RSAConference2015
San Francisco | April 20-24 | Moscone Center

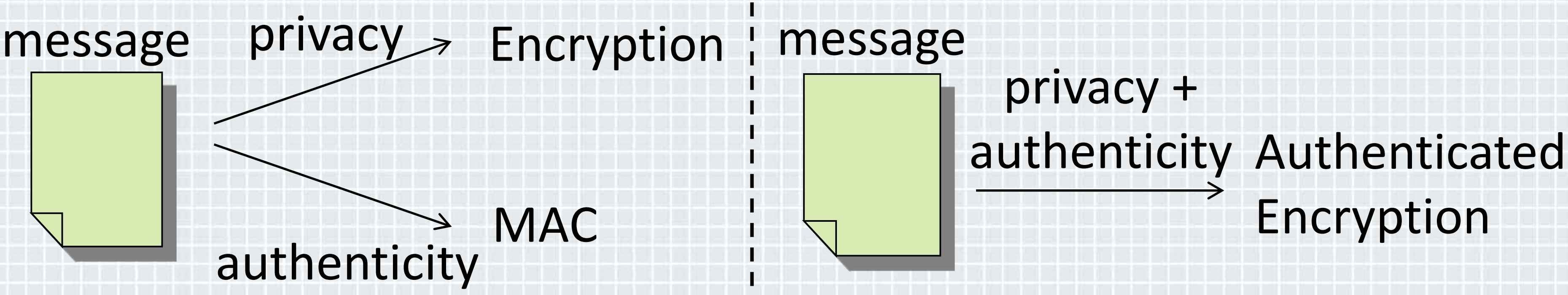
SESSION ID: CRYP-R04

How to Incorporate Associated Data in Sponge-Based Authenticated Encryption

Yu Sasaki and **Kan Yasuda**

NTT Secure Platform Laboratories

Authenticated Encryption



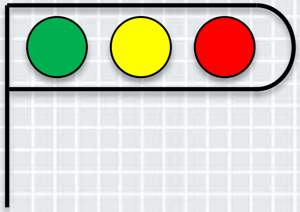
independently computed

all-in-one

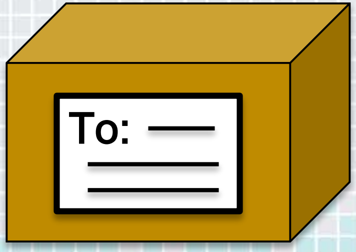
- Simple security discussion
- Higher performance

Associated Data (AD)

- The data to be authenticated but not encrypted
  - Ex: Traffic Signal



- AD makes sense only when two types of data co-exist in communication
  - Ex: Packet Header



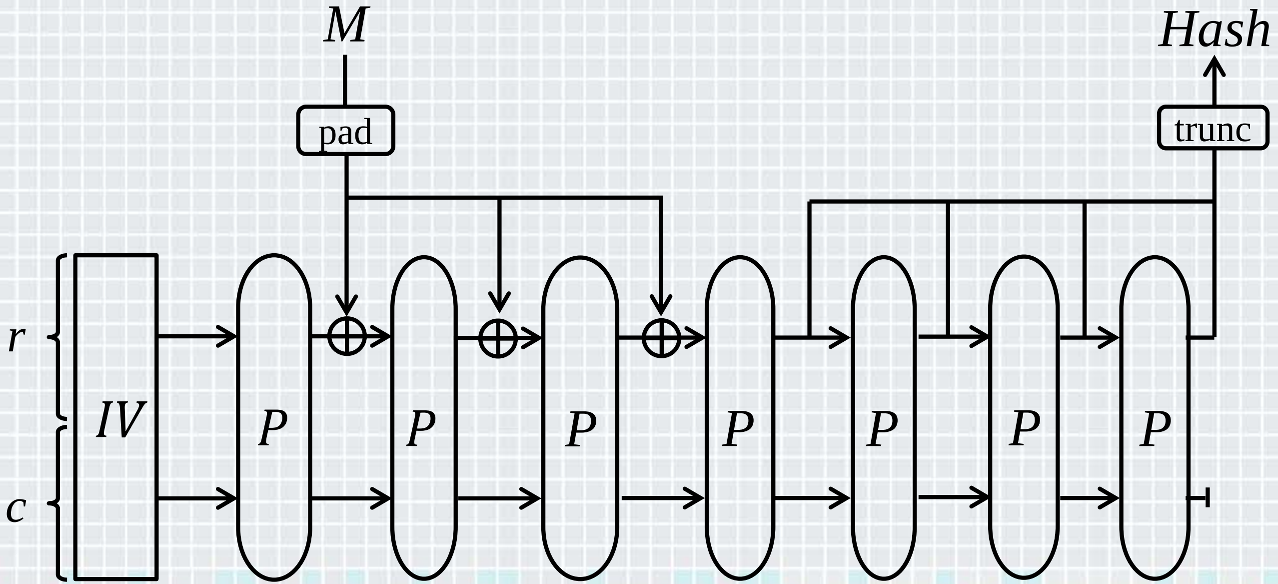
How to Build Authenticated Encryption

- Using symmetric-key primitive as a base
  - Block-cipher
  - Hash function
  - Stream cipher
  - Random permutation
- Sponge construction [Keccak-team 2007]
  - Designing permutation is easier than other primitives.
  - It turned out that the sponge construction can be lightweight.
  - 7 out of 57 designs in CAESAR are adopting the sponge construction.

Previous Sponge-Based Constructions

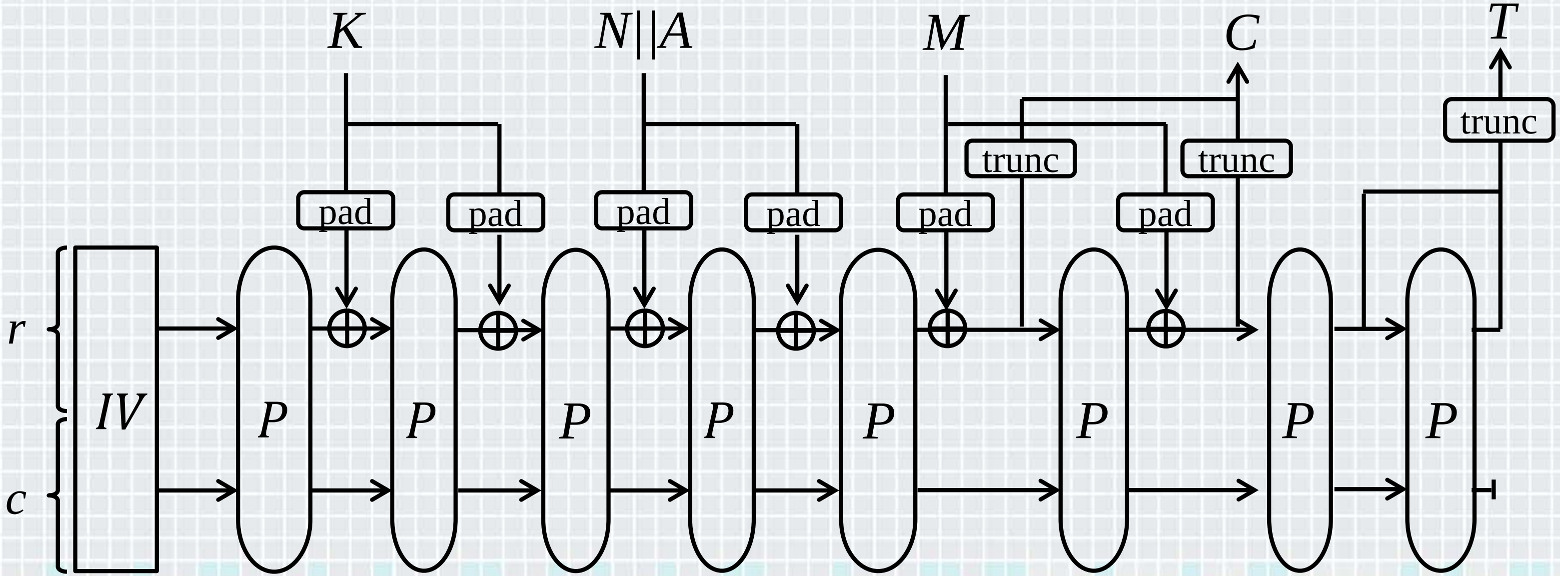
Sponge Construction (Hash Function)

- First absorb message, then squeeze the output.
- Security is $c/2$ bits.



