AUTHENTICATED ENCRYPTION

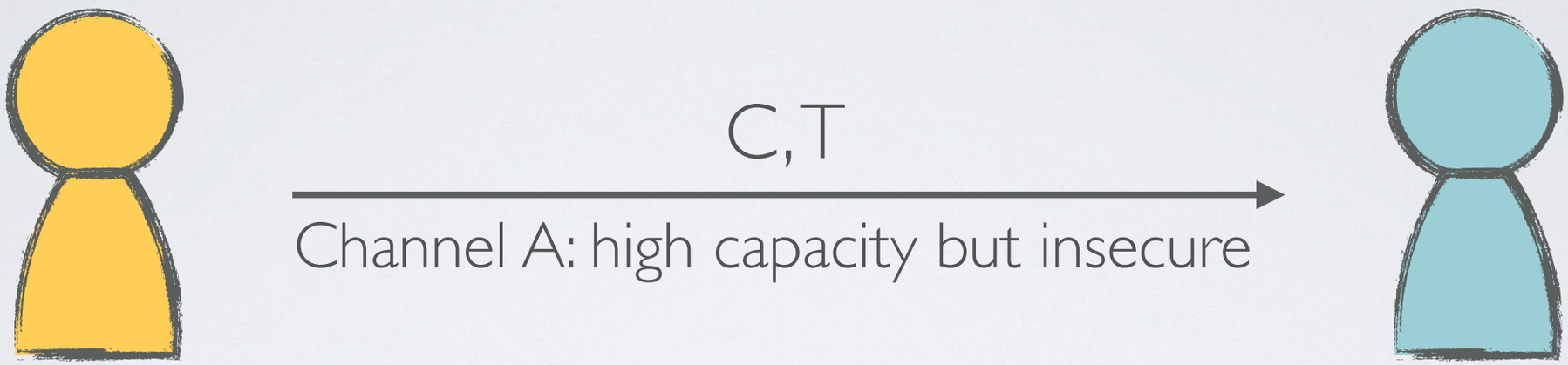
Florian Mendel

Central European Conference on Cryptology
June 24 - 26, 2020

GOALS

- **Confidentiality**
  - as provided by block cipher modes
- **Authenticity, integrity**
  - as provided by message authentication codes

INTERFACE



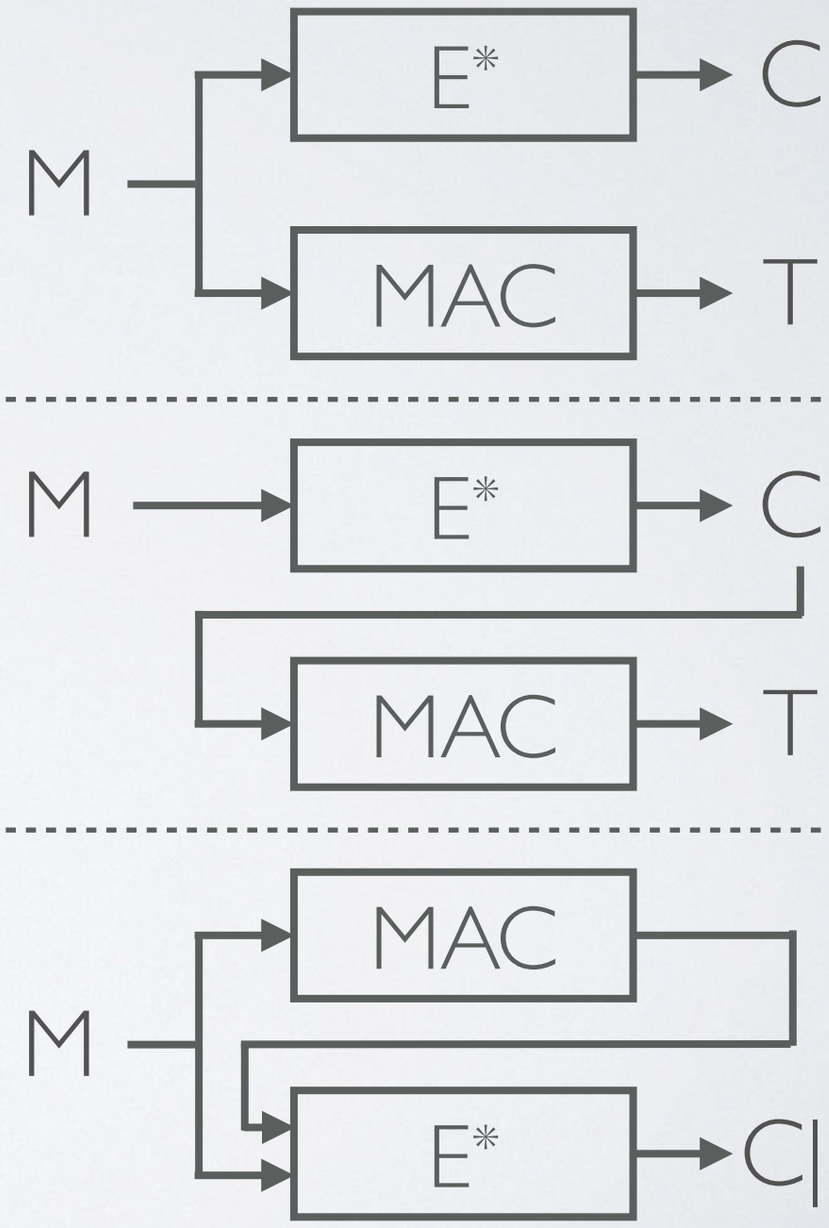
- **Encryption & Authentication**
  - (K, M) ⇒ (C, T)
- **Decryption & Verification**
  - (K, C, T) ⇒ {M, ⊥}

INTERFACE

- **Encryption & Authentication**
  - (K, N, A, M) ⇒ (C, T)
- **Decryption & Verification**
  - (K, N, A, C, T) ⇒ {M, ⊥}

GENERIC COMPOSITIONS

- **Encrypt-and-MAC (E&M)**
  - C = E^*(M), T = MAC(M)
- **Encrypt-then-MAC (EtM)**
  - C = E^*(M), T = MAC(C)
- **MAC-then-Encrypt (MtE)**
  - C||T = E^*(M || MAC(M))



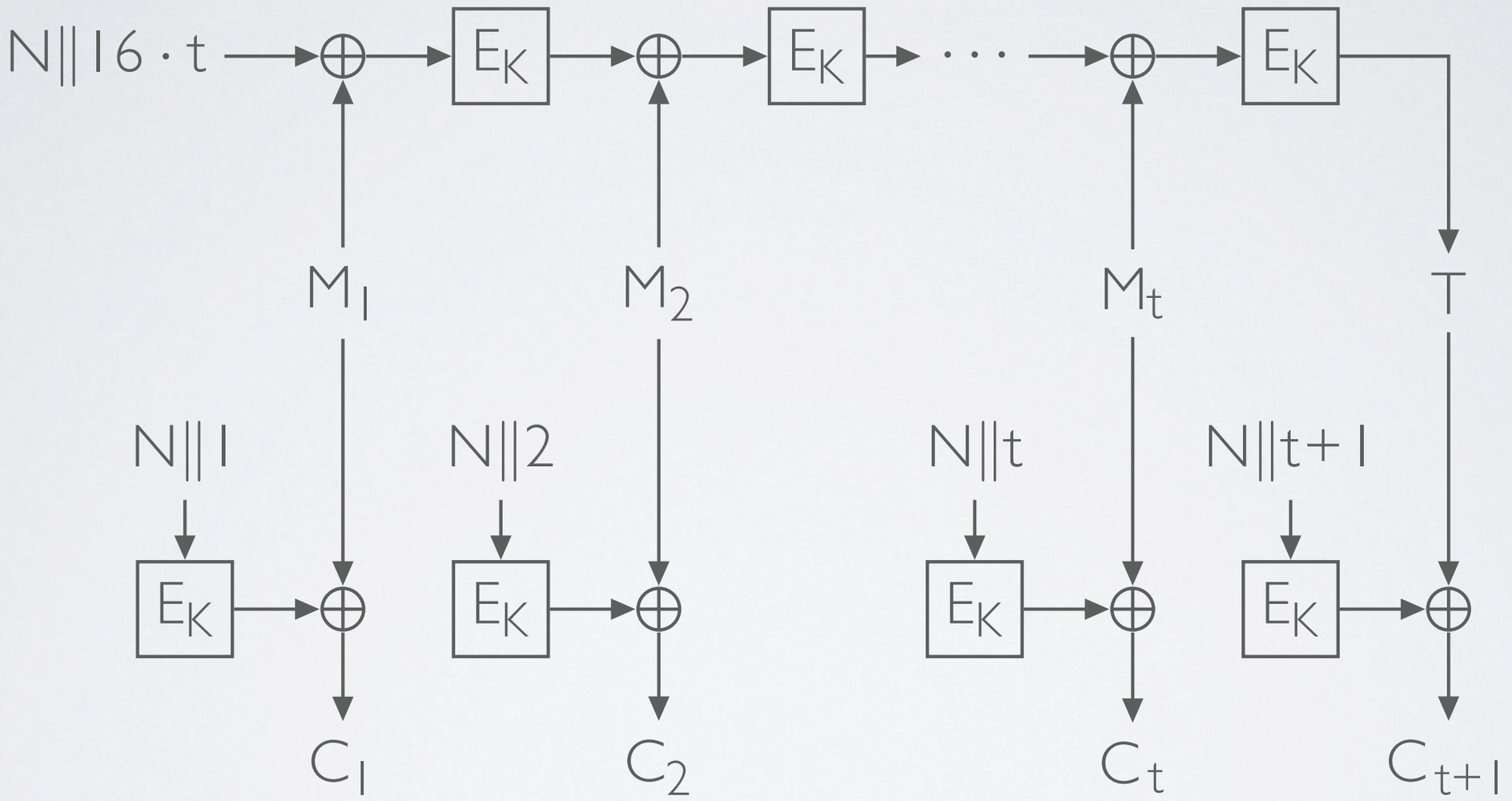
GENERIC COMPOSITIONS

- **Encrypt-and-MAC (E&M)**
  - e.g., in SSH
  - security depends on E^* and MAC details
- **Encrypt-then-MAC (EtM)**
  - e.g., in IPSec; standard ISO/IEC 19772:2009
  - provably secure
- **MAC-then-Encrypt (MtE)**
  - e.g., in SSL/TLS
  - security depends on E^* and MAC details

