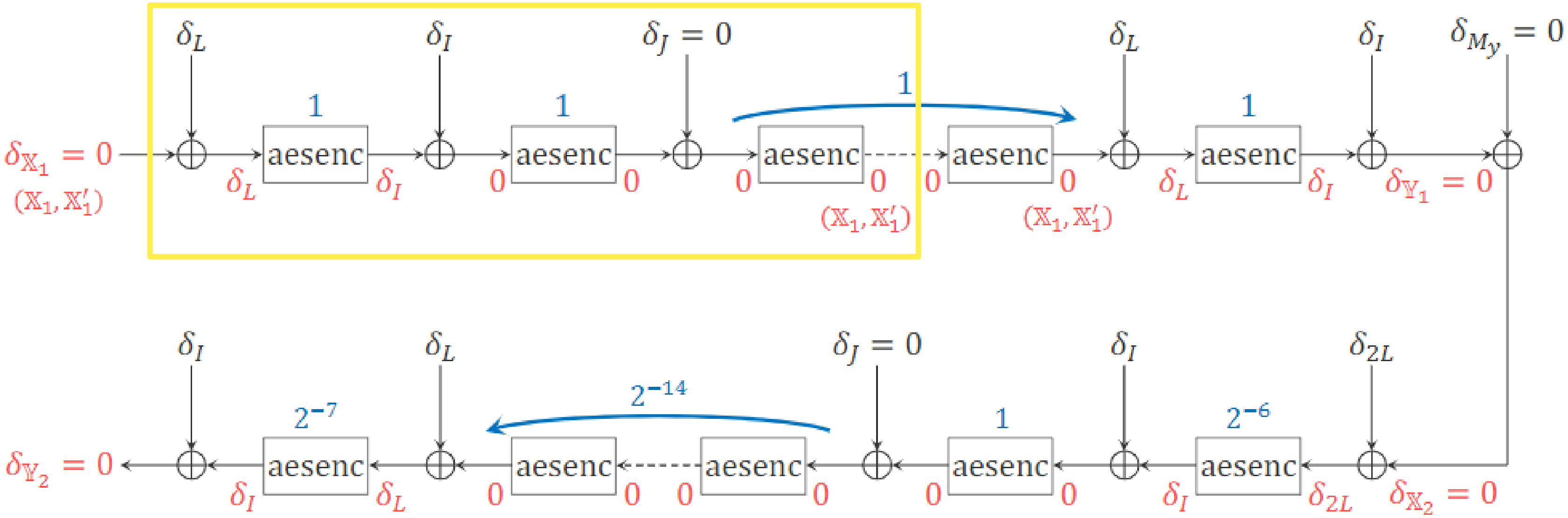




Attack detail

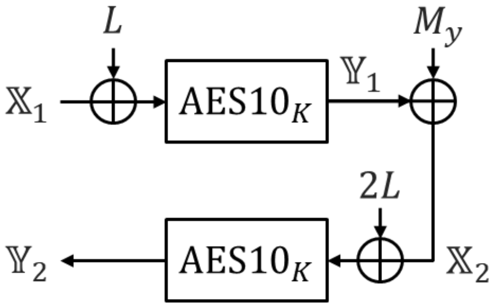
- Find $K = I \,||\, J \,||\, L$, $K' = I' \,||\, J' \,||\, L'$, s.t. $(\delta_{\mathbb{X}_1}, \delta_{\mathbb{Y}_1}, \delta_{\mathbb{X}_2}, \delta_{\mathbb{Y}_2}) = (0,0,0,0)$ $(\delta_{\mathbb{X}_1} = \mathbb{X}_1 \oplus \mathbb{X}_1')$
  - Set $\delta_{\mathbb{X}_1} = 0$, and set δ_L so that δ_L and δ_{2L} have only 1 active S-box
  - Set δ_I to cancel out diff. propagation caused by δ_L and δ_{2L}
  - Set J, J' so that **3rd aesenc outputs go back to $\mathbb{X}_1, \mathbb{X}_1'$** (here, $\delta_J = 0$)
  - 3 aesenc with (L, I, J) and (L', I', J') maps $\mathbb{X}_1$ to $\mathbb{X}_1$ $\Rightarrow$ **$\delta_{\mathbb{Y}_1} = 0$ w/ prob. 1**
  - Set $\delta_{M_y} = 0 \rightarrow \delta_{\mathbb{X}_2} = \delta_{\mathbb{Y}_1} = 0$