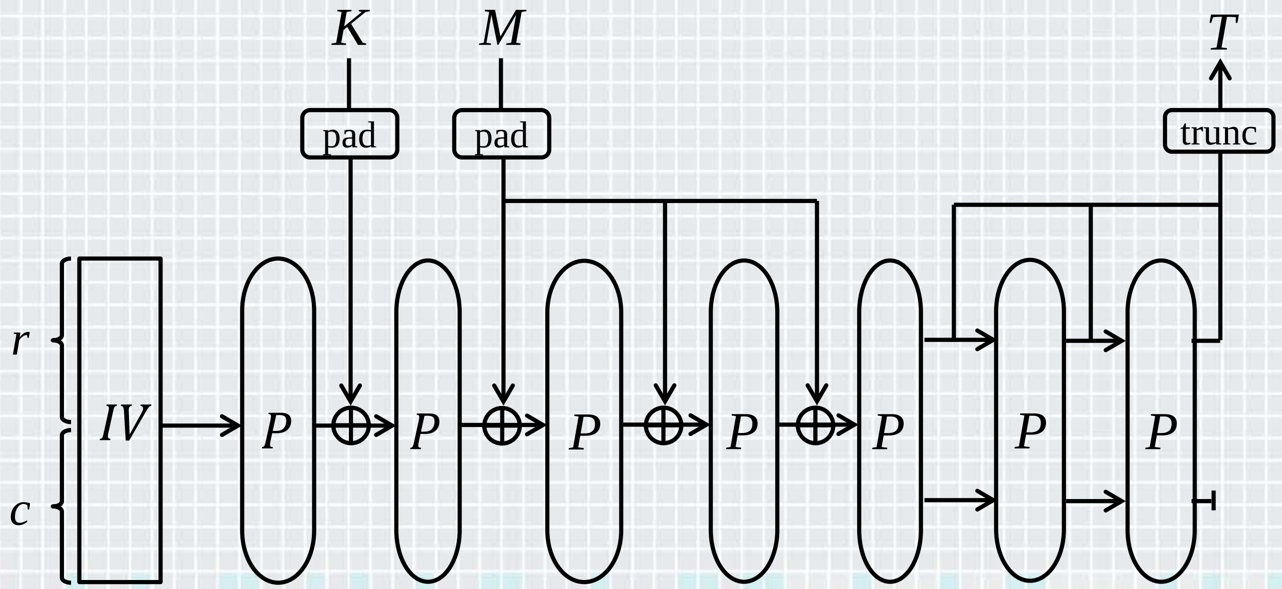
SpongeWrap (Authenticated Encryption)

- Absorb K, N, A. Squeeze T
- Both of absorb an squeeze are done for the encryption part (duplex)



donkeySponge (MAC)

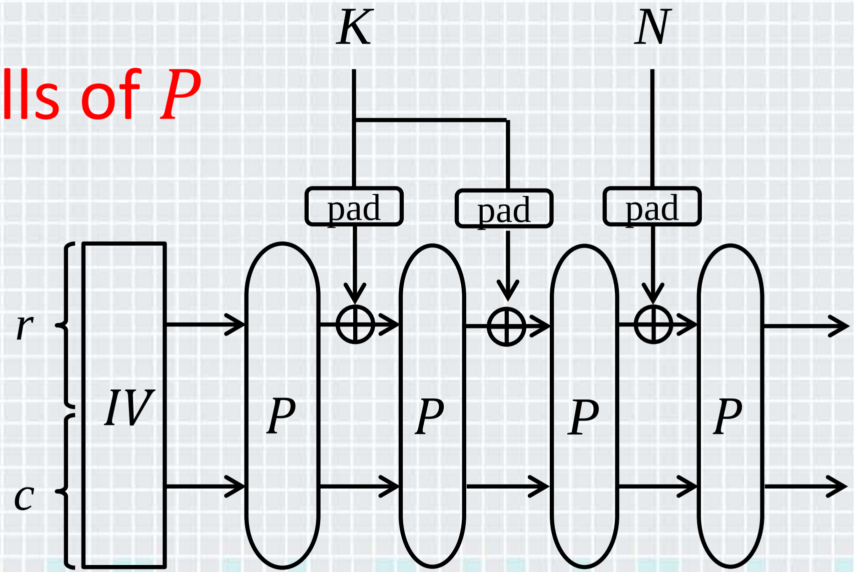
- Absorb (K, M) in $r + c$ bits. (inspired by Alpha-MAC)
- Internal state is secret → $b/2$-bit security.



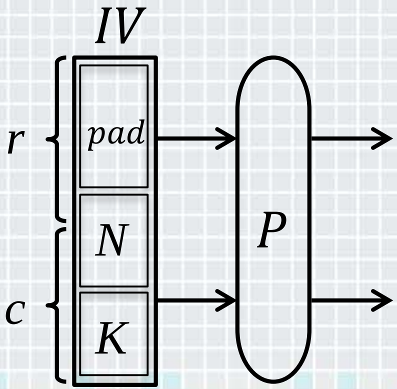
monkeyDuplex

- Efficient initialization for nonce-based scheme
- For different (K, M) state after P is randomized.