STANDARDISED SCHEMES

- ISO/IEC specifies six AE modes for block ciphers
  - EtM, CCM, EAX, GCM, OCB, SIV

CCM – CTR AND CBC-MAC



- MtE with CTR encryption mode and CBC-MAC

Image: Maria Eichlseder

CCM PROPERTIES

✓Secure for ideal cipher E_K

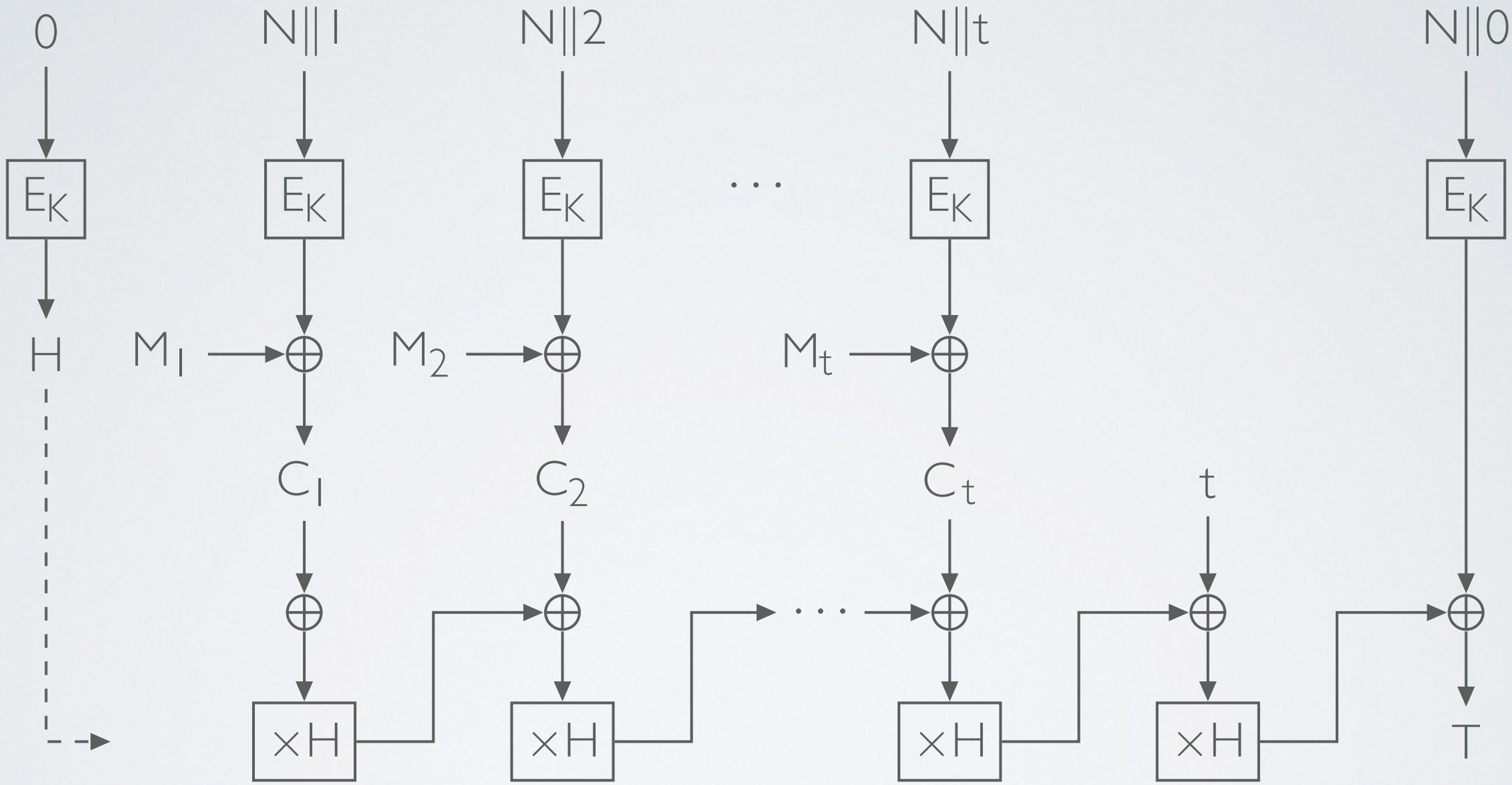
✓Needs no D_K (decryption)

✗Two block cipher calls per block

✗Two-pass, not online (need length in advance)

✗CBC-MAC not parallelizable

GCM – GALOIS/CTR MODE



- EtM with CTR and Carter-Wegman MAC

Image: Maria Eichlseder

GCM PROPERTIES

✓E_K parallelizable

✓Needs no DK (decryption)

✓one block cipher call per block

✗Harder to implement (nasty multiplications)

✗Some weak keys due to MAC properties

COMPETITIONS

- CAESAR (2014 - 2019)
- NIST LWC (ongoing)

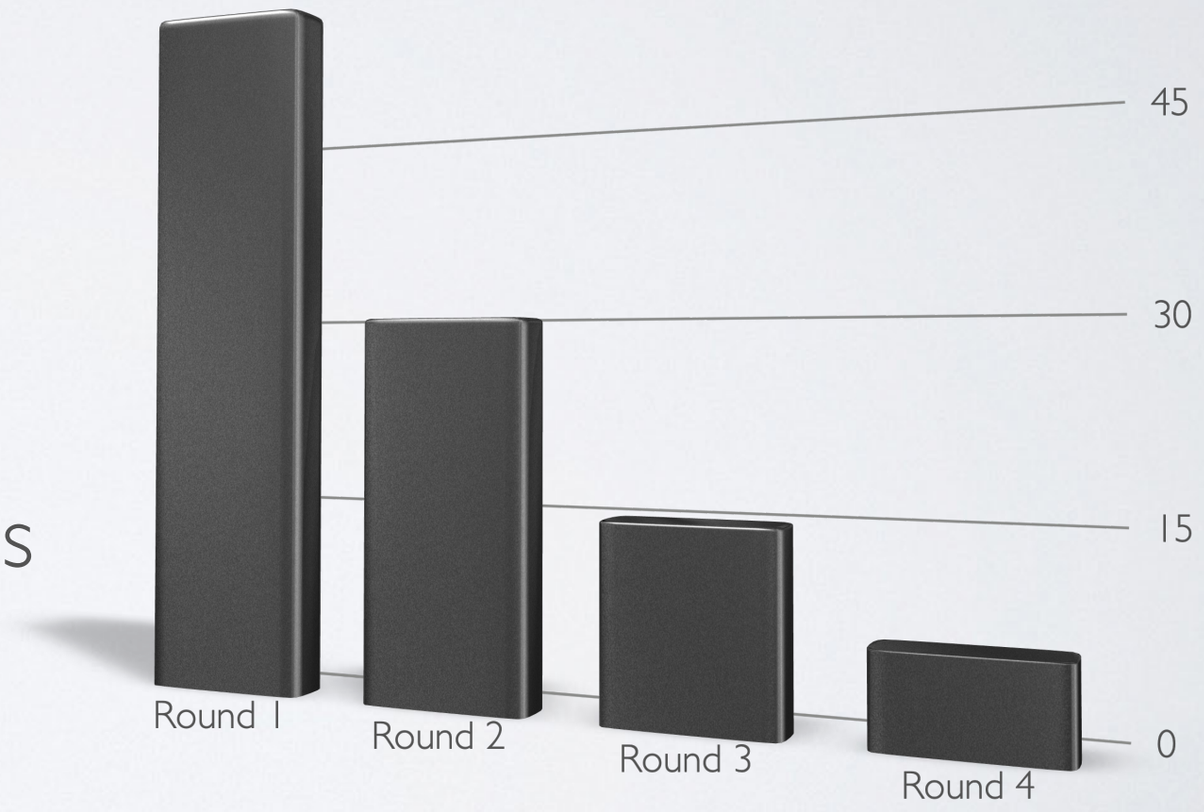
CAESAR

Goal: Select portfolio of authenticated ciphers

Timeline: 2014 - 2019, 4 rounds

Categories:

