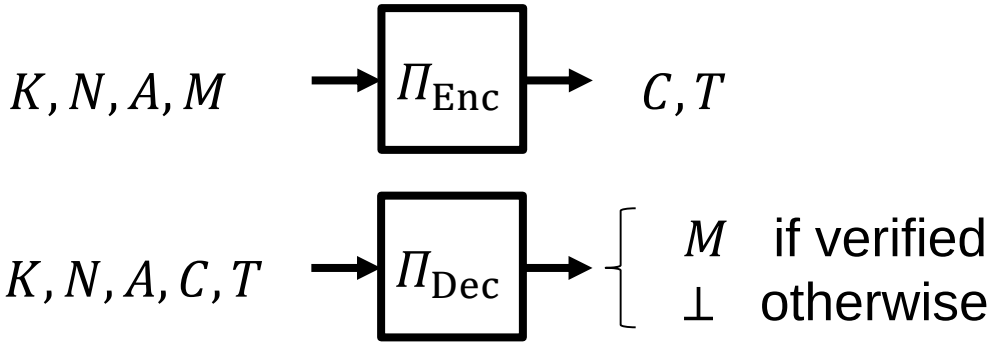
Generic Committing Attacks: Zero-Padded Ascon is Less Secure than Expected

Nilanjan Datta[1], Hrithik Nandi[1,2], Soumit Pal[3], Yu Sasaki[4], Patrick Struck[4], Maximiliane Weishäupl[5] (from group work at GAPS 2024)

1. IAI TCG CREST, 2. RKMVERI, 3. Indian Statistical Institute, 4. NTT Social Informatics Laboratories, NIST Associate, 5. University of Konstanz, 6. University of Regensburg

August 19, 2026, CRYPTO 2026 @ UCSB

Authenticated Encryption with Associated Data



- AEAD provide both integrity and privacy in a single scheme, enabling high efficiency and design simplicity.
- Security of AEAD is well studied. Schemes usually come with security proofs with formal security notions.
- However, some protocols may use AE beyond the premise of the traditional AE-security guarantee.

Committing Security and Zero-padding

- Committing Security of AEAD [Farshim et al. 2017]

  It should be hard to find two different inputs processed to the same output;
  $(K_1, N_1, A_1, M_1), (K_2, N_2, A_2, M_2)$ s.t. $ENC(K_1, N_1, A_1, M_1) = F(K_2, N_2, A_2, M_2)$.

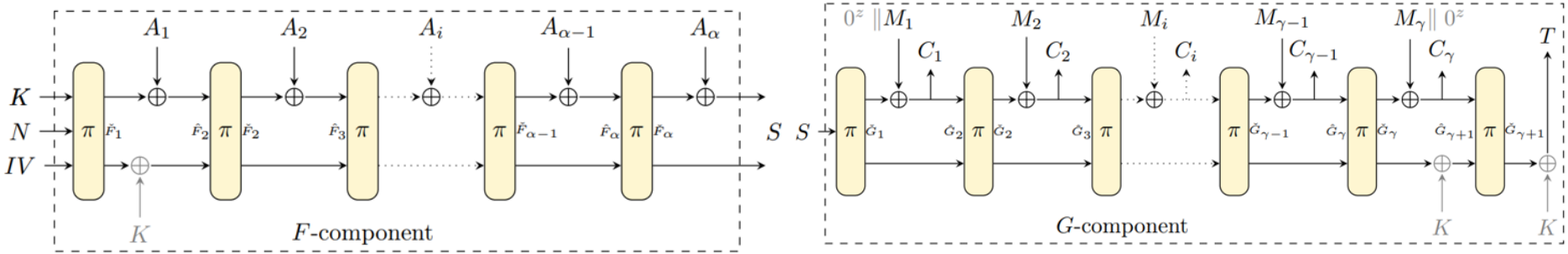
  - Key commitment (CMT-1/CMT-K): $K_1 \neq K_2$
  - Context commitment (CMT-4): $(K_1, N_1, A_1, M_1) \neq (K_2, N_2, A_2, M_2)$
  - CMT-K* [Menda et al. 2023]: $K_1 \neq K_2, A_1 = A_2, N_1 = N_2$

- Zero padding (ZP) [Albertini et al. 2022]
  - Key committing security of GCM is broken in $O(1)$, which increases to $\tau/2$-bit security (under the same nonce) by prepending 0^τ in M.
  - two possibilities of appended bit positions: prefix or suffix

Our Target Construction: Duplex and Ascon

We treat Duplex and Ascon in an integrated way and consider ZP.