4 calls of P

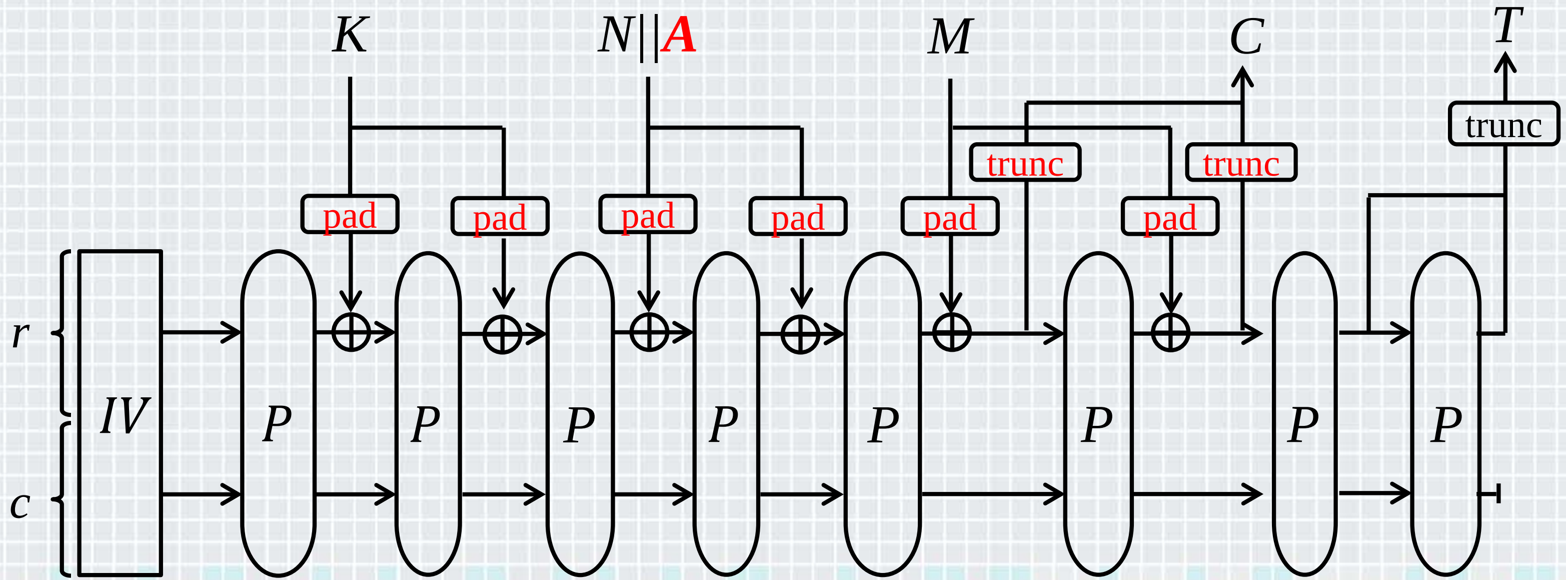


1 call of P



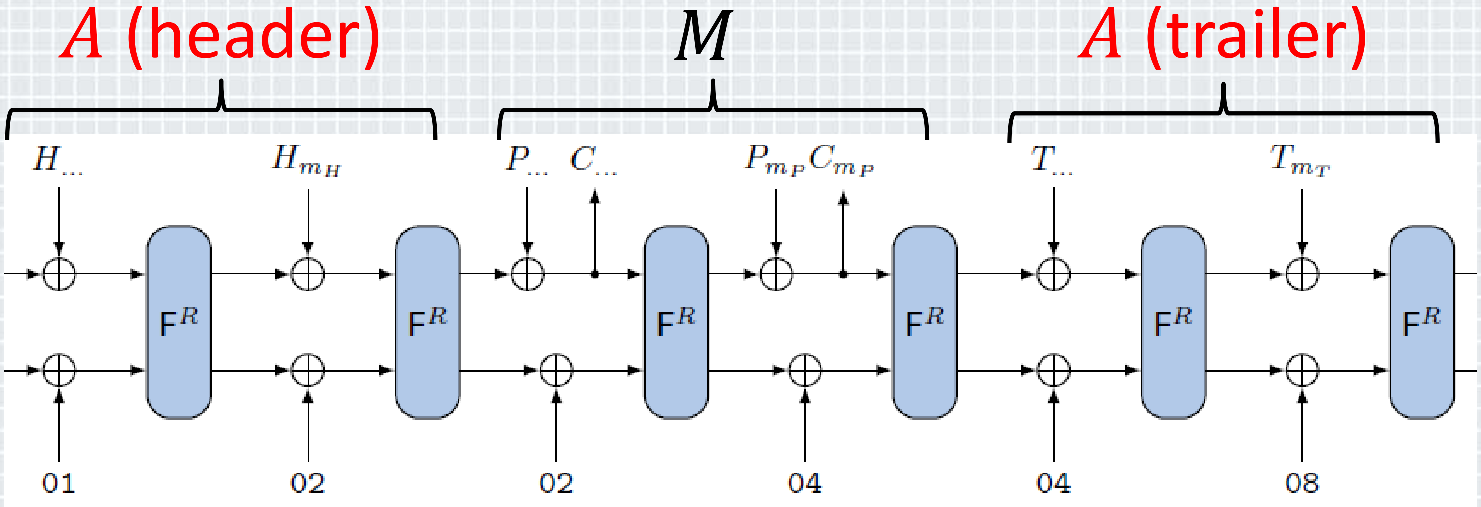
Drawbacks of Sponge-Based AE

- A must be provided before M. Otherwise, the computation gets stuck.
- Padding (frame bit) in every block occupies 1 bit.



Approach of NORX

- NORX is a CAESAR submission by Aumasson et al.
- It accepts associated data after M, called “ trailer.”

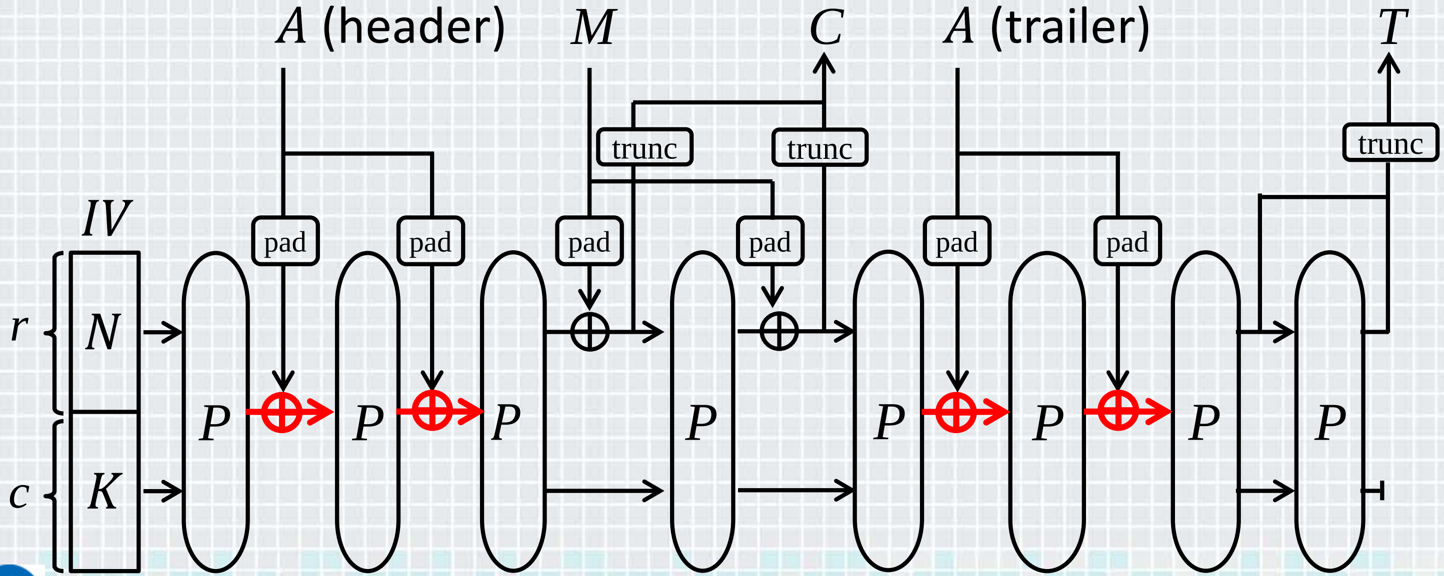


Jean-Phillip Aumasson, Philipp Jovanovic and Samuel Neves , *NORX v1*, Submitted to CAESAR.

Our Constructions

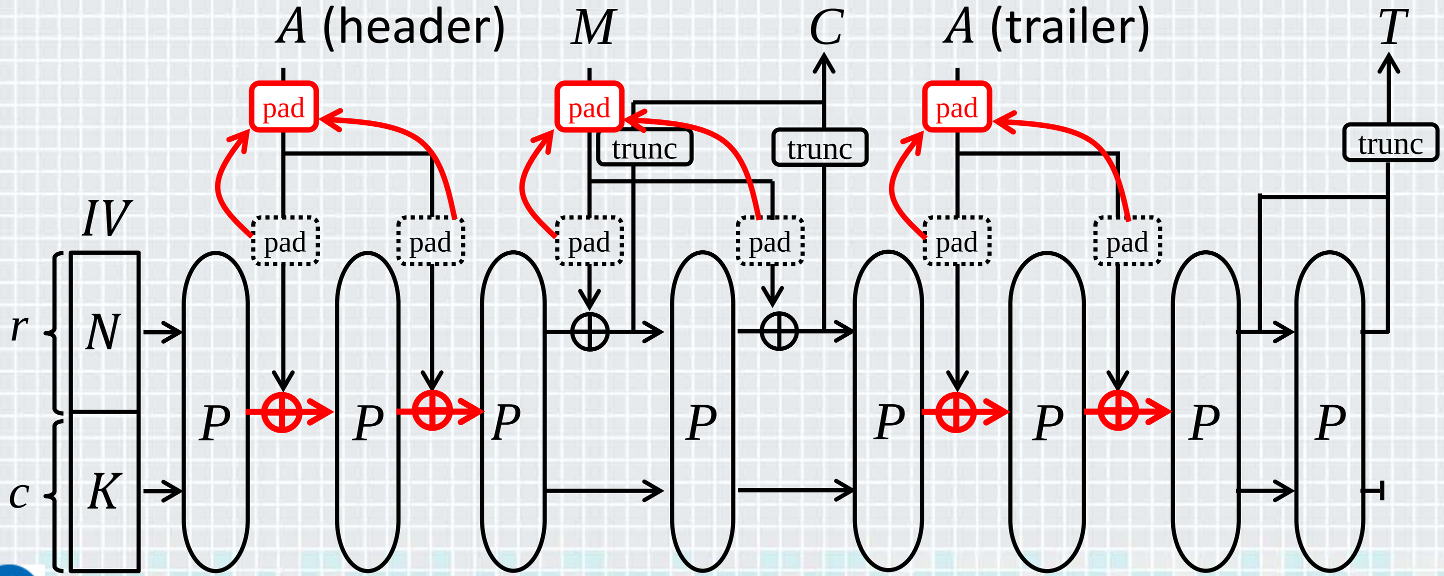
Simple Construction

- Introducing Donkey for associated data
- SpongeWrap + monkeyDuplex + donkeySponge + Header/Trailer