- Lightweight applications
- High-performance applications
- Defense in depth



CAESAR PORTFOLIO

- **Lightweight applications**
  - Ascon and ACORN
- **High-performance applications**
  - AEGIS and OCB
- **Defense in depth**
  - Deoxys-II and COLM

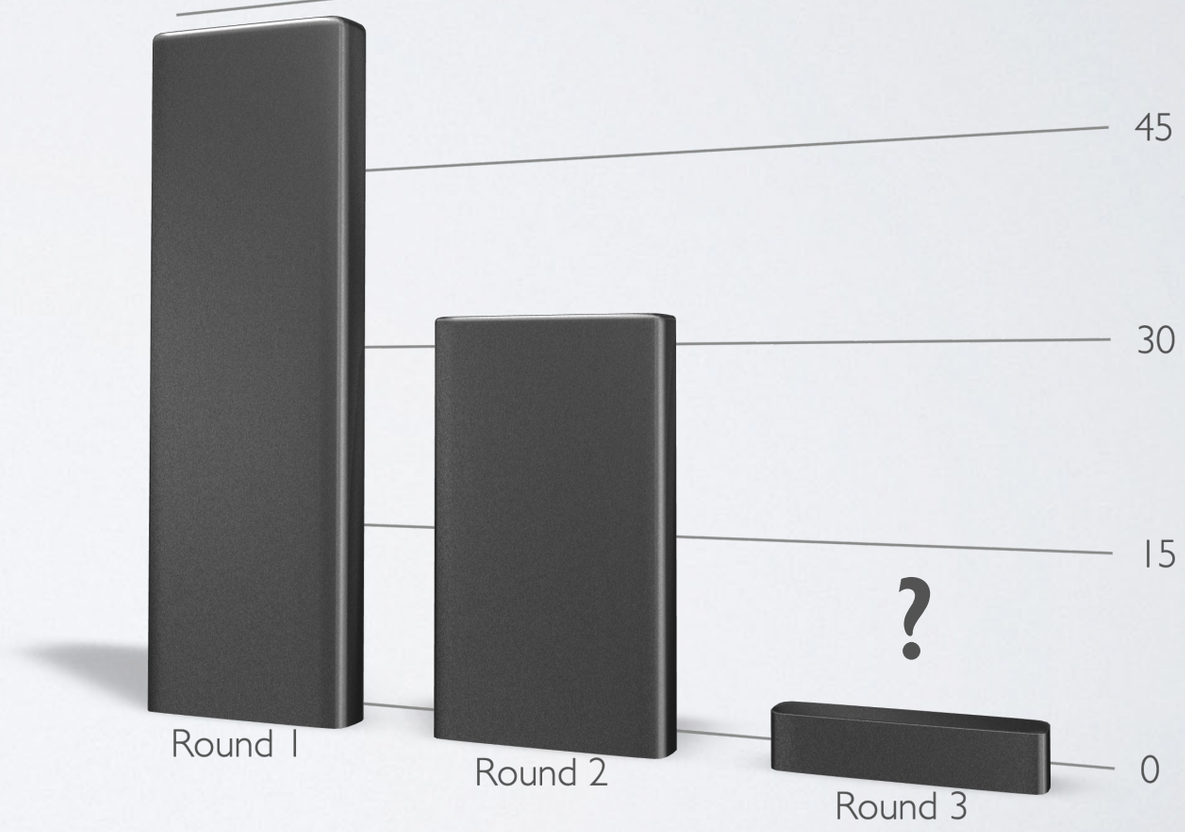
NIST LWC

Goal: Select authenticated ciphers for standardisation

Timeline: 2018 - now

Category:

- Lightweight applications



ROUND 2 CANDIDATES

ACE	**Ascon**	COMET	DryGASCON
Elephant	ESTATE	ForkAE	GIFT-COFB
Gimli	Grain-128AEAD	HYENA	**ISAP**
KNOT	LOTUS & LOCUS	mixFeed	ORANGE
Oribatida	PHOTON-Beetle	Pyjamask	Romulus
SAEAES	Saturnin	SKINNY	SPARKLE
SPIX	SpoC	Spook	Subterranean 2.0
SUNDAE-GIFT	TinyJambu	WAGE	Xoodyak

ASCON

AUTHENTICATED ENCRYPTION AND HASHING

ASCON TEAM

- Christoph Dobraunig

- Maria Eichlseder

- Florian Mendel

- Martin Schläffer

ASCON FAMILY

- Authenticated encryption (CAESAR)
  - Ascon-128
  - Ascon-128a
- Hashing (NEW)
  - Ascon-Hash
  - Ascon-Xof (eXtendable output function)

MAIN DESIGN GOALS

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

AUTHENTICATED ENCRYPTION

- Nonce-based AE scheme
- Sponge construction

	ASCON-128	ASCON-128a
Security	128 bits	128 bits
State size	320 bits	320 bits
Capacity	256 bits	192 bits
Rate (r)	64 bits	128 bits

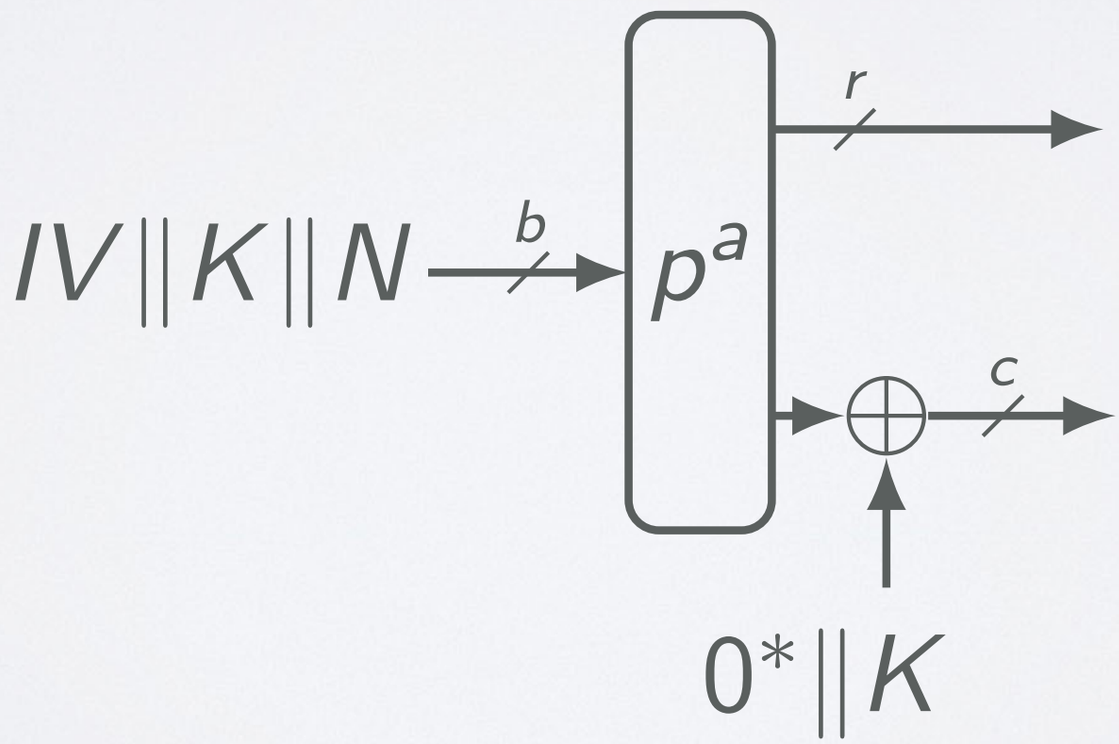
WORKING PRINCIPLE

The encryption process is split into four phases:

- Initialisation
- Associated Data Processing
- Plaintext Processing
- Finalisation