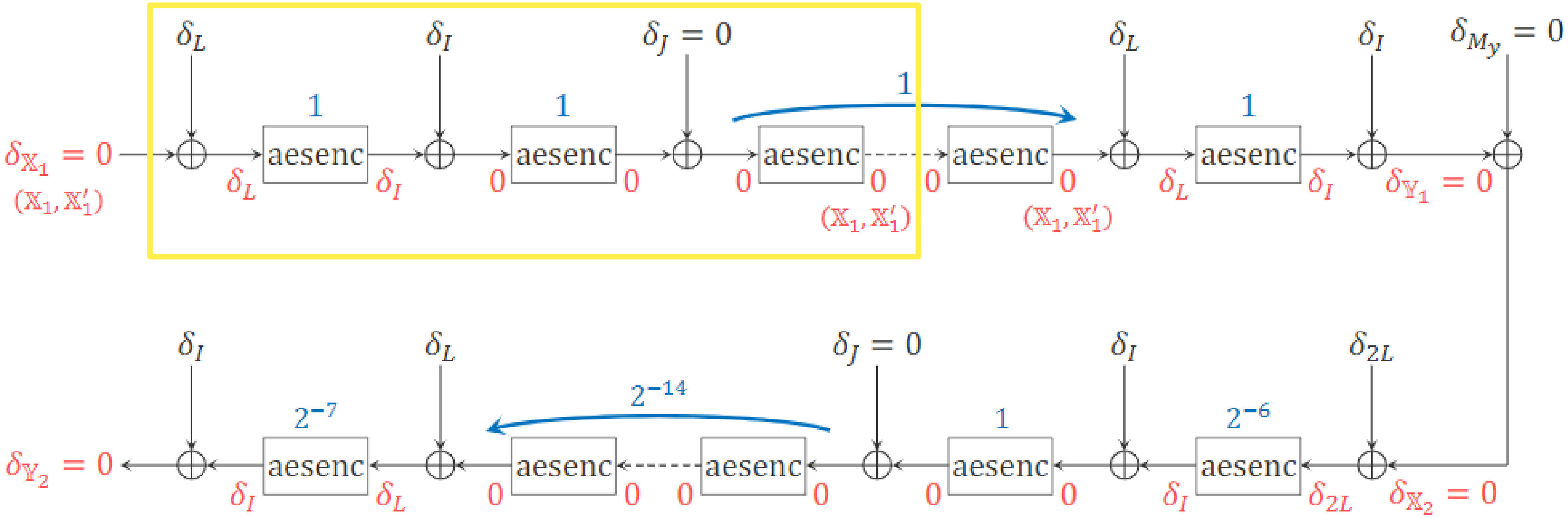




Attack detail

- Find $K = I \,||\, J \,||\, L,\ K' = I' \,||\, J' \,||\, L'$, s.t. $(\delta_{\mathbb{X}_1}, \delta_{\mathbb{Y}_1}, \delta_{\mathbb{X}_2}, \delta_{\mathbb{Y}_2}) = (0,0,0,0)$ $(\delta_{\mathbb{X}_1} = \mathbb{X}_1 \oplus \mathbb{X}'_1)$
  - Set $\delta_{\mathbb{X}_1} = 0$, and set δ_L so that δ_L and δ_{2L} have only 1 active S-box
  - Set δ_I to cancel out diff. propagation caused by δ_L and δ_{2L}
  - Set J, J' so that **3rd aesenc outputs go back to $\mathbb{X}_1, \mathbb{X}'_1$** (here, $\delta_J = 0$)
  - 3 aesenc with (L, I, J) and (L', I', J') maps $\mathbb{X}_1$ to $\mathbb{X}_1$ $\Rightarrow$ **$\delta_{\mathbb{Y}_1} = 0$ w/ prob. 1**
  - Set $\delta_{M_y} = 0 \rightarrow \delta_{\mathbb{X}_2} = \delta_{\mathbb{Y}_1} = 0$
  - **2nd $AES10$: event of $\delta_{\mathbb{Y}_2} = 0$ is probabilistic, but only 1 active S-box per one aesenc**
  - attack comp. : $\leq 2^{28}$
  - actual comp. : 2^{27}





Conclusion

- First key-committing analysis on concrete EtE schemes
  - For Adiantum/HCTR2 : (we omit here, but) a small detail that has little impact on the standard model security can significantly impact KCS, which makes some cases difficult to analyze.

Scheme	CMT-1 A	CMT-1 P	CMT-4 (A & P)	Proof
general AEZ	$O(2^{n/2})$	(not specified)	$O(1)$	$n/2$ (Sect. 7.1)
full-spec AEZ	2^{27}	(not specified)	$O(1)$	—
EtE-Adiantum	$O(2^{n/2})$	$O(2^{n/2})$	$O(1)$	$n/2$ (Sect. 7.2)
EtE-HCTR2	$O(2^{n/2})$	$O(2^{n/2})$	$O(1)$	—

- Future work
  - Analysis of AEZ-tiny and other EtE

Thank you!

We appreciate anonymous reviewers for their insightful comments!

Appendix

Ref.