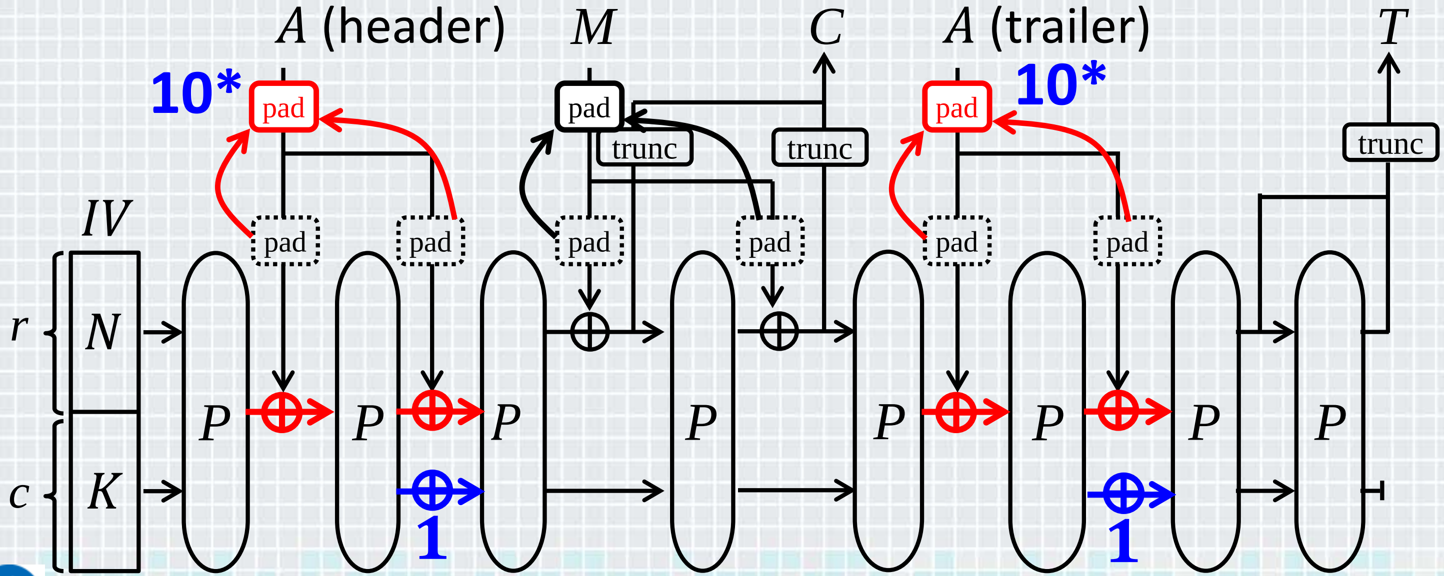
Avoiding Frame bits

- New padding schemes are necessary
- New domain separations are necessary



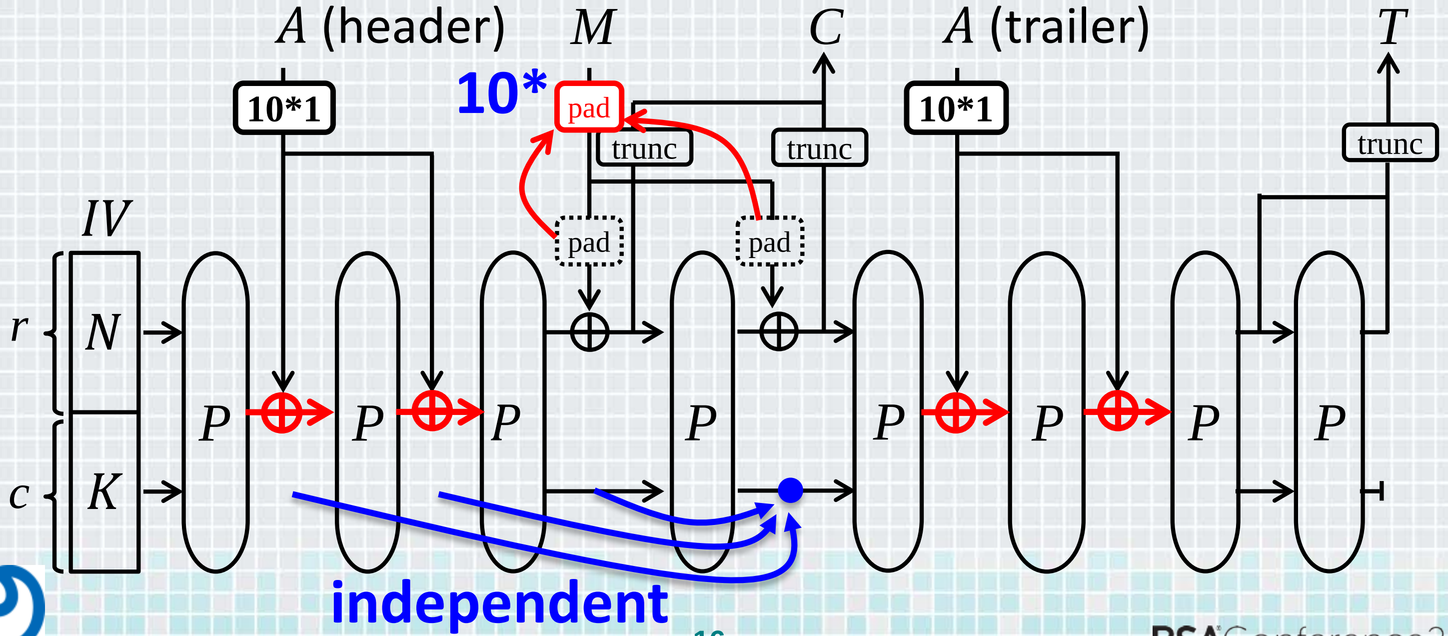
Padding for A

- 10* padding for the last block
- Constant addition for the outer part of the last block → **10*1 padding**