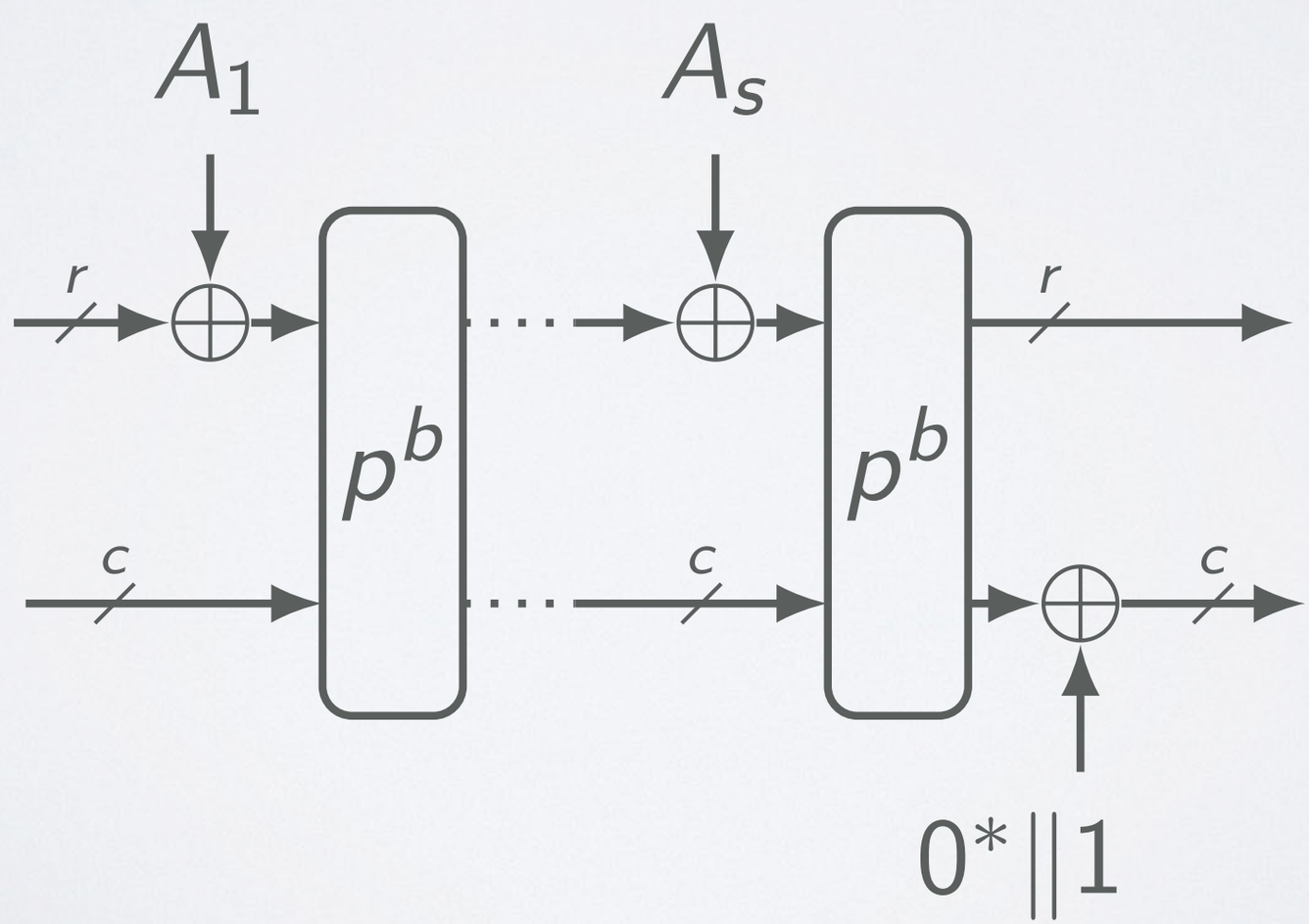
INITIALISATION

- **Initialisation:** updates the 320-bit state with the key K and nonce N



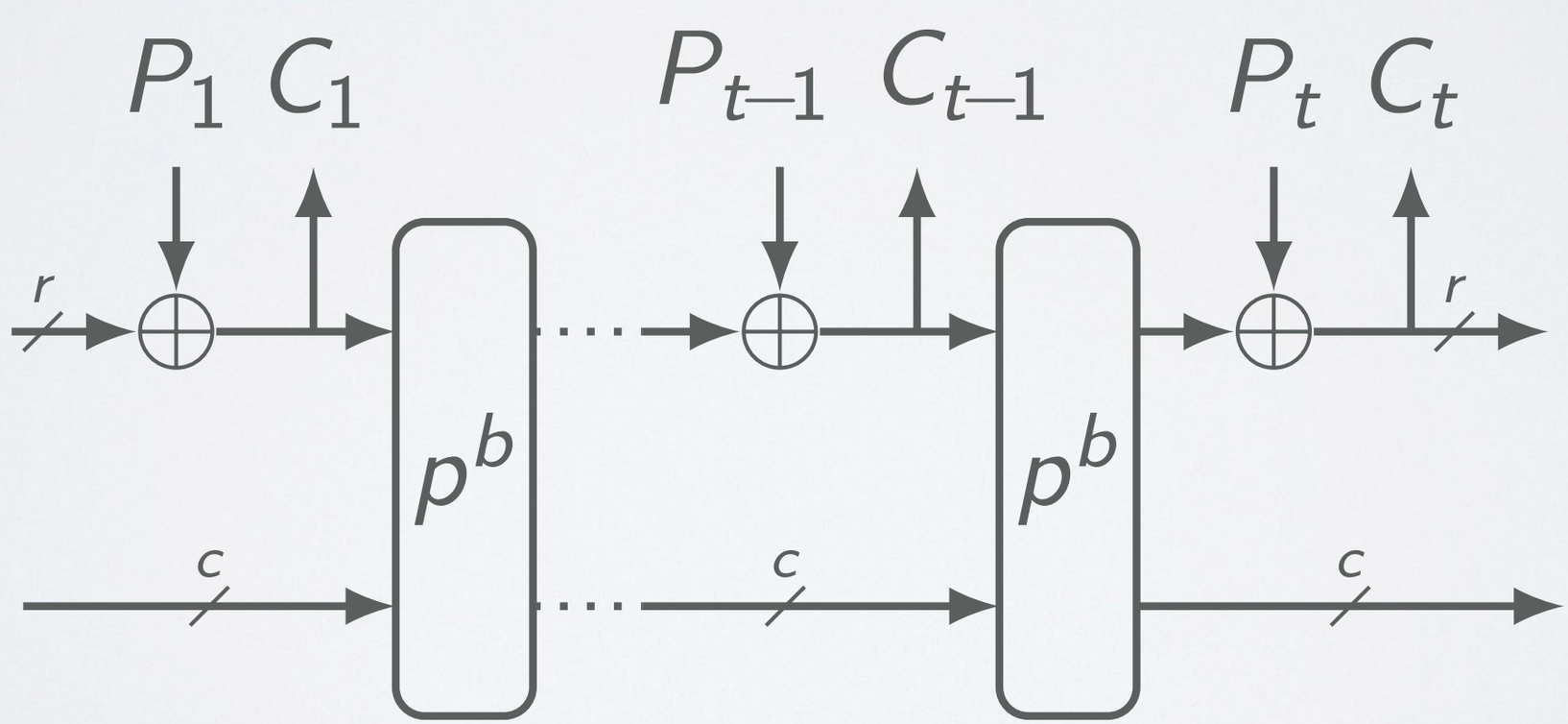
ASSOCIATED DATA

- **Associated Data Processing:** updating the 320-bit state with associated data blocks A_i



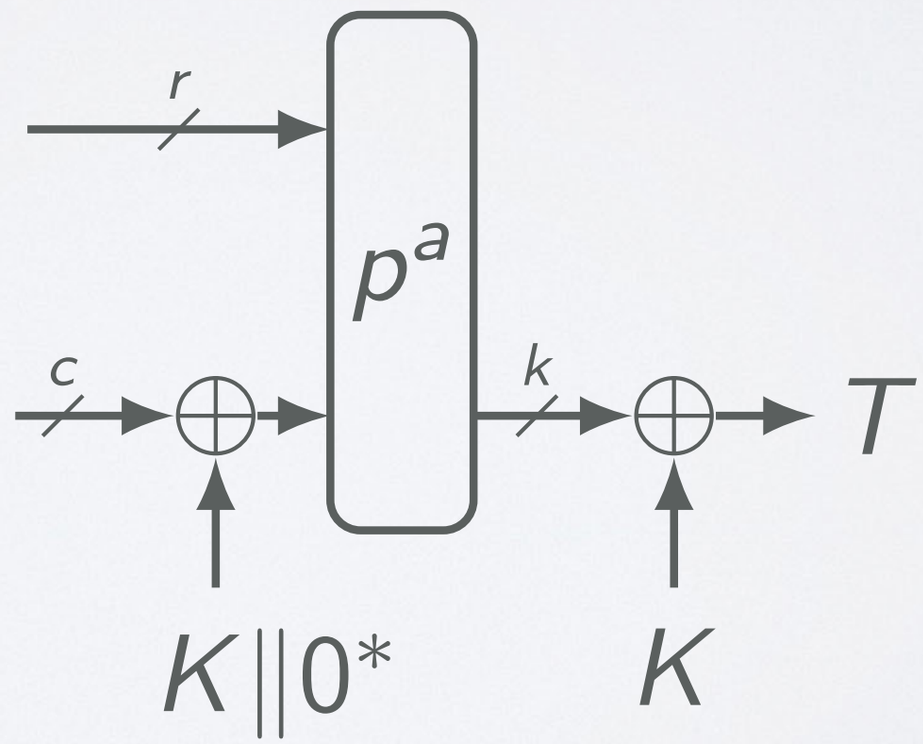
ENCRYPTION

- **Plaintext Processing:** inject plaintext blocks P_i in the state and extract ciphertext blocks C_i