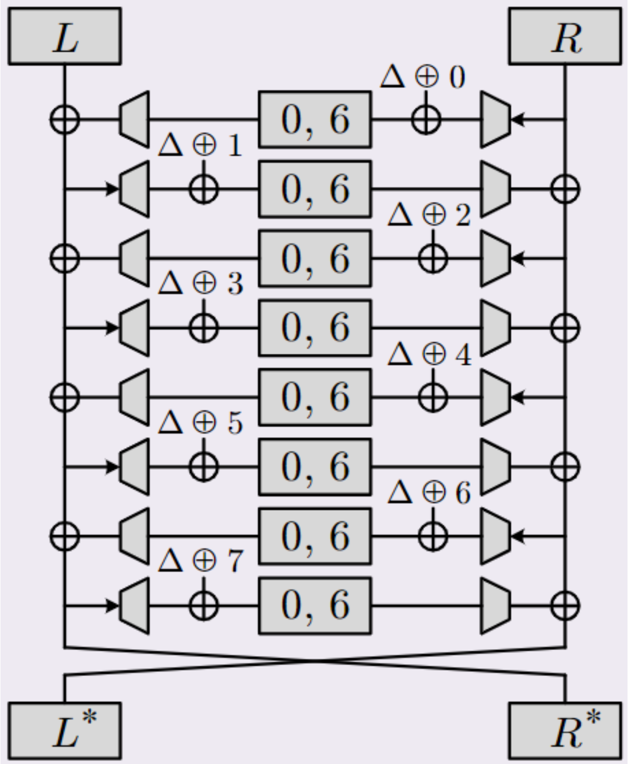
- [DGRW18]: Dodis, Y., Grubbs, P., Ristenpart, T., Woodage, J.: Fast message franking: From invisible salamanders to encryptment. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 155–186. Springer, Heidelberg (Aug 2018). https://doi.org/10.1007/978-3-319-96884-1_6
- [LGR21]: Len, J., Grubbs, P., Ristenpart, T.: Partitioning oracle attacks. In: Bailey, M., Greenstadt, R. (eds.) 30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021. pp. 195–212. USENIX Association (2021), https://ia.cr/2020/1491
- [IIM21]: Takanori Isobe, Ryoma Ito, and Kazuhiko Minematsu. Security analysis of SFrame. In Elisa Bertino, Haya Shulman, and Michael Waidner, editors, ESORICS 2021, Part II, volume 12973 of LNCS, pages 127–146. Springer, Heidelberg, October 2021.
- [ADG+22]: Albertini, A., Duong, T., Gueron, S., Kölbl, S., Luykx, A., Schmieg, S.: How to abuse and fix authenticated encryption without key commitment. USENIX Security 2022 (2022), https://ia.cr/2020/1456
- [BH22]: Mihir Bellare and Viet Tung Hoang. Efficient schemes for committing authenticated encryption. In Orr Dunkelman and Stefan Dziembowski, editors, EUROCRYPT2022,PartII, volume 13276 of LNCS, pages 845–875. Springer, Heidelberg, May / June 2022.
- [MLGR23]: Sanketh Menda, Julia Len, Paul Grubbs, and Thomas Ristenpart. Context discovery and commitment attacks - how to break CCM, EAX, SIV, and more. In Carmit Hazay and Martijn Stam, editors, EUROCRYPT 2023, Part IV, volume 14007 of LNCS, pages 379–407. Springer, Heidelberg, April 2023.
- [FOR17]: Pooya Farshim, Claudio Orlandi, and Răzvan Roşie. Security of symmetric primitives under incorrect usage of keys. IACR Trans. Symm. Cryptol., 2017(1):449–473, 2017.
- [GLR17]: Paul Grubbs, Jiahui Lu, and Thomas Ristenpart. Message franking via committing authenticated encryption. In Jonathan Katz and Hovav Shacham, editors, CRYPTO 2017, Part III, volume 10403 of LNCS, pages 66–97. Springer, Heidelberg, August 2017.

Ref.

- [BR00]: Mihir Bellare and Phillip Rogaway. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In Tatsuaki Okamoto, editor, ASIACRYPT 2000, volume 1976 of LNCS, pages 317–330. Springer, Heidelberg, December 2000.
- [HKR15]: Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In Elisabeth Oswald and Marc Fischlin, editors, EUROCRYPT 2015, Part I, volume 9056 of LNCS, pages 15–44. Springer, Heidelberg, April 2015.
- [CB18]: Paul Crowley and Eric Biggers. Adiantum: length-preserving encryption for entry-level processors. IACR Trans. Symm. Cryptol., 2018(4):39–61, 2018.
- [CHB21]: Paul Crowley, Nathan Huckleberry, and Eric Biggers. Length-preserving encryption with HCTR2. Cryptology ePrint Archive, Report 2021/1441, 2021. https://eprint.iacr.org/2021/1441.

AEZ-tiny

- Input length less than 256 bits: AEZ-tiny
  - Feistel with a minimum of 8 rounds
  - Number of steps varies depending on input length
  - Fig: [HKR15]



Attack details

- Once getting C_y collision, other ciphertext blocks are easy to collide
  - Verification is OK if M_y is zeros
  - $CC_1, \ldots, CC_m$ can be any value because they are irrelevant to M_y, C_y
  - To invoke C_x collision, we manipulate Δ
  - Δ can be any value like CMT-4 attack