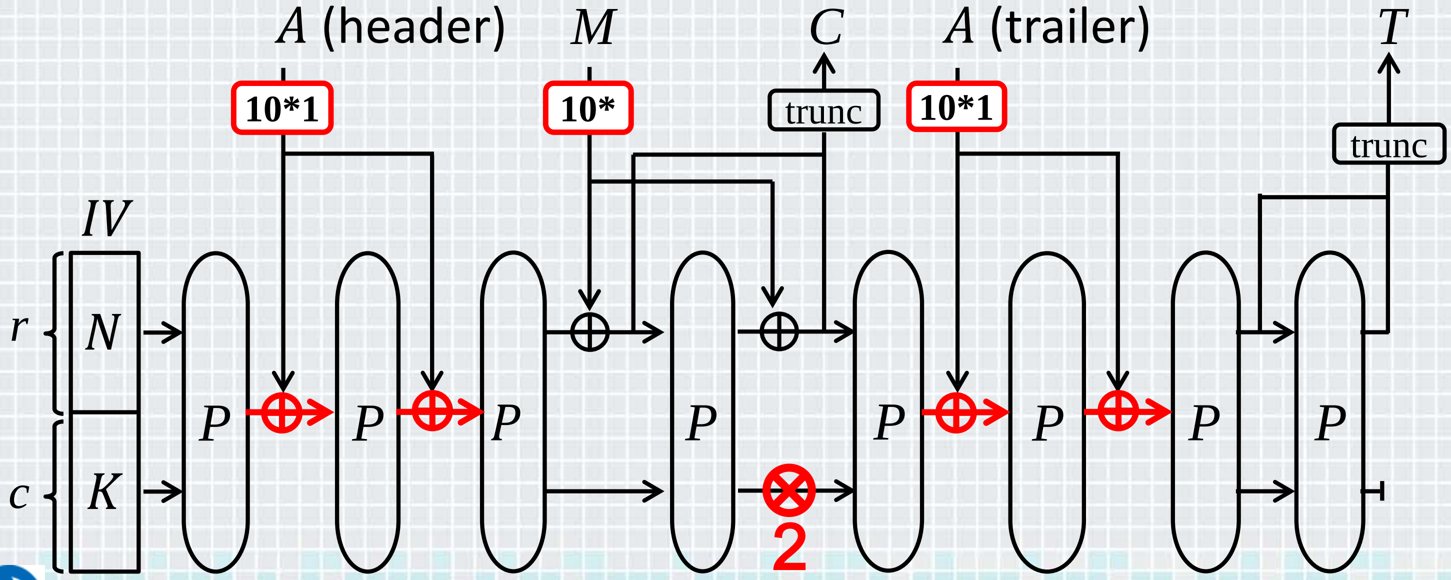
Padding for *M*

- 10* padding for the last block
- Outer part of the last block must be independent of the previous blocks



Construction 1: donkeyHeaderTreailer

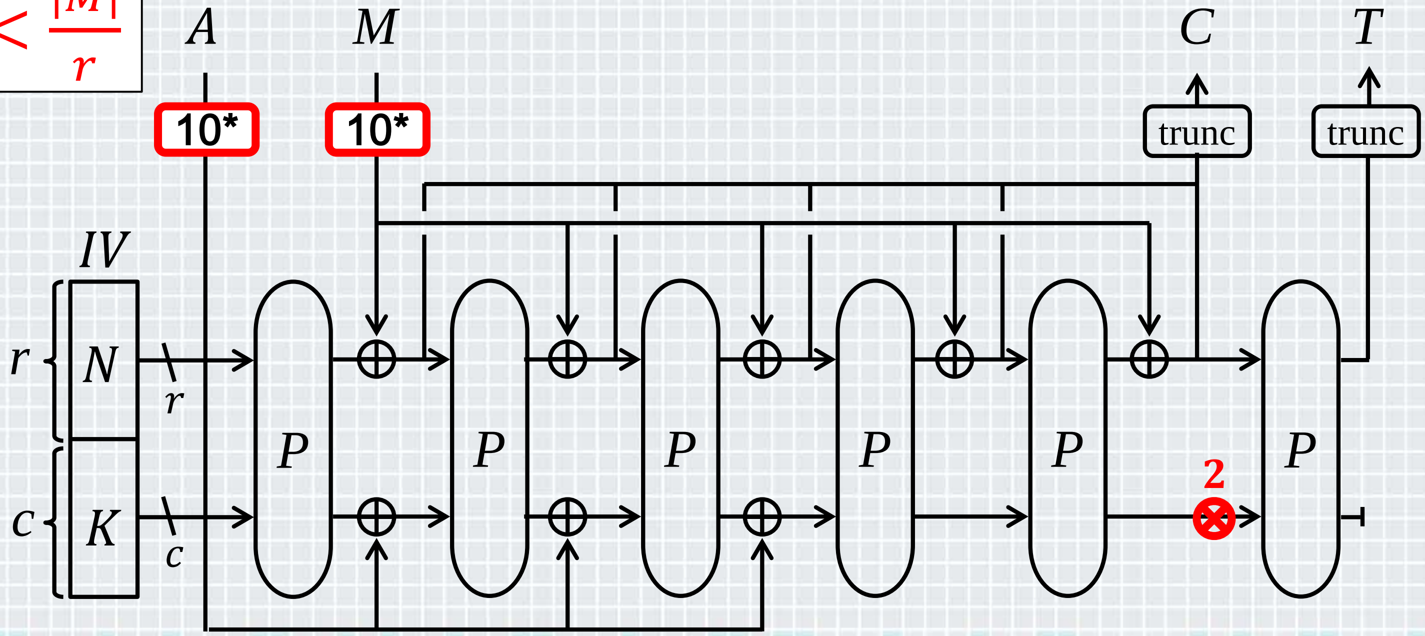
- The same security bound as Jovanovic et al. at Asiacrypt 2014.