- **Duplex**: a permutation based construction
- **Ascon**: NIST standard for lightweight cryptography (SP800-232)
  - State is initialized by a key K, a nonce N, and a fixed constant IV.
  - Key blinding: XORs K to the state, in 3 places
    - › Initial-KB, Final-KB, Tag-KB



Summary of Results

Systematic analysis of generic committing attacks

- Three existing attack approaches: IS / CC / TC
- Analysis under KB and ZP under the notion of CMT-4 and CMT-K*

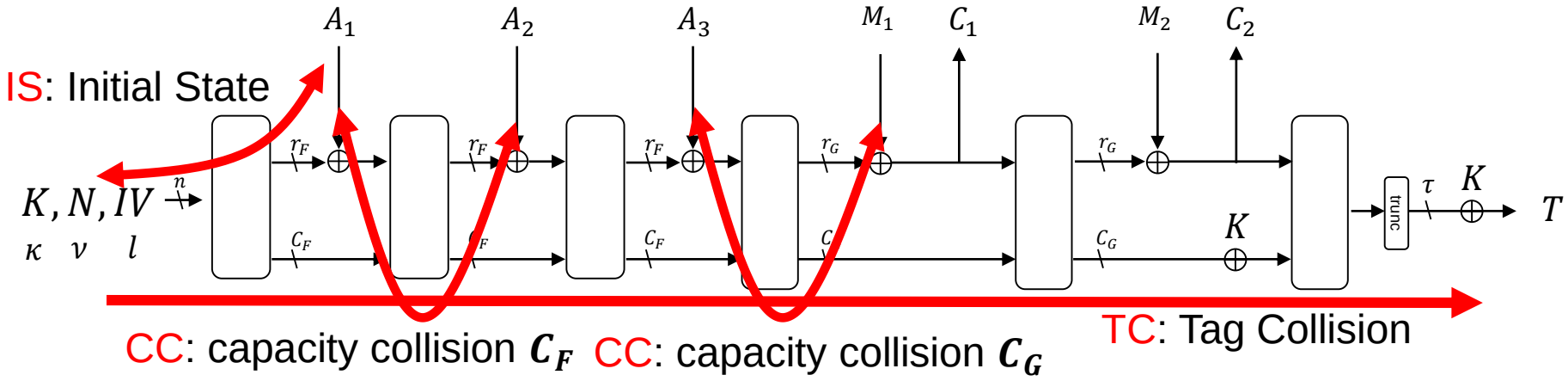
New attacks

- **2S-TC**: separately attack zero-padding and tag collisions
  - › application to tag-truncated Ascon by NIST
  - › counterexample of previous proof on Ascon-like-ZP
- **2R-IS**: extend the applicable parameter range
  - › application to a CAESAR candidate Ketje
- **MitM**: a new attack approaches emerges when only tag KB is used.