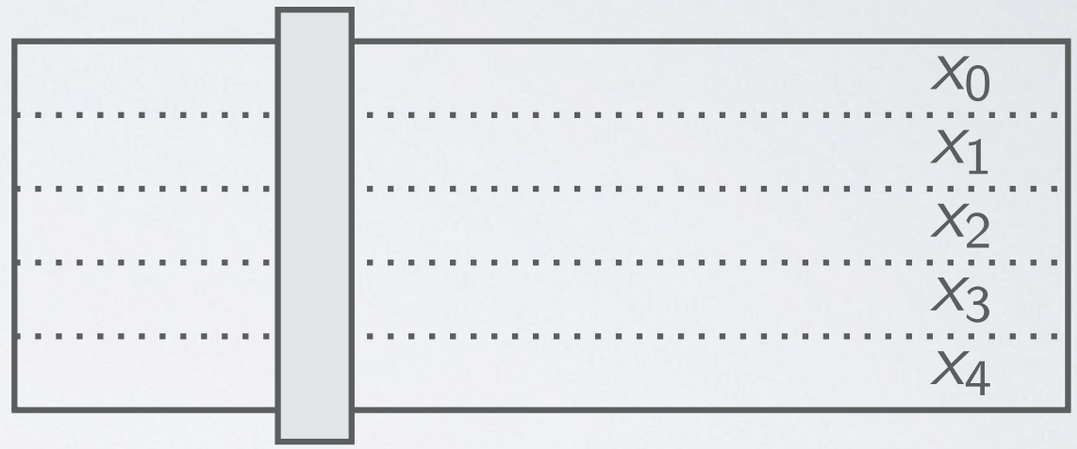
FINALISATION

- **Finalisation:** inject the key K and extracts a tag T for authentication

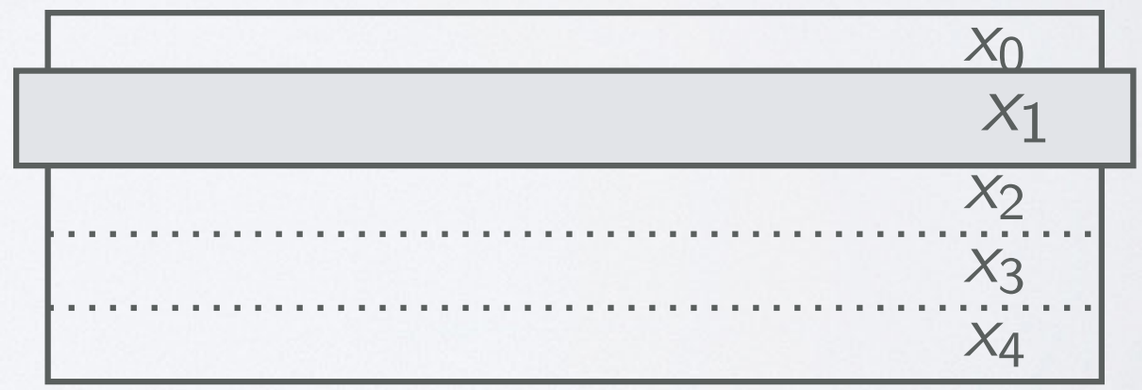


PERMUTATION

- SP-Network:
  - S-Layer:

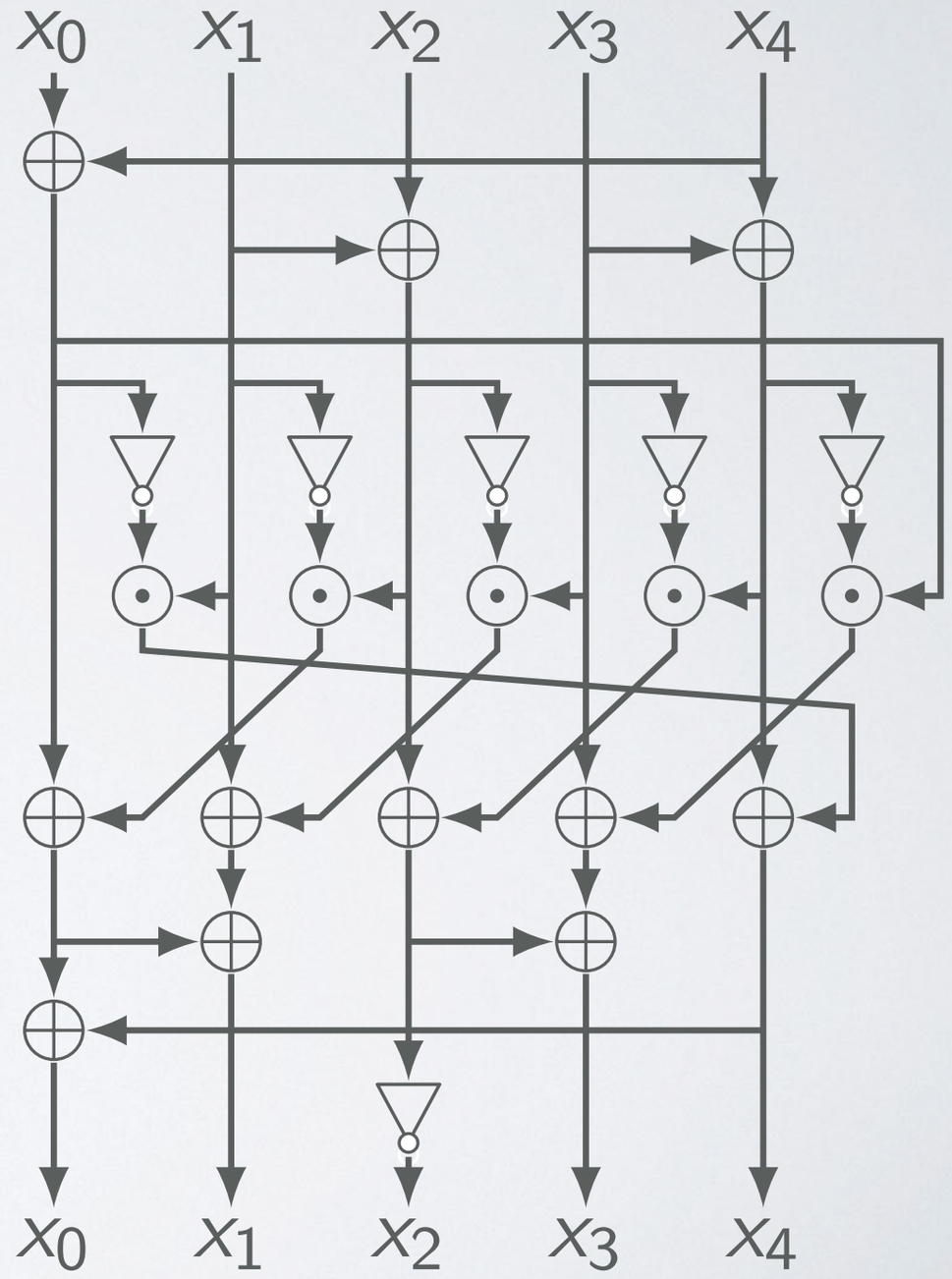


  - P-Layer:



PERMUTATION: S-LAYER

- Algebraic Degree 2
  - Ease TI (3 shares)
- Branch Number 3
  - Good Diffusion
- Bit-sliced Impl.



PERMUTATION: P-LAYER

- Branch Number 4

$$\Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$
$$\Sigma_1(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$
$$\Sigma_2(x_2) = x_2 \oplus (x_2 \ggg \ \ 1) \oplus (x_2 \ggg \ \ 6)$$
$$\Sigma_3(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$
$$\Sigma_4(x_4) = x_4 \oplus (x_4 \ggg \ \ 7) \oplus (x_4 \ggg 41)$$

SECURITY ANALYSIS

- Differential and Linear Cryptanalysis

Rounds	Differential	Linear
1	1	1
2	4	4
3	15	13
4	44	43
…	>64	>64

Asiacrypt 2015

SECURITY ANALYSIS

- Analysis of round-reduced versions

Method	Rounds	Complexity
cube-like	6/12	2^{66}
	7/12	2^{104}
Differential-Linear	4/12	2^{18}
	5/12	2^{36}

CT-RSA 2015, FSE 2017

OTHER ANALYSIS

- Achiya Bar-On, Orr Dunkelman, Nathan Keller, Ariel Weizman. DLCT: A New Tool for Differential-Linear Cryptanalysis. EUROCRYPT 2019

- Gregor Leander, Cihangir Tezcan, Friedrich Wiemer. Searching for Subspace Trails and Truncated Differentials. FSE 2018

- Zheng Li, Xiaoyang Dong, Xiaoyun Wang. Conditional Cube Attack on Round-Reduced ASCON. IACR Transactions on Symmetric Cryptology 2017

- Yanbin Li, Guoyan Zhang, Wei Wang, Meiqin Wang. Cryptanalysis of round-reduced ASCON. Science China Information Sciences 2017

OTHER ANALYSIS

- Ashutosh Dhar Dwivedi, Miloš Klouček, Pawel Morawiecki, Ivica Nikolič, Josef Pieprzyk, Sebastian Wójtowicz. SAT-based Cryptanalysis of Authenticated Ciphers from the CAESAR Competition. 2017

- Faruk Göloglu, Vincent Rijmen, Qingju Wang. On the division property of S-boxes. 2016

- Cihangir Tezcan. Truncated, Impossible, and Improbable Differential Analysis of Ascon. ICISSP 2016

- Yosuke Todo. Structural Evaluation by Generalized Integral Property. EUROCRYPT 2015

OTHER ANALYSIS

- Christoph Dobraunig, Maria Eichlseder, Florian Mendel. Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates. ASIACRYPT 2015

- Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer. Cryptanalysis of Ascon. CT-RSA 2015