Construction 2: Concurrent Absorption

- Absorb M in r bits, absorb A in c bits, simultaneously

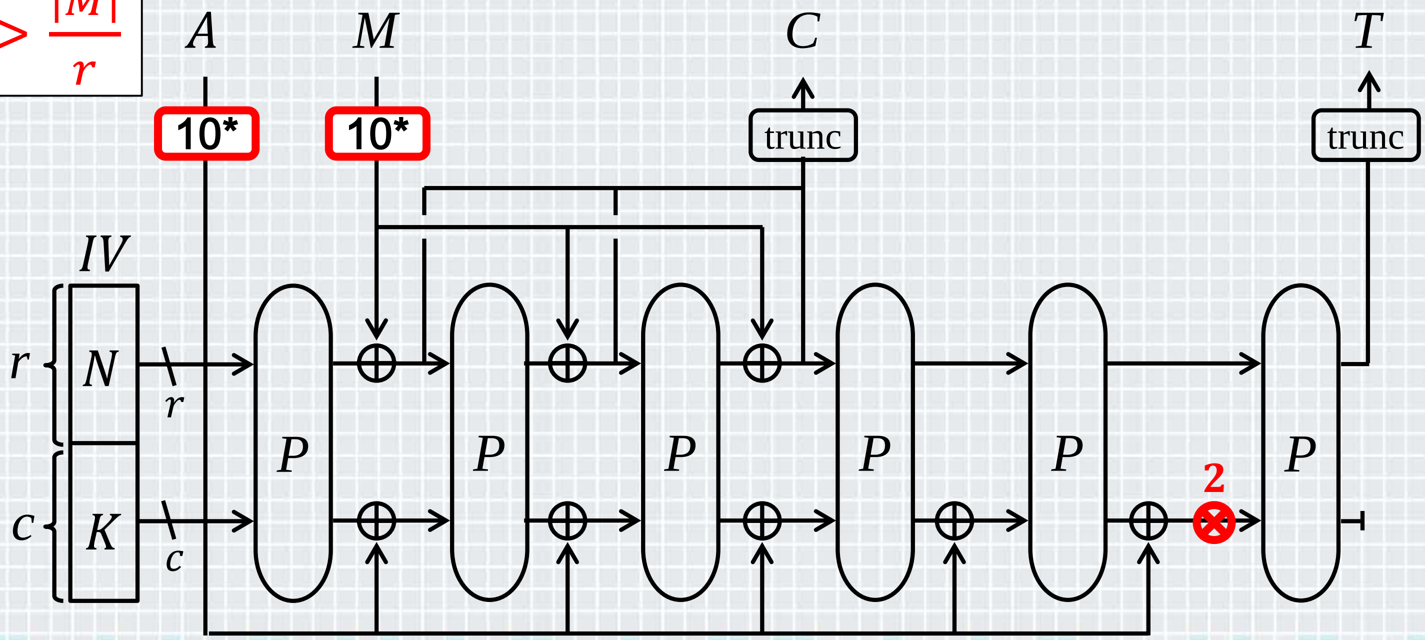
case: $\frac{|A|}{c} < \frac{|M|}{r}$



Construction 2: Concurrent Absorption

- Absorb M in r bits, absorb A in c bits, simultaneously

case: $\frac{|A|}{c} > \frac{|M|}{r}$

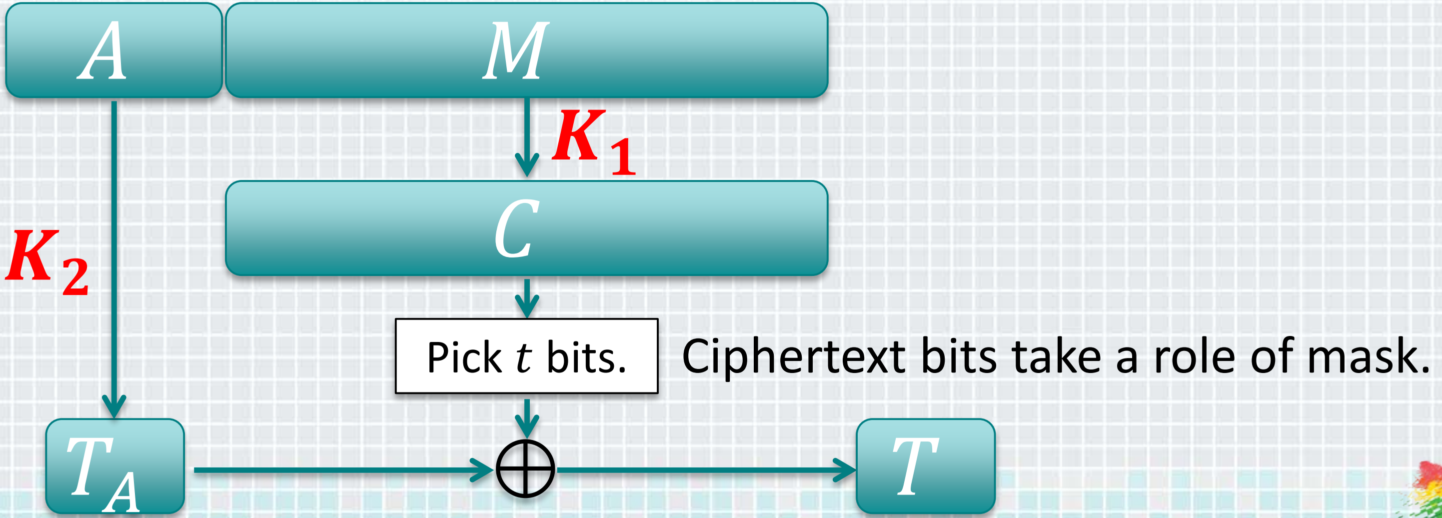


Remarks on Concurrent Absorption

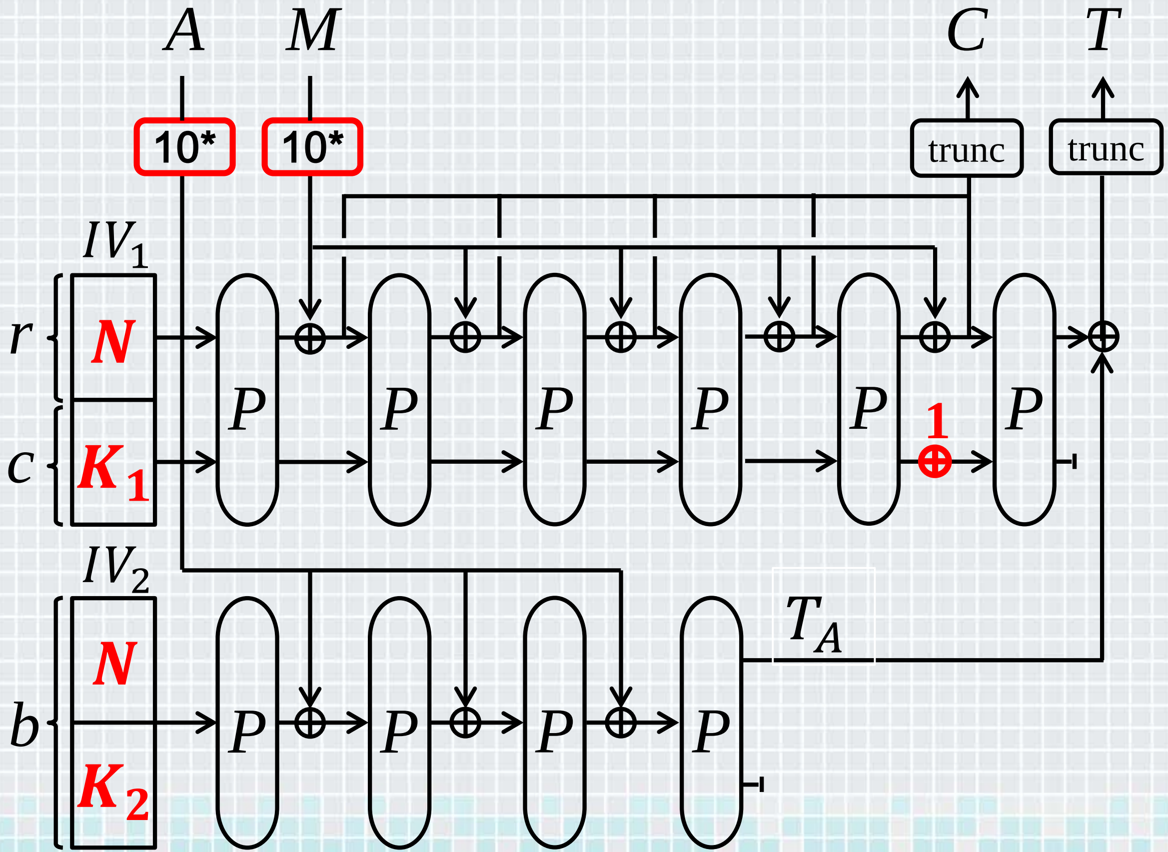
- The number of P calls is minimized.
  - minimum power consumption (Green CRYPTO!!)
  - suitable for light-weight circumstances
- A, M must be provided in suitable timing.
  - wouldn't be a problem if A and M can be stored
- When $A < M$, A is processed with free of cost.

Ciphertext Translation (CT)

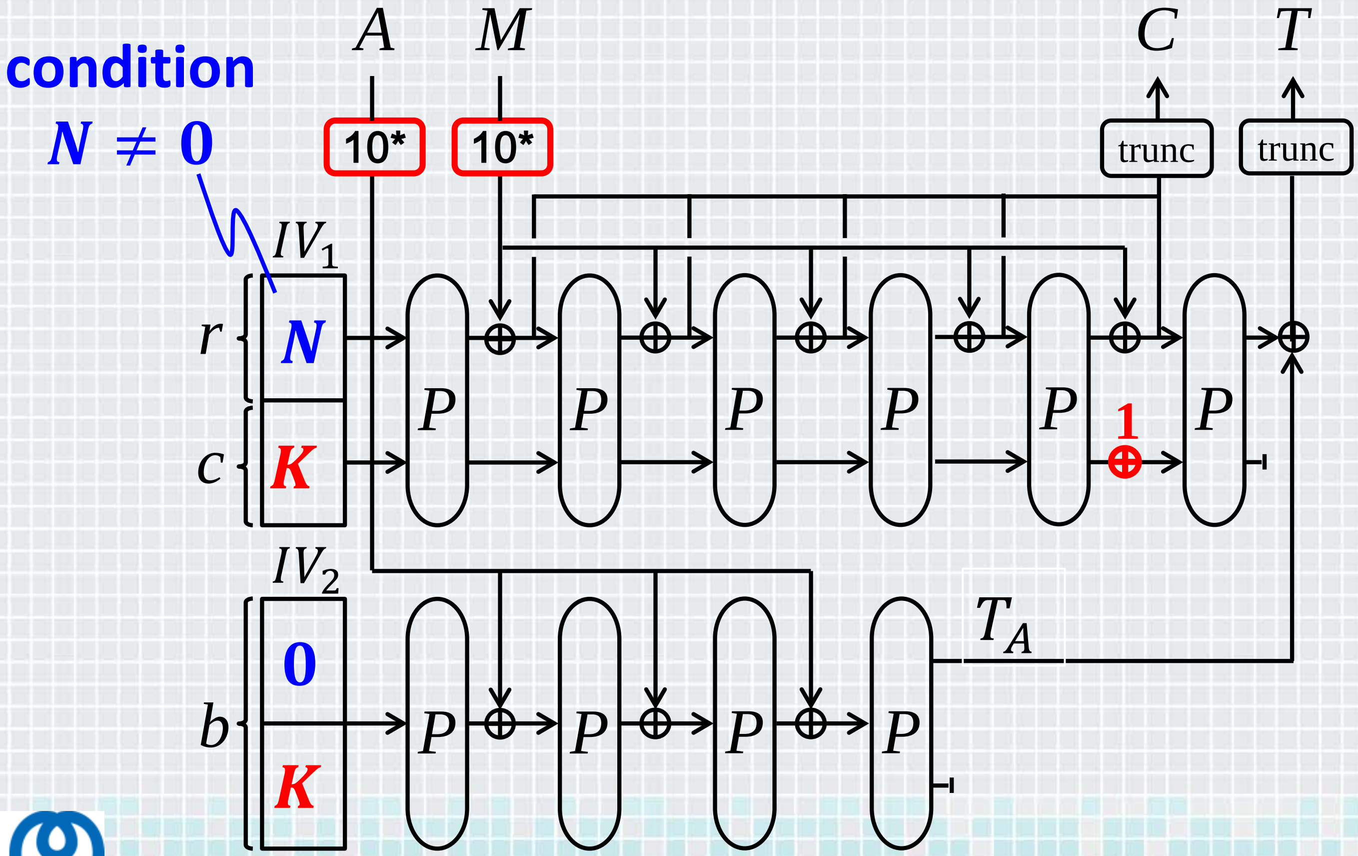
- Proposed by Rogaway to process A and M independently.
- Tag for A is later masked by a part of ciphertext.
- secure in the nonce-respecting setting