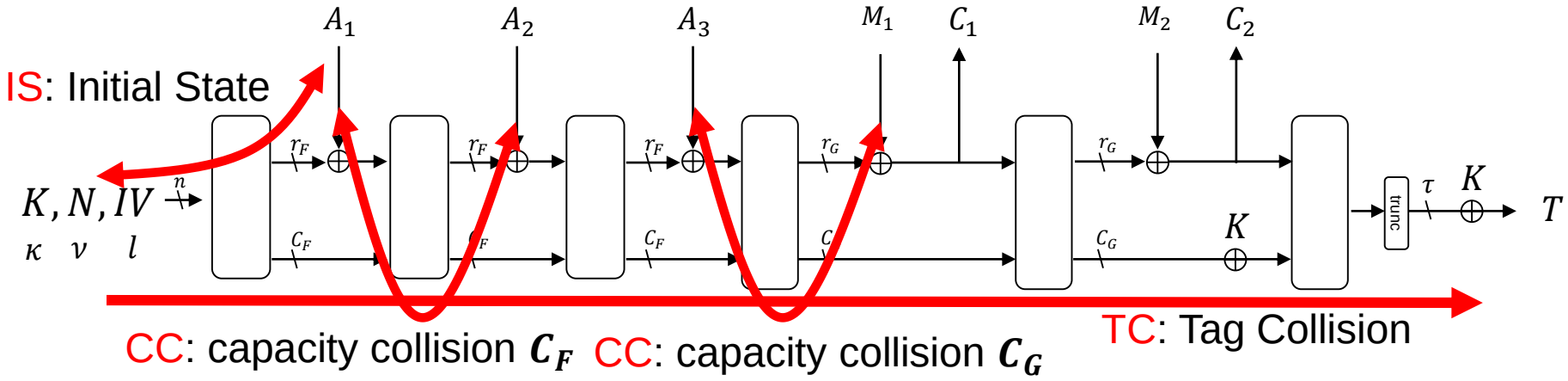
Systematic analysis of generic committing attacks

- A part of analysis on CMT-4 will be explained.
- Please refer to the paper for CMT-K*.

Existing Three Approaches of Attacking CMT-4



Complexity Evaluation with ZP and KB



	IS	CC (prefix ZP)	CC (suffix ZP)	TC
ZP-Duplex	l	$\min(\frac{C_F}{2}, \frac{C_G + z}{2})$	$\min(\frac{C_F}{2}, \frac{C_G}{2})$	$\frac{\tau + z}{2}$
Variants w/ initial-KB	$\frac{\kappa}{2} + l$	$\min(\frac{C_F}{2}, \frac{C_G + z}{2})$	$\min(\frac{C_F}{2}, \frac{C_G}{2})$	$\frac{\tau + z}{2}$

- The cost of TC increases by $\frac{z}{2}$ ⇒ ZP has the same effect as a tag.
- Initial-KB contributes to CMT-4 security.

New Attacks

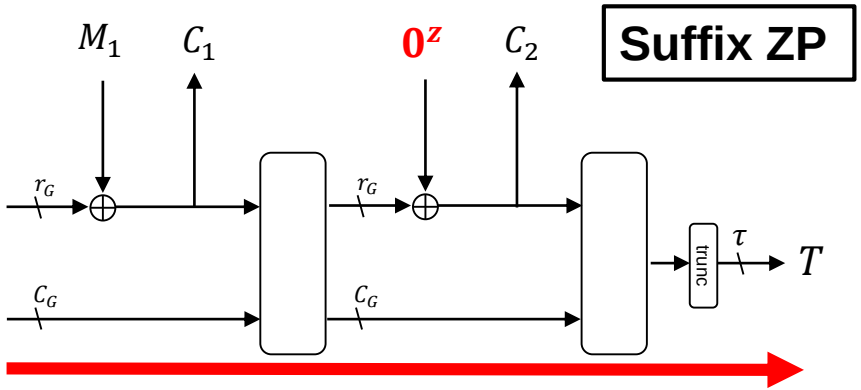
Overview of Two-Stage Tag Collision: 2S-TC

NTT

"*ZP has the same effect as a tag*"

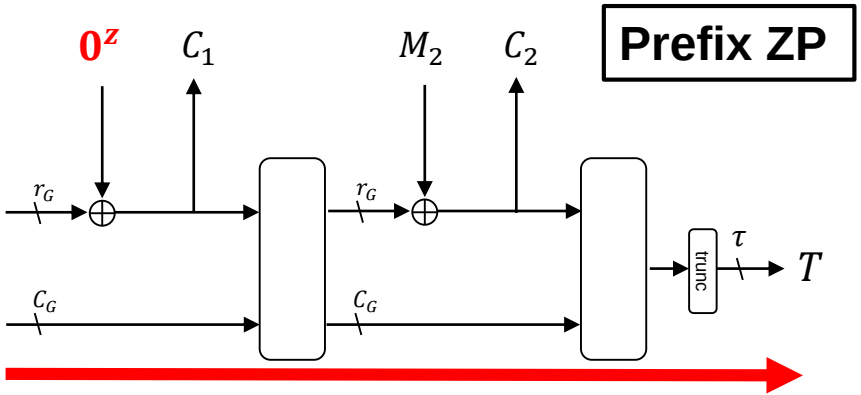
Reasonable for suffix

- Attackers check collision on $C_2||T$ together.
- Cost: $2^{\frac{z+\tau}{2}}$
- matches the proof for suffix [NSS23,Theorem 1]