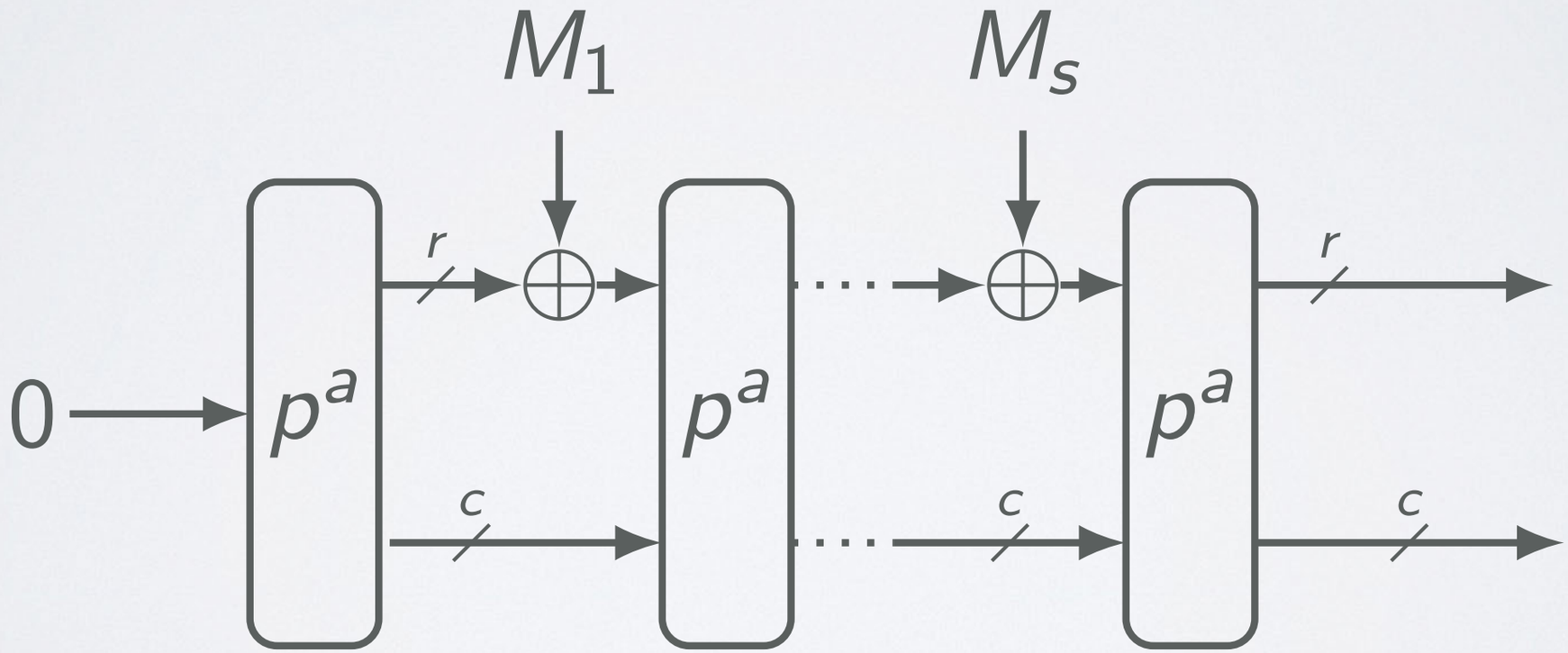
HASHING

- Hash Function and Xof
- Sponge construction

	ASCON-Hash	ASCON-Xof
Hash size	256 bits	variable
State size (b)	320 bits	320 bits
Capacity (c)	256 bits	256 bits
Rate (r)	64 bits	64 bits

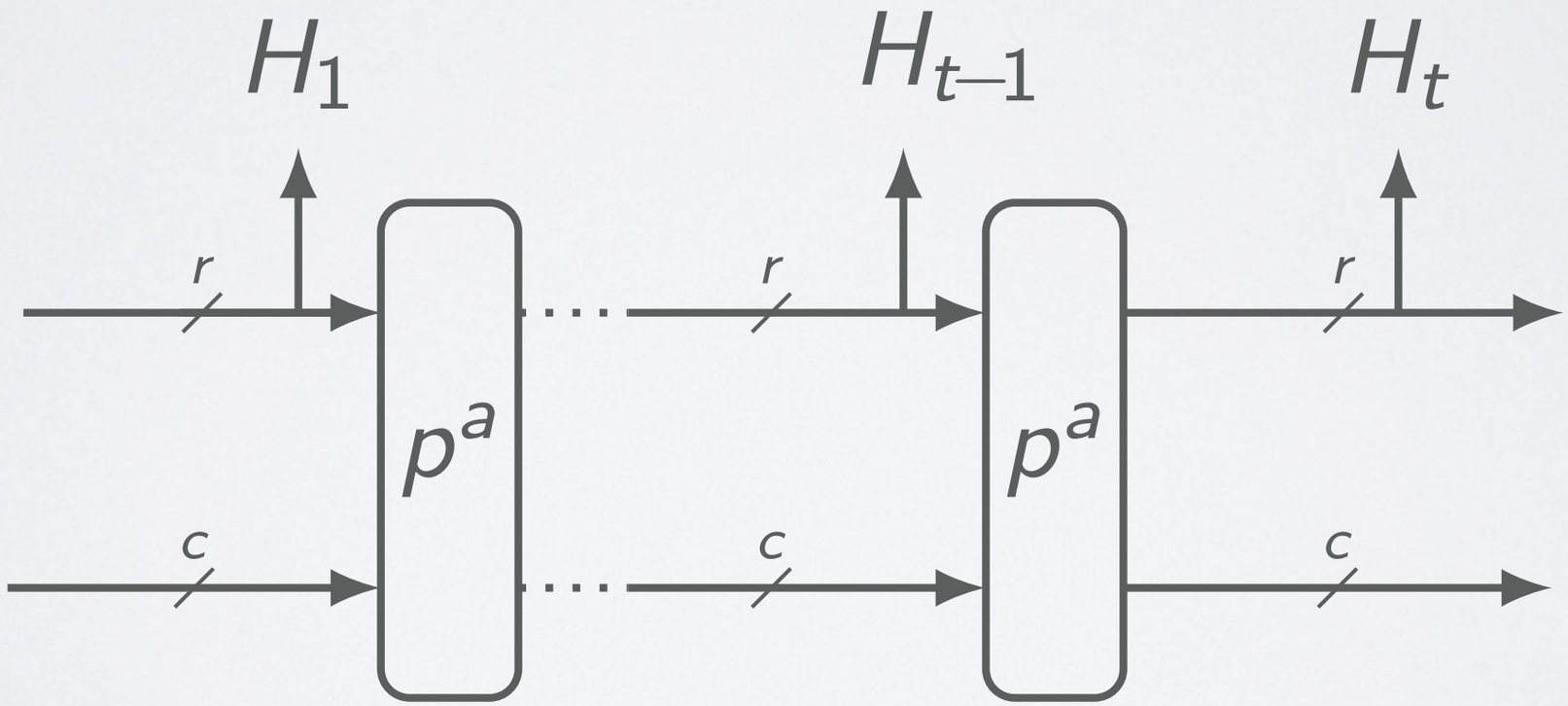
HASHING

- **Absorbing:** updates the 320-bit state with the data block M_i



HASHING

- **Squeezing:** extracts the final hash value



SECURITY ANALYSIS

	Rounds	Complexity
Ascon-Hash	2/12	2^{105}
Ascon-Xof (64 bits)	2/12	2^{15}
	6/12	$2^{63.3}$

- Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer. Preliminary Analysis of Ascon-Xof and Ascon-Hash. 2019
- Rui Zong and Xiaoyang Dong and Xiaoyun Wang. Collision Attacks on Round-Reduced Gimli-Hash, Ascon-Xof and Ascon-Hash. 2019

IMPLEMENTATION

- Software
  - Intel Xeon
  - ARM Cortex-A53
- Hardware
  - High-speed
  - Low-area

SOFTWARE

- Intel Xeon

	64	512	1024	4096
ASCON-128 (cycles/byte)	17.3	12.9	10.8	**10.5**
ASCON-128a (cycles/byte)	14.1	9.7	7.3	**6.9**

SOFTWARE

- ARM Cortex-A53

	64	512	1024	4096
ASCON-128 **(cycles/byte)**	18.3	14.4	11.3	**11.0**
ASCON-128a **(cycles/byte)**	15.1	11.2	7.6	**7.3**

HARDWARE

- Unprotected Implementations

	Variant 1	Variant 2	Variant 3
Area (kGE)	7.1	24.9	2.6
Throughput (MByte/s)	5 524	13 218	14

HARDWARE

- Threshold Implementations

	Variant 1	Variant 2	Variant 3
Area (kGE)	28.6	123.5	7.9
Throughput (MByte/s)	3 774	9 018	14

ASCON FEATURES

- Small hardware area
- Efficiency in software
- Natural side-channel protection
- Limited damage in misuse settings
- Low overhead for short messages
- …

SUMMARY

- Security
  - Well analysed/understood
  - Large security margin
- Efficiency
  - Efficient on constraint devices in HW and SW
  - Natural side-channel protection
  - Fast on modern CPUs

⇨ IoT

FURTHER INFORMATION

https://ascon.iaik.tugraz.at

ISAP

LIGHTWEIGHT AUTHENTICATED ENCRYPTION

ISAP TEAM

- Christoph Dobraunig
- Maria Eichlseder
- Stefan Mangard
- Florian Mendel
- Bart Mennink
- Thomas Unterluggauer
- Robert Primas







MOTIVATION

- **Problem:** side-channel attacks
- **Countermeasures:** hiding, masking, TI, …
- Reduce overhead of countermeasures
  - ASCON, KETJE/KEYAK,Gimli, Xoodyak, …
- Can we do more?