Construction 3: Sponge-Based CT (two keys)



Construction 3: Sponge-Based CT (one key)

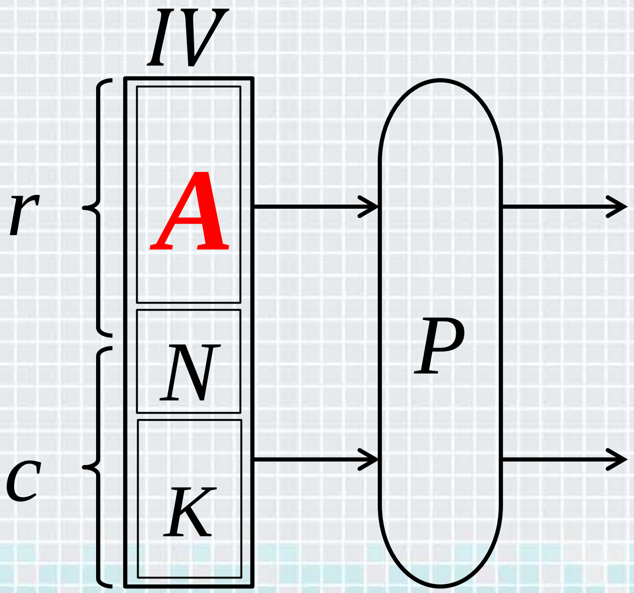


#RSAC

Further Optimization

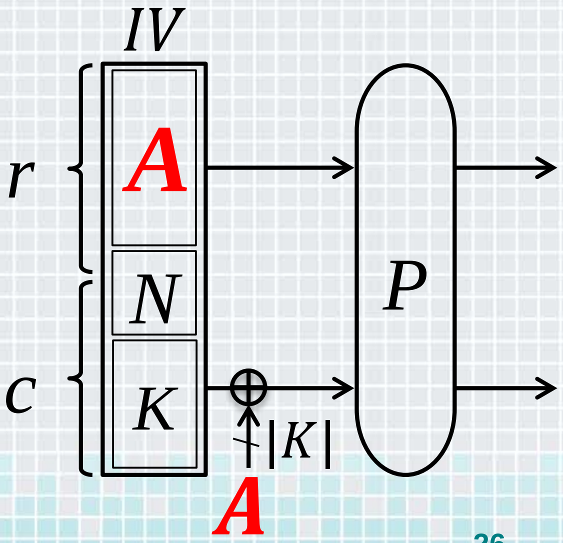
Nonce Stealing in Sponge

- Nonce stealing was proposed by Rogaway.
- IV is usually big in sponge. Many bits of A can be embedded.



Key Translation

- Absorb $|K|$ more bits of A during the initialization
  - Trivial related-key attacks
  - Trivial key-length-extension attacks
  - Key recovery with $2^{K/2}$ in the nonce-repeat setting



Concluding Remarks

Concluding Remarks

- Proposal of three Sponge variants focusing on associated data

  donkeyHeaderTrailer / Concurrent Absorption / Sponge-Based Ciphertext Translation

  - high efficiency / implementation flexibility
  - the same level of the provable security as the ordinary sponge
  - Avoiding frame bits

- Further efficiency optimization with techniques for block-ciphers

  Nonce stealing / Key translation

Thank you for your attention!!

TU Graz

Analysis of ASCON

Ch. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer
Graz University of Technology

April 2015

Overview

- Broad analysis of CAESAR candidate ASCON-128

- Attacks on round-reduced versions
  - Key-recovery (6/12 rounds)
  - Forgery (4/12 rounds)

CAESAR

- CAESAR: Competition for Authenticated Encryption – Security, Applicability, and Robustness
  - http://competitions.cr.yp.to/caesar.html

- Inspired by
  - AES
  - SHA-3
  - eStream

CAESAR – Candidates

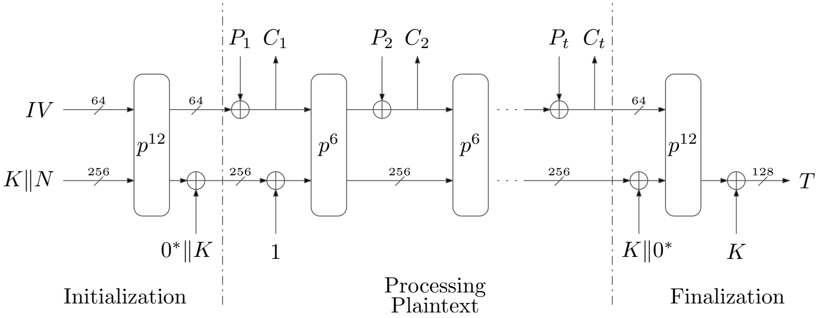
ACORN	++AE	AEGIS	AES-CMCC
AES-COBRA	AES-COPA	AES-CPFB	AES-JAMBU
AES-OTR	AEZ	Artemia	Ascon
AVALANCHE	Calico	CBA	CBEAM
CLOC	Deoxys	ELmD	Enchilada
FASER	HKC	HS1-SIV	ICEPOLE
iFeed[AES]	Joltik	Julius	Ketje
Keyak	KIASU	LAC	Marble
McMambo	Minalpher	MORUS	NORX
OCB	OMD	PAEQ	PAES
PANDA	π-Cipher	POET	POLAWIS
PRIMATEs	Prøst	Raviyoyla	Sablier
SCREAM	SHELL	SILC	Silver
STRIBOB	Tiaoxin	TriviA-ck	Wheesht
YAES			

ASCON – Design Goals

- Security
- Efficiency
- Lightweight
- Simplicity
- Online
- Single pass
- Scalability
- Side-Channel Robustness

ASCON – General Overview

- Focus on ASCON-128
- Nonce-based AE scheme
- Sponge inspired

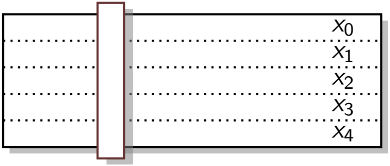


ASCON – Permutation

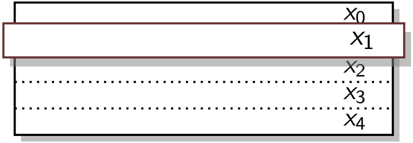
- Iterative application of round function
- One round
  - Constant addition
  - Substitution layer
  - Linear layer