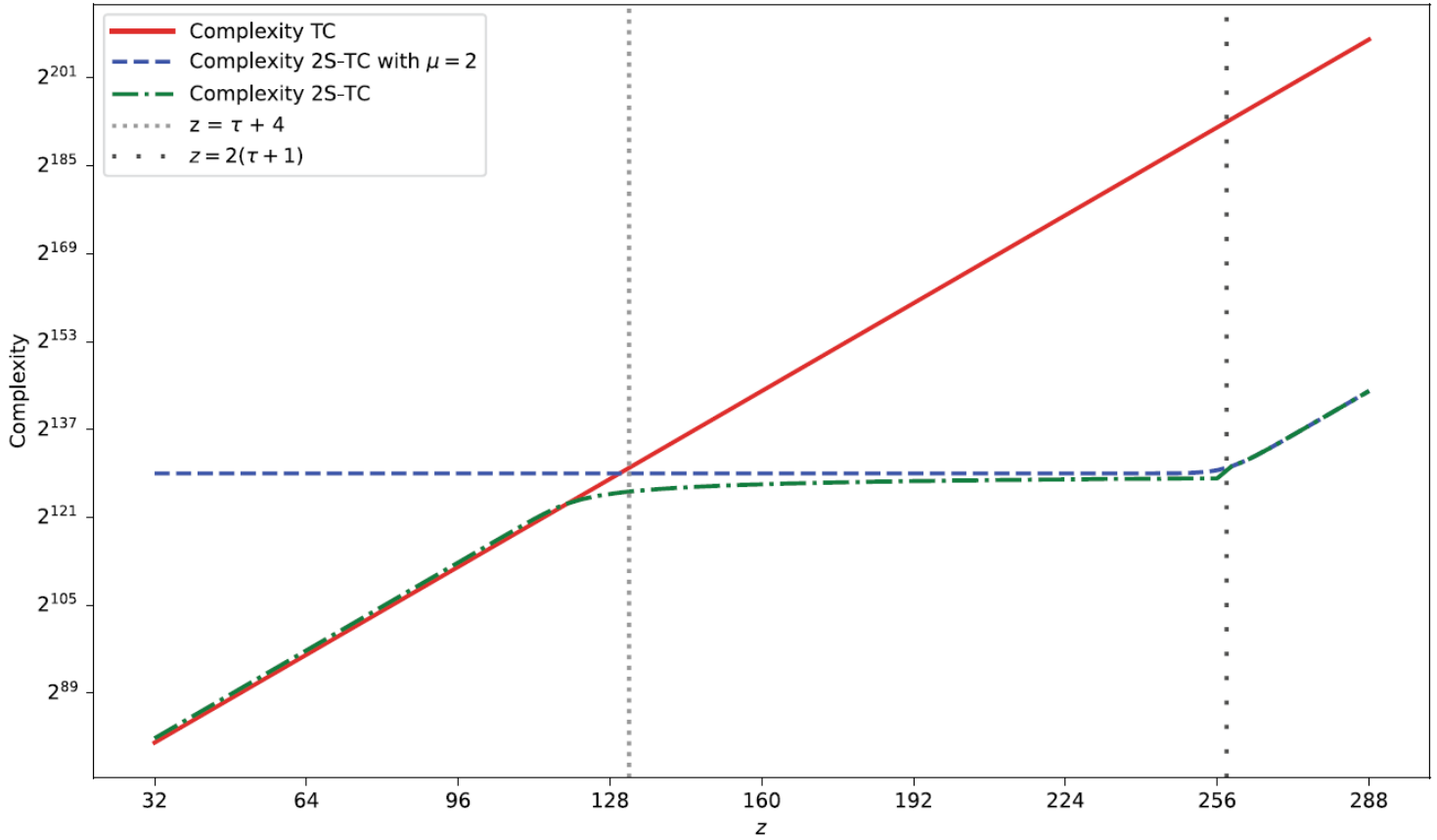


Unreasonable for prefix

- After generating a collision on C_1, a collision on T can be found in a brute-force manner.
- Cost : $2^{\frac{z}{2}} + 2^{\tau}$
- counterexample of [NSS23,Theorem 2] that generalizes the proof for suffix to any encoding

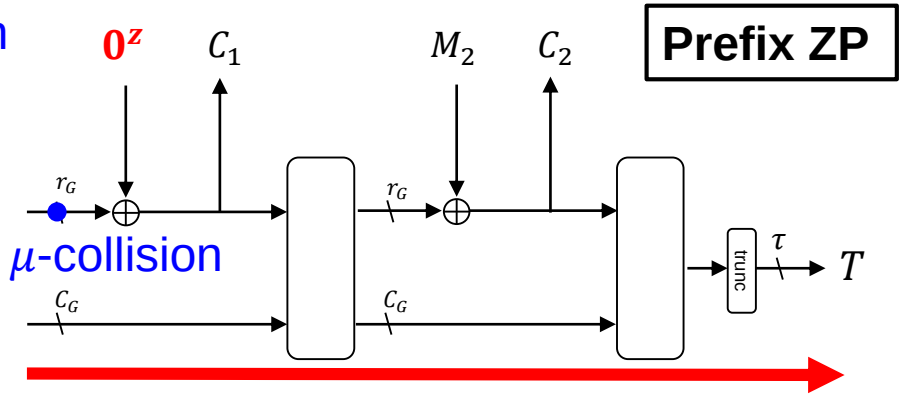


Complexity Comparison for Tag Collisions



Further Improvement of 2S-TC by Multicollisions

- When a C_1-collision is generated, μ-collision can be generated instead.
- The brute-force search on T becomes a collision search over μ choices.
