Committing Security of ASCON: Cryptanalysis on Primitive and Proof on Mode

Yusuke Naito — Mitsubishi Electric Corporation
Yu Sasaki — NTT Social Informatics Laboratories; NIST Associate
Takeshi Sugawara — The University of Electro-Communications

03/25/2024 FSE2024@Leuven

Summary

NTT

We study the context committing (CMT-4) security of ASCON.

Known Fact: Security upper-bound of AEAD with a t-bit tag is $\frac{t}{2}$ bits.

Our Mode Results

- We prove $\frac{t}{2}$ bits of CMT-4 security of ASCON. (best achievable)
- By adding z-bits of zeros to the message (ASCON-zp), provable CMT-4 security increases $\min\{\frac{t+z}{2}, \frac{n+t-k-v}{2}, \frac{c}{2}\}$, where n is permutation size, k is key size, v is nonce size, c is capacity; $\min\{64 + \frac{z}{2}, 96\}$ for ASCON.

Our Primitive Results

We practically break CMT-4 security of ASCON up to 3 rounds of ASCON-permutation, which is 1 round longer than the existing collision attacks.

Authenticated Encryption with Associated Data

$$K, N, A, M \longrightarrow \boxed{\Pi_{\mathrm{Enc}}} \longrightarrow C, T$$

$$K, N, A, C, T \longrightarrow \boxed{\Pi_{\mathrm{Dec}}} \longrightarrow \begin{cases} M & \text{if verified} \\ \perp & \text{otherwise} \end{cases}$$

- Security of AE is well studied. Schemes usually come with security proofs with formal security notions.
- However, AE schemes are sometimes misused or abused beyond their promise.

Key Commitment

- Key-committing security used to be discussed in the context of PKC.
- Farshim et al. proposed the theoretical framework of the symmetric-key counterpart of the key-committing security: In AEAD, any ciphertext should be decrypted only with the key that is used to generate it.
- Without key commitment, an attacker can efficiently find a ciphertext decrypted with multiple keys:

$$\Pi_{Enc}(K, N, A, M) = \Pi_{Enc}(K', N', A', M') \text{ with } K \neq K'$$

- Conventional AE security notions do not support the key commitment.
- $O(1)$ attacks exist in GCM, GCM-SIV, CCM, ChaCha20-Poly1305.

Context Commitment

In 2022, Bellare-Hoang introduced generalization of key commitment called "*context commitment*."

- **Key commitment (CMT-1)**: K is different but no limit on N, A.

$$\Pi_{\mathrm{Enc}}(K, N, A, M) = \Pi_{\mathrm{Enc}}(K', N', A', M') \text{ with } K \neq K'.$$

- **Context commitment (CMT-4)**: different values can be located in any of K, N, A, M.

$$\Pi_{\mathrm{Enc}}(K, N, A, M) = \Pi_{\mathrm{Enc}}(K', N', A', M') \text{ with } (K, N, A, M) \neq (K', N', A', M')$$

CMT-4 guarantees more robust security than CMT-1.

AE with CMT-4 security is an ongoing research challenge.

ASCON

NTT

- **ASCON**: The winner of NIST lightweight crypto competition.
- Duplex-like mode (ASCON mode) with a dedicated permutation (ASCON permutation)
  - 3 schemes in ASCON family: ASCON-128, ASCON-128a, ASCON-80pq
- NIST is standardizing ASCON and real-world systems will migrate to ASCON in near future.

Our Interest

- How strong is ASCON with respect to committing security?
- Can we improve CMT-4 security of ASCON with a slight change?

Generic Attacks on CMT-4

NTT

- Consider AEAD s.t. the decryption function computes a t-bit tag T' from decryption context (K, N, A, C) and verifies its correctness by matching it with the received T.

- Generic attack complexity of CMT-4 security, i.e. complexity to generate $\Pi_{\mathrm{Enc}}(K, N, A, M) = \Pi_{\mathrm{Enc}}(K', N, A', M')$ is $2^{\frac{t}{2}}$.

- Fix C to a constant. Compute a tag for $2^{\frac{t}{2}}$ choices of (K, N, A) and find a collision of the tag.

- For ASCON, $t = 128$. CMT-4 security of ASCON is at most 64 bits.

Towards Higher CMT-4 Security

- CMT4 is **offline security**; typically k-bit security is required for a k-bit key due to exhaustive search. 64-bit security is too small.