ASCON – Round

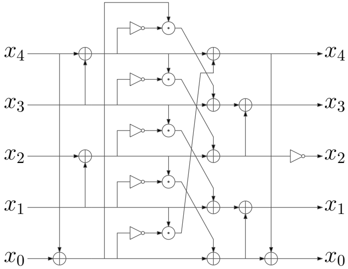
- Substitution layer



- Linear layer



ASCON – Round



S-box

$$
\begin{aligned}
x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41) &\to x_4 \\
x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) &\to x_3 \\
x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) &\to x_2 \\
x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39) &\to x_1 \\
x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) &\to x_0
\end{aligned}
$$

Linear transformation

Ch. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer

Analysis – ASCON

- Attacks on round-reduced versions of ASCON-128
  - Key-recovery
  - Forgery
- Analysis of the building blocks
  - Permutation

Key-recovery – Idea

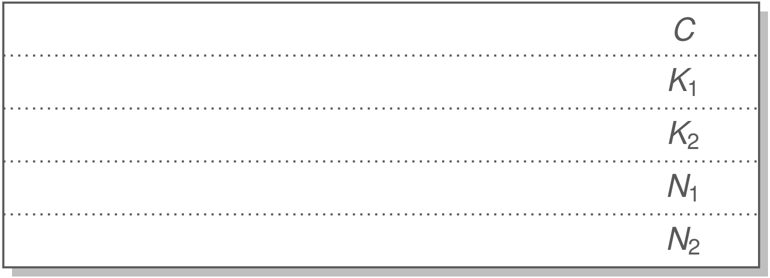
- Target initialization
- Choose nonce
- Observe key-stream
- Deduce information about the secret key

	rounds	time	method
ASCON-128	6 / 12	2^{66}	cube-like
	5 / 12	2^{35}	
	5 / 12	2^{36}	differential-linear
	4 / 12	2^{18}	

Cube-like Attack – Idea

- Key-recovery attack based on Dinur et al. [DMP+15]
- Utilizes low algebraic degree of one round
- Output bits of initialization function of input bits
- Choose cube variables so that cube sum only depends on a fraction of all key bits
- Now able to create a “fingerprint” of a part of the secret key

Initialization – Input



Cube-like Attack – Cube Tester

- Take all cube variables from N_1
- After **one** round **one** cube variable per term
- After **two** rounds **two** cube variables per term
- After **6** rounds **32** cube variables per term

Cube-like Attack – Cube Tester

- Take all cube variables from N_1
- After **one** round **one** cube variable per term
- After **two** rounds **two** cube variables per term
- After **6** rounds **32** cube variables per term

- Take 33 cube variables from N_1
- Cube sum after 6 rounds definitely zero
- Although degree about 64

Cube-like Attack – Borderline Cubes

- Take 32 cube variables from N_2 e.g. $N_2[0..31]$
- Degree after 6 rounds about 64
- Cube sum result of non-linear equation
- Which variables are involved?

Cube-like Attack – After first S-Layer

$$x_0[i] = N_2[i]K_1[i] + N_1[i] + K_2[i]K_1[i] + K_2[i] + K_1[i]C[i] + K_1[i] + C[i]$$
$$x_1[i] = N_2[i] + N_1[i]K_2[i] + N_1[i]K_1[i] + N_1[i] + K_2[i]K_1[i] + K_2[i] + K_1[i] + C[i]$$
$$x_2[i] = N_2[i]N_1[i] + N_2[i] + K_2[i] + K_1[i] + 1$$
$$x_3[i] = N_2[i]C[i] + N_2[i] + N_1[i]C[i] + N_1[i] + K_2[i] + K_1[i] + C[i]$$
$$x_4[i] = N_2[i]K_1[i] + N_2[i] + N_1[i] + K_1[i]C[i] + K_1[i]$$

Cube-like Attack

- Take 32 cube variables from N_2 e.g. $N_2[0..31]$
- Cube sum after 6 rounds result of non-linear equation
  - Known constants
  - Key-bits $K_1[0..31]$
  - **Not** key-bits $K_1[32..63]$
  - **Not** key-bits $K_2[0..63]$

Ch. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer

Cube-like Attack – 6/12 Rounds

- Online Phase: Take fingerprint of 32 key-bits
- Offline Phase: Match fingerprint by brute-forcing those 32 key-bits

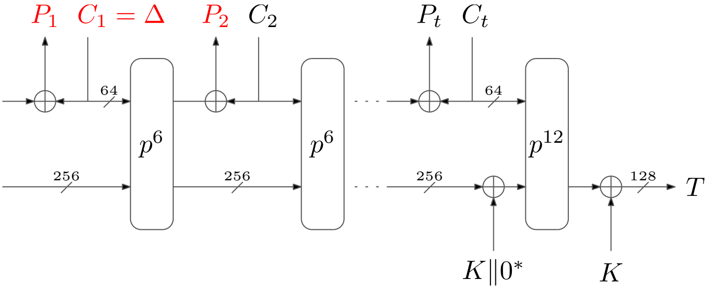
Cube-like Attack – 6/12 Rounds

- Online Phase: Take fingerprint of 32 key-bits
- Offline Phase: Match fingerprint by brute-forcing those 32 key-bits
- For 5/12 rounds, attack has practical complexity and has been implemented

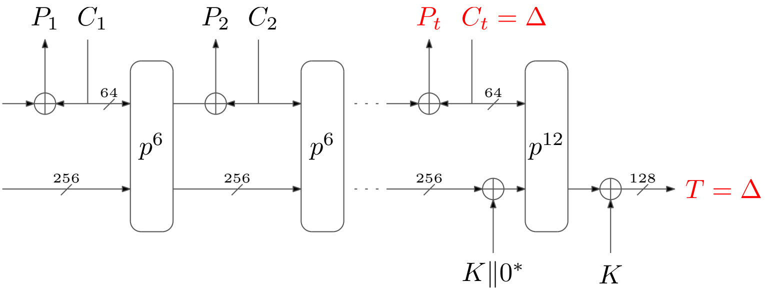
Forgery – Idea

- Based on differential cryptanalysis
- Create forgeries from known ciphertext and tag pairs
  - Target encryption
  - Target finalization
- Need for good differential characteristics

Forgery – ASCON-128



Forgery – ASCON-128



Forgery – ASCON-128

- 3/12 rounds finalization probability 2^{-33}

	input difference		after 1 round		after 2 rounds		after 3 rounds
x_0	8000000000000000		8000100800000000		8000000002000080		????????????????
x_1	0000000000000000		8000000001000004		9002904800000000		????????????????
x_2	0000000000000000	$\rightarrow$	0000000000000000	$\rightarrow$	d200000001840006	$\rightarrow$	????????????????
x_3	0000000000000000		0000000000000000		0102000001004084		4291316c5aa02140
x_4	0000000000000000		0000000000000000		0000000000000000		090280200302c084

- 4/12 rounds finalization probability 2^{-101}

	input difference		after 4 rounds
x_0	8000000000000000		????????????????
x_1	0000000000000000		????????????????
x_2	0000000000000000	$\rightarrow$	????????????????
x_3	0000000000000000		280380ec6a0e9024
x_4	0000000000000000		eb2541b2a0e438b0

Ch. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer
April 2015

Analysis – Permutation

- Zero-sum distinguisher 12 rounds with complexity 2^{130}
- Search for differential and linear characteristics
- Proof on minimum number of active S-boxes

result	rounds	differential	linear
proof	1	1	1
	2	4	4
	3	15	13
heuristic	4	44	43
	≥ 5	> 64	> 64

Conclusion

- Many state-of-the-art techniques applied
- ASCON provides a large security margin
- For more information visit http://ascon.iaik.tugraz.at

Analysis of ASCON

Ch. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer
Graz University of Technology

April 2015

Reference

[CAE14] CAESAR committee.

CAESAR: Competition for authenticated encryption: Security, applicability, and robustness.

`http://competitions.cr.yp.to/caesar.html`, 2014.

[DEMS14] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.

Ascon.

Submission to the CAESAR competition: `http://ascon.iaik.tugraz.at`, 2014.

[DMP+15] Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michal Straus.

Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak Sponge Function.

Proceedings of EUROCRYPT 2015 (to appear), 2015.