- Cost: $\log(2^{mulcoll(z,\mu)} + 2^{\tau-\log(\mu)})$, can be faster than $2^{\frac{z}{2}} + 2^t$ by a factor of up to $\log z$.



- For certain parameter choices, 2S-TC outperforms existing attacks: IS, CC, TC
  - best attack for Ascon with tag truncation standardized by NIST [SP800-232]
  - best attack for Ascon-128, a primary member of Ascon submission in NIST LWC
- For the default choice of SP800-232, the results by [NSS23] hold.

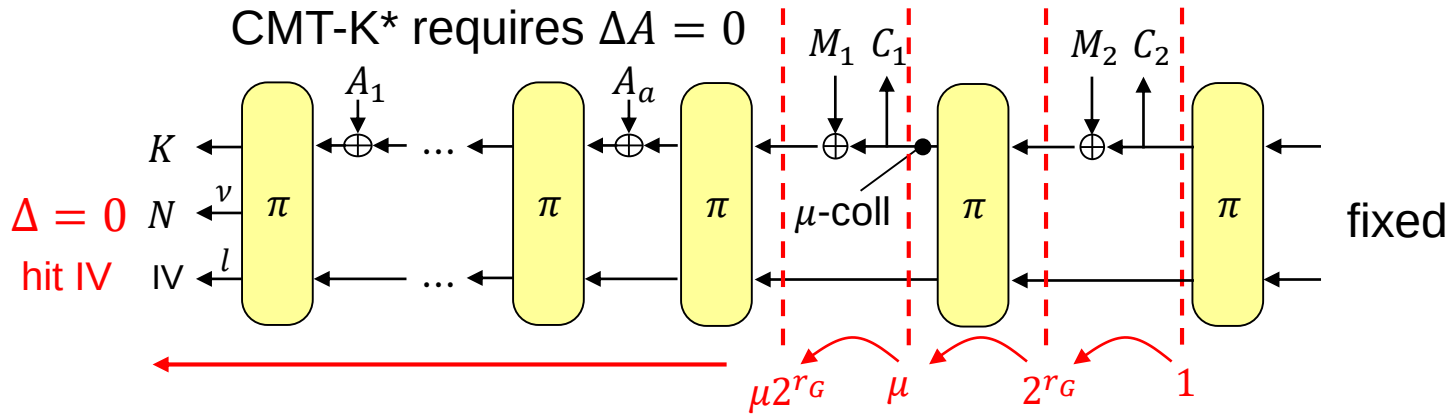
2-Round Initial State (2R-IS)