Previous work on **enhancing CMT-x security**

- Appending zero bits to M (**zero-padding**)
  - Proposed to improve CMT-1 security rather than CMT-4
  - Ciphertext size increases, higher load in bandwith
- **Combining collision-resistant hash $\boldsymbol{H}$** (eg HtE, CTX, KIVR).
  - Need extra primitive
  - Security is bounded by the output of H.
  - It may break black-box access to the underlying AEAD.

We consider zero-padding to improve ASCON's CMT-4 security.

Existing Results on Duplex AEAD

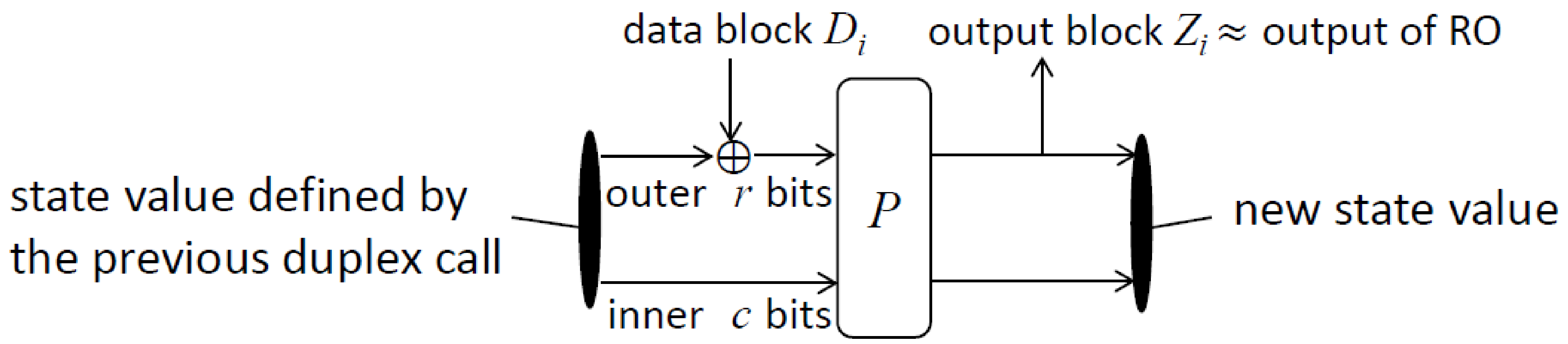
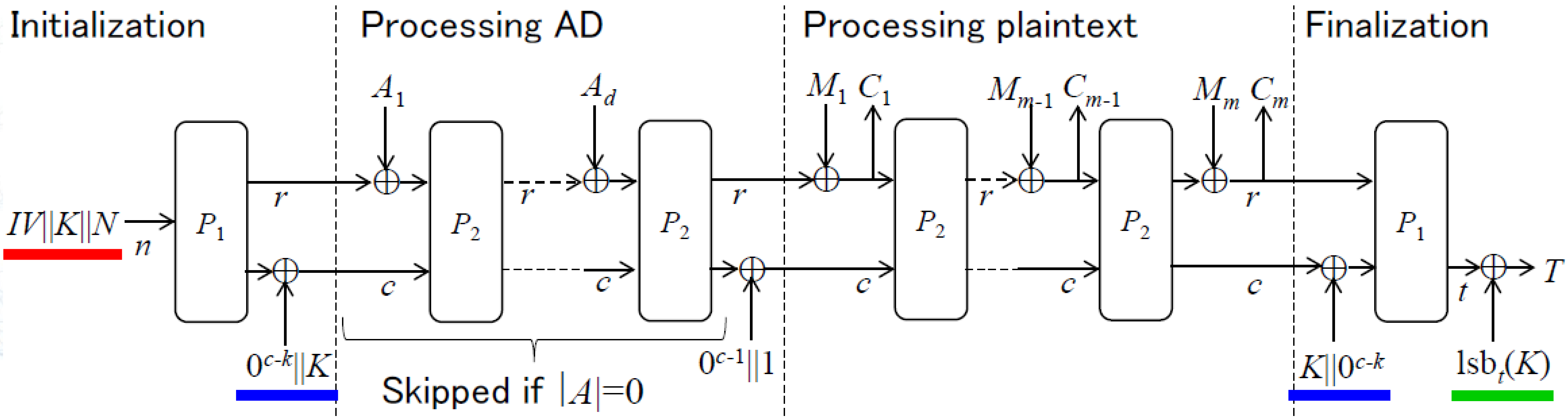


Figure 1: Duplex Construction [BDPV11]. P is a $(r+c)$-bit permutation.

- Duplex AEAD easily achieves the committing security because its security is reducible to the indifferentiability of the sponge construction [BDPV08].
- The output can be seen as that from a random oracle (RO) up to $c/2$ bits.
- For example, Dodis et al. proposed a concrete duplex-based scheme that satisfies the key-committing security [DGRW18].