RELATED WORK

- C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer: ISAP - Towards Side-Channel Secure Authenticated Encryption FSE 2017

- G. Barwell, D. P. Martin, E. Oswald, and M. Stam: Authenticated Encryption in the Face of Protocol and Side Channel Leakage ASIACRYPT 2017

- F. Berti, O. Pereira, T. Peters, and F.-X. Standaert: On Leakage-Resilient Authenticated Encryption with Decryption Leakages FSE 2018

ISAP

- Robustness against DPA on algorithmic level for
  - Encryption
  - Decryption
- Solely based on the sponge construction
  - Limits the attack surface against SPA

SPA AND DPA

- **Simple Power Analysis (SPA)**
  - Observe device processing the same or a few inputs
  - Techniques directly interpreting measurements

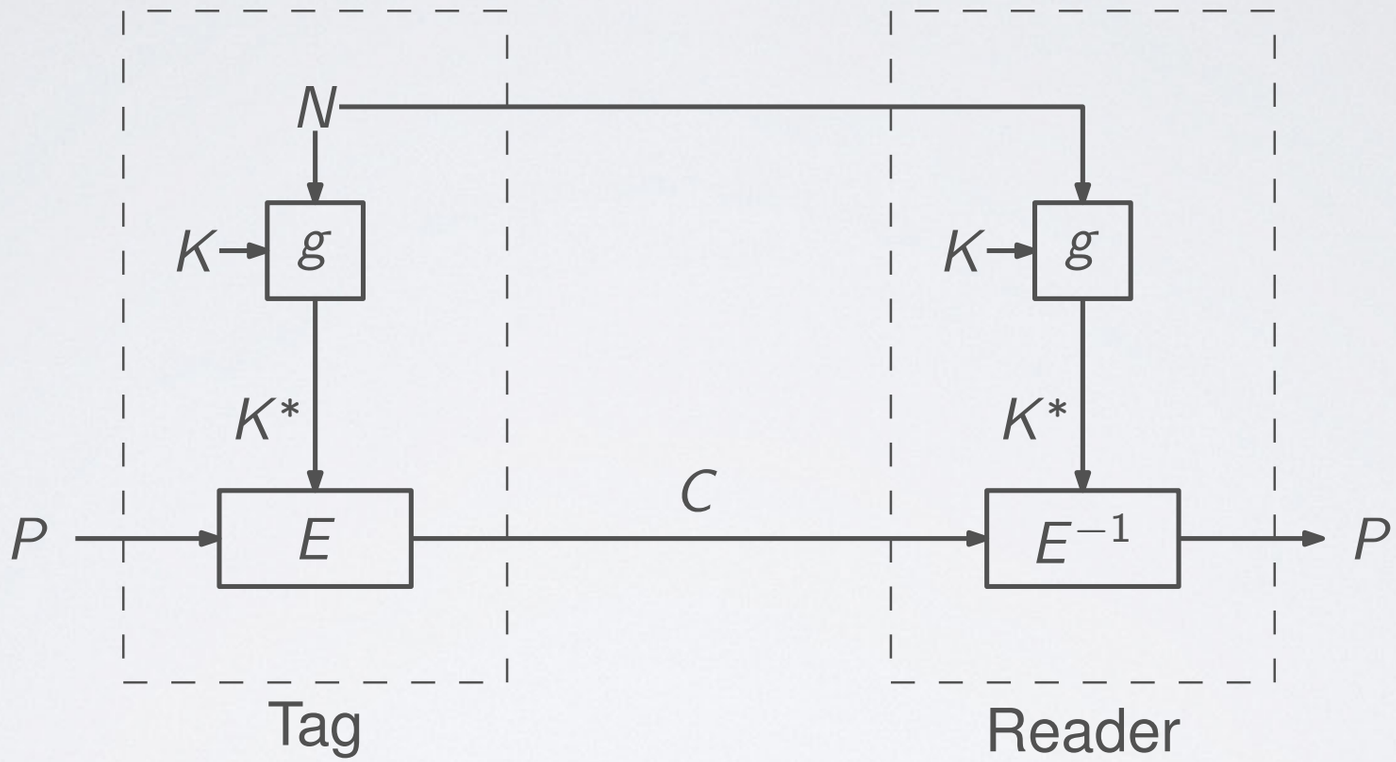
- **Differential Power Analysis (DPA)**
  - Observe device processing many different inputs
  - Allows for the use of statistical techniques

IS DPA A THREAT ?

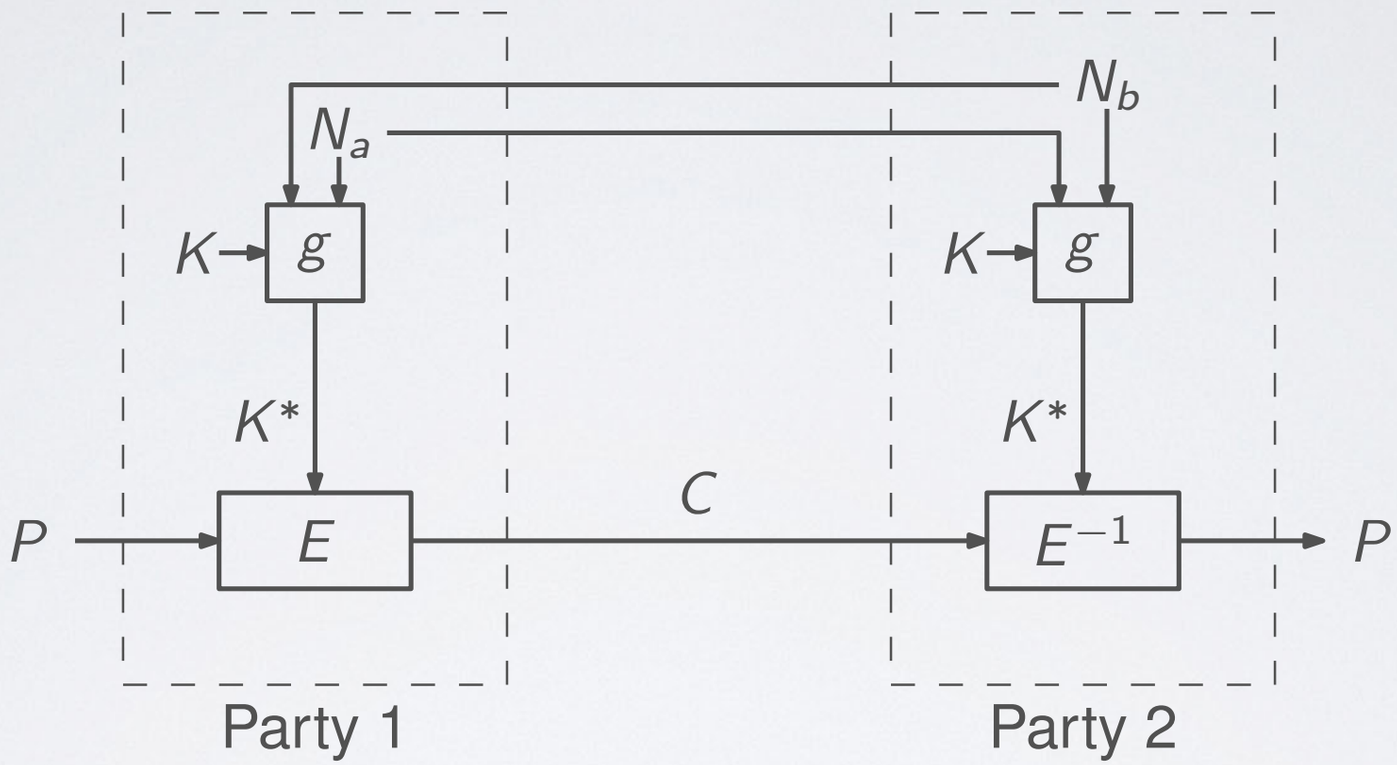
- A. Moradi and T. Schneider: Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series
  COSADE 2016

- E. Ronen, A. Shamir, A. Weingarten, and C. O'Flynn: IoT Goes Nuclear: Creating a ZigBee Chain Reaction
  S&P 2017