Existing CMT-K* attack for duplex + suffix ZP

- Requirement is nonce collision & IV hit; the attack cost is $\frac{\nu}{2} + l$
- Degrees of freedom (DoF) is 1 msg block, r_g; deriving the condition $r_g \geq \frac{\nu}{2} + l$.

We improve DoF to μr_g with a multi-collision, enlarge the attacked parameter range.

- Ketje allows a user to choose ν. For some ν, 2R-IS outperforms existing attack.



New MitM Attack only with Tag-KB

- Construction adopted by a NIST LWC finalist SCHWAEMM.
- With $\Delta M \neq 0$, Tag-KB can lower the security of Duplex. (see ePrint2026/1160)

Without tag-KB

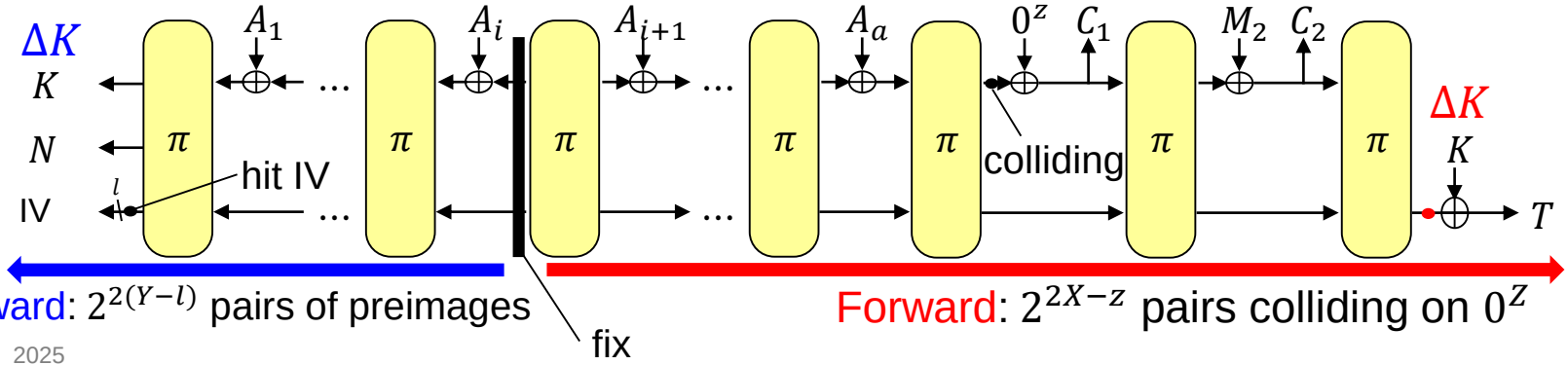
Collision on tag

Cost: $2^{\frac{z+\tau}{2}}$

With tag-KB

match ΔK independently computed in two directions

Cost: $2^{\frac{z+\tau}{4}+\frac{l}{2}+1}$



Conclusion

Systematic analysis:

- 3 attacks IS / CC / TC for each KB / ZP w.r.t. CMT-4 / CMT-K*

Takeaway from New Attacks:

- 2S-TC shows that Zero-padding ≠ simply a longer tag
- Impact of multicollision needs to be considered carefully
  - It may lower the attack cost or enlarge the attackable parameters
  - Impact on Ascon tag truncation by NIST, Ascon-128, KetJe
- Committing security is parameter- and structure-sensitive
  - Padding position matters
  - Tag KB blocks some attacks, but can enable a new MitM attack

Innovating a Sustainable Future for People and Planet


NTT