Unique Features in ASCON Mode



ASCON mode is similar to duplex, yet has **several important differences**.

- Initial state is chosen such that the inner part is controlled.
- Tag is generated from the inner part.
- Key, chosen by the attacker in CMT-4, is added to the inner part.

Proof for duplex does not work. A new proof is required.

Very Brief Proof Intuition

At the first glance,

1. $(k + v)$-bits of the initial state is controllable.
2. r bits of the outer part and t bits of the inner part are observable.

These might degrade the security to $\frac{n-\max\{k+v,r+t\}}{2}$ bits. However,

1. The key masking serves as the feed-forward and prevents security degradation.
2. Use of two permutations P_1 and P_2 prevents from observing r and t bits simultaneously.

In the end, when z bits of zeros are padded to M, we can prove $\min\{\frac{t+z}{2}, \frac{n+t-k-v}{2}, \frac{c}{2}\}$ bits of CMT-4 security of ASCON with z-bit zero-padding.

Implication with ASCON's Parameters

- Our bound $\min\{\frac{t+z}{2}, \frac{n+t-k-v}{2}, \frac{c}{2}\}$ with ASCON's parameters offer $\mathbf{\min\{64+\frac{z}{2}, 96\}}$.
  - Original ASCON ($z=0$) ensures 64-bit CMT-4 security.
  - Zero-padding increases the security by a factor of $\frac{z}{2}$ up to 96 bits ($z \leq 64$).
  - The bound is tight as long as $z \leq 64$.

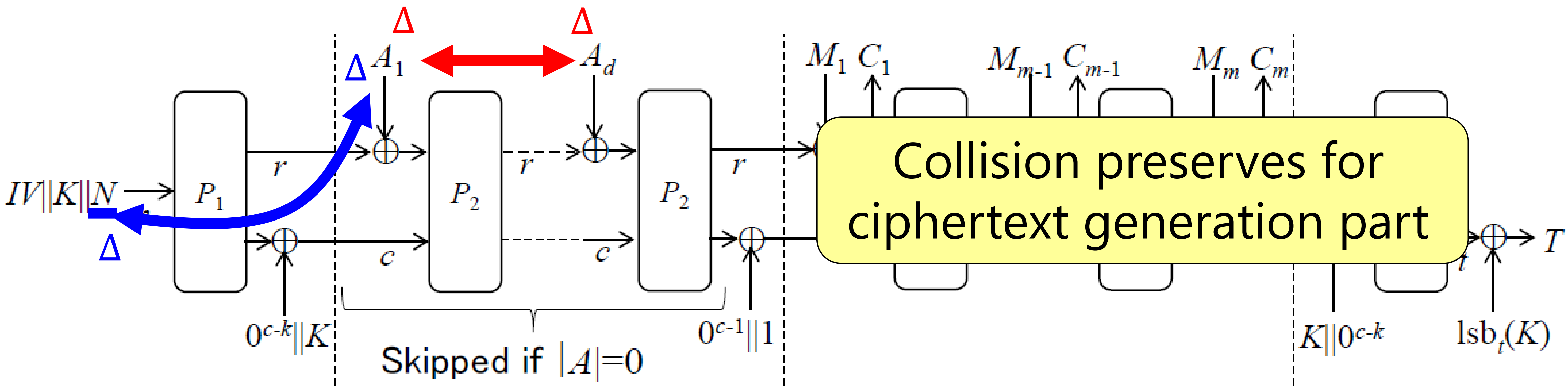
- There are boundaries of increasing the number of primitive calls due to the zero padding.
- We can avoid having additional primitive calls for several messages lengths, for example, the last message block is partial by the zero-padding length z.

Cryptanalysis Approaches (Mode Level)

For primitive analysis, the goal is to find two distinct (K, N, A, M) that collide on (C, T) with a smaller cost than the generic attack, i.e. 2^{64}.

Two possible approaches

1. Fix (K, N, M). Inject difference from A_i and cancel it with A_{i+1}.
2. Fix (K, M). Inject difference from N and cancel it with A_1.



Existing Results that can Break CMT4 Security

For cryptanalysis on primitive, the goal is to find two distinct (K, N, A, M) that collides on (C, T) with a smaller cost than the generic attack, i.e. 2^{64}.

No existing work aiming at CMT4, but collision and forgery attacks with approach 1 may work.

- 2-round collision with complexity $2^{62.6}$ [YLW+23] can attack CMT-4.
- 3-round forgery [GPY21] may work if differential trail with prob 2^{-117} can be satisfied with $< 2^{64}$ cost by using the knowledge of K.