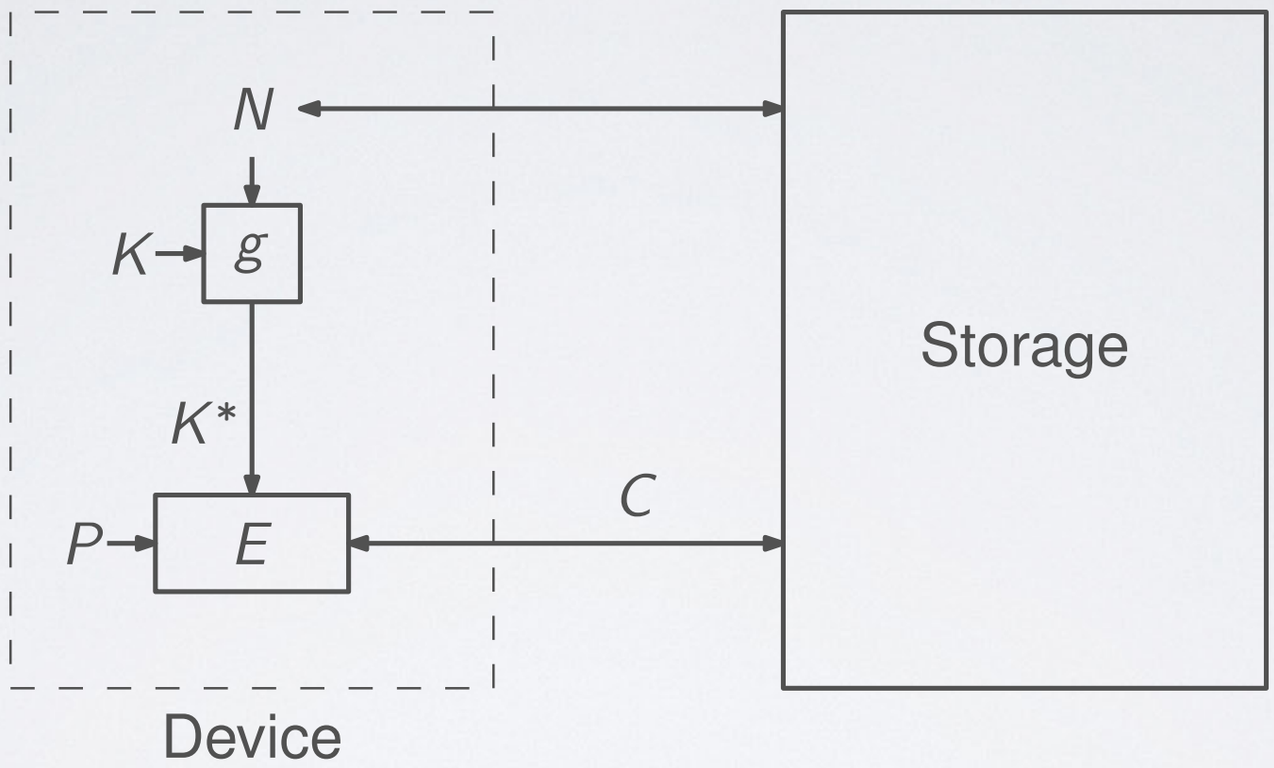
FRESH RE-KEYING



FRESH RE-KEYING



WHAT ABOUT STORAGE ?



- Encryption still fine
- Decryption might be critical

HOW TO PROTECT DECRYPTION ?

- **Rely on implementation countermeasures**
  - Costly
  - Makes re-keying for encryption kind of obsolete
- **Limit to one decryption**
  - Keep track of the nonce
  - Re-encrypt data
  - Time consuming
  - Damaging

MULTIPLE DECRYPTION

Retain principles of fresh re-keying allowing multiple decryption

DPA robustness in storage settings

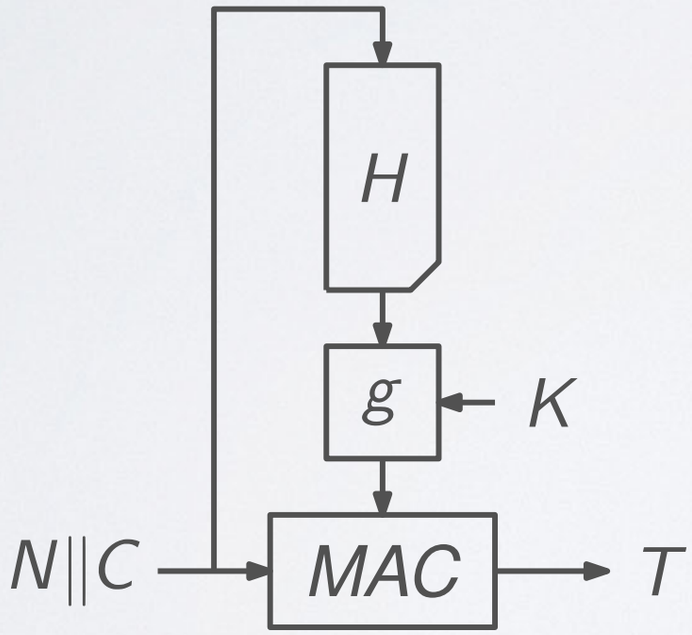
- A. Moradi and T. Schneider: Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series. COSADE 2016

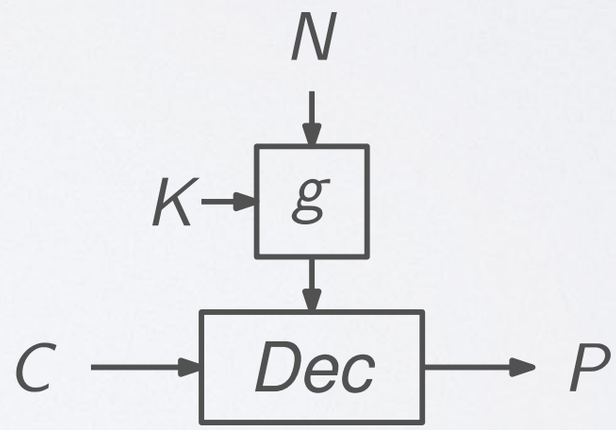
DPA robustness in unidirectional/broadcast settings

- E. Ronen, A. Shamir, A. Weingarten, and C. O'Flynn: IoT Goes Nuclear: Creating a ZigBee Chain Reaction. S&P 2017

PRINCIPLE OF DECRYPTION

- "Bind" the session key to the data that is decrypted

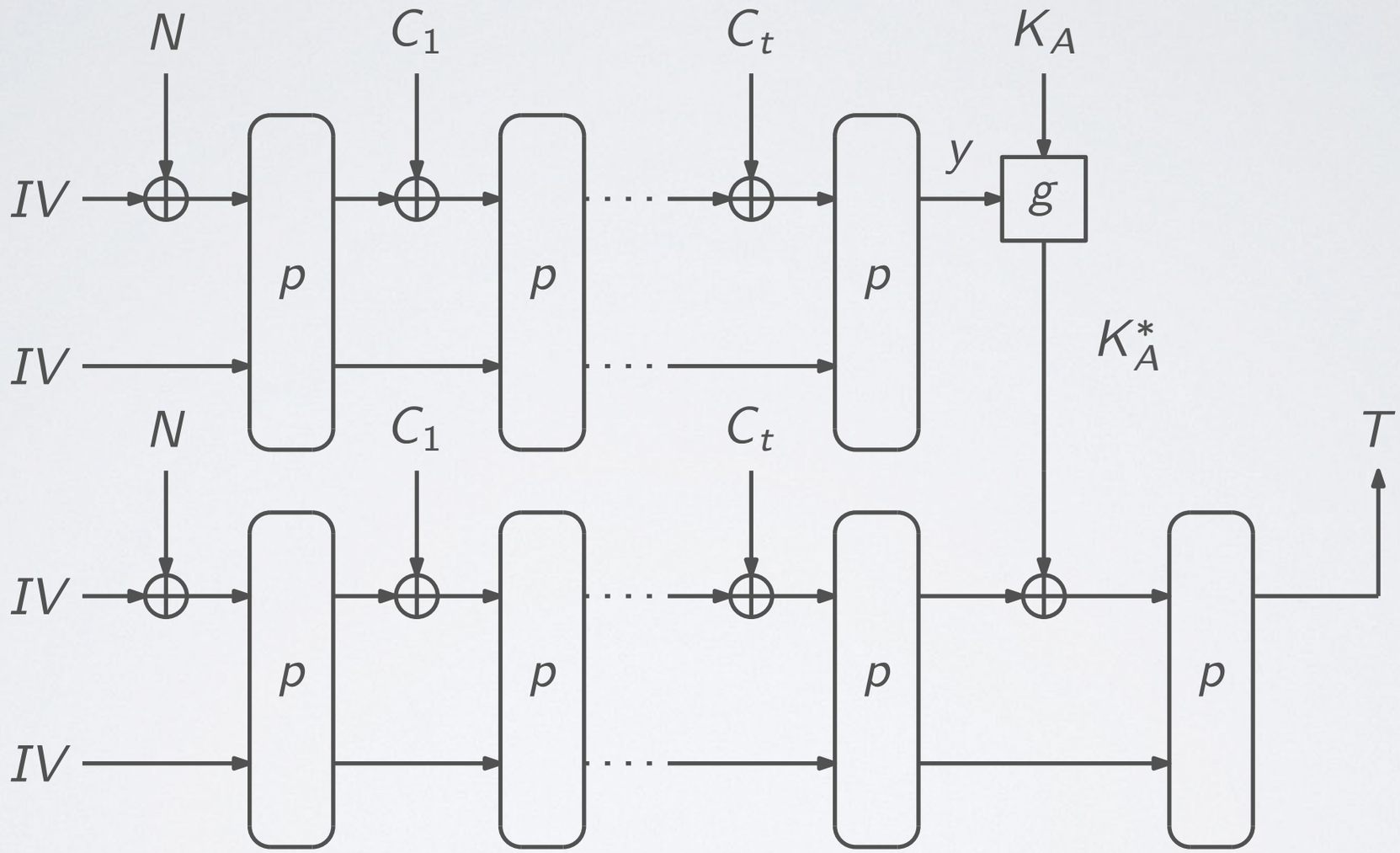