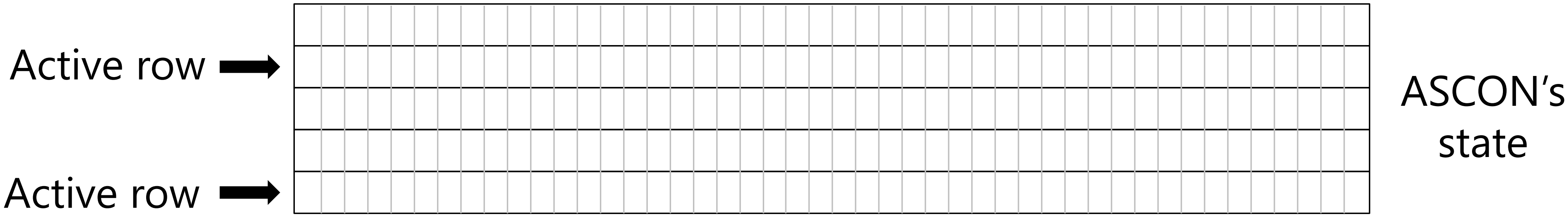
Collision with $< 2^{64}$ cost is already a big challenge even for 3 rounds.

We adopt approach 2, which has not been investigated in previous work.

Analytic Techniques (Primitive Level)

- We searched for differential trail using **MILP** and practically generated 2 distinct contexts resulting in the same ciphertext.

- MILP model for ASCON-permutation is too heavy in general.
- The most effective effort is divide-and-conquer approach.
  - For some round, we only allowed 2 active rows.
  - Try (5 choose 2) = 10 patterns.
  - Limit runtime to several hours. If effective trail exists, the solver stops quickly.



Generated Colliding Contexts for ASCON-128

NTT

Table 7: An Example of Paired Values for 3-Round ASCON-128.

	Value 1	Value 2	Difference
$IV_{k,r,a,b}$	80400c0600000000	80400c0600000000	0000000000000000
K_{MSB}	2164995204d2b154	2164995204d2b154	0000000000000000
K_{LSB}	21408952161a8984	21408952161a8984	0000000000000000
N_{MSB}	8040043400204008	a1009d660470d14c	2140995204509144
N_{LSB}	0470021110020000	25309f4314529144	21409d5204509144
After 1R	51e48a98919f2c82	51e48a98919f2c82	0000000000000000
	efbdf90bc9751bbb	efbdcd2bcb358b93	0000342002409028
	79f1b4b6785bf32f	79f1b4b6785bf32f	0000000000000000
	b261490a843943c3	b261490a843943c3	0000000000000000
	aeb407337089aef5	aeb4331372c13edd	0000342002489028
After 2R	9d6061940da22156	9d6061940da22156	0000000000000000
	08d70052ebfab2bb	48d60452f9f6a29b	40010400120c1020
	ae20f09b6d80208f	ae20f09b6d80208f	0000000000000000
	39aa88b8440203ca	39aa88b8440203ca	0000000000000000
	7cbea6bfd0266b48	3cbfa2bfc22a7b68	40010400120c1020
After 3R (Output)	a50d1f38a255a0d4	47c9113c90c9f2b4	e2c40e04329c5260
	67cc3c30332574dc	67cc3c30332574dc	0000000000000000
	f7e64d0ddad70381	f7e64d0ddad70381	0000000000000000
	ca05427803f501e0	ca05427803f501e0	0000000000000000
	20542b670894ef04	20542b670894ef04	0000000000000000

No difference in IV and key

Difference in nonce

Difference in the 64-bit outer part

Conclusion

We study the context committing (CMT-4) security of ASCON.

Our Mode Results

- We prove $\min\{\frac{t+z}{2}, \frac{n+t-k-\nu}{2}, \frac{c}{2}\}$ bits of CMT-4 security of ASCON-zp.
- With ASCON's parameters, the security is $\mathbf{min\{64+\frac{z}{2}, 96\}}$ bits.

Our Primitive Results

- Practical collision-type attacks on 3 rounds by using ΔN.

Target	Type	Round	Complexity	Ref.
Ascon-128, Ascon-80pq	CMT-3	2	$2^{62.6}$	[YLW+23]
Ascon-128a	CMT-3	3	$2^{117\dagger}$	[GPT21]
Ascon-128, Ascon-80pq	CMT-3	3	$2^{48\ddagger}$	This Work
Ascon-128a	CMT-3	3	$2^{36\ddagger}$	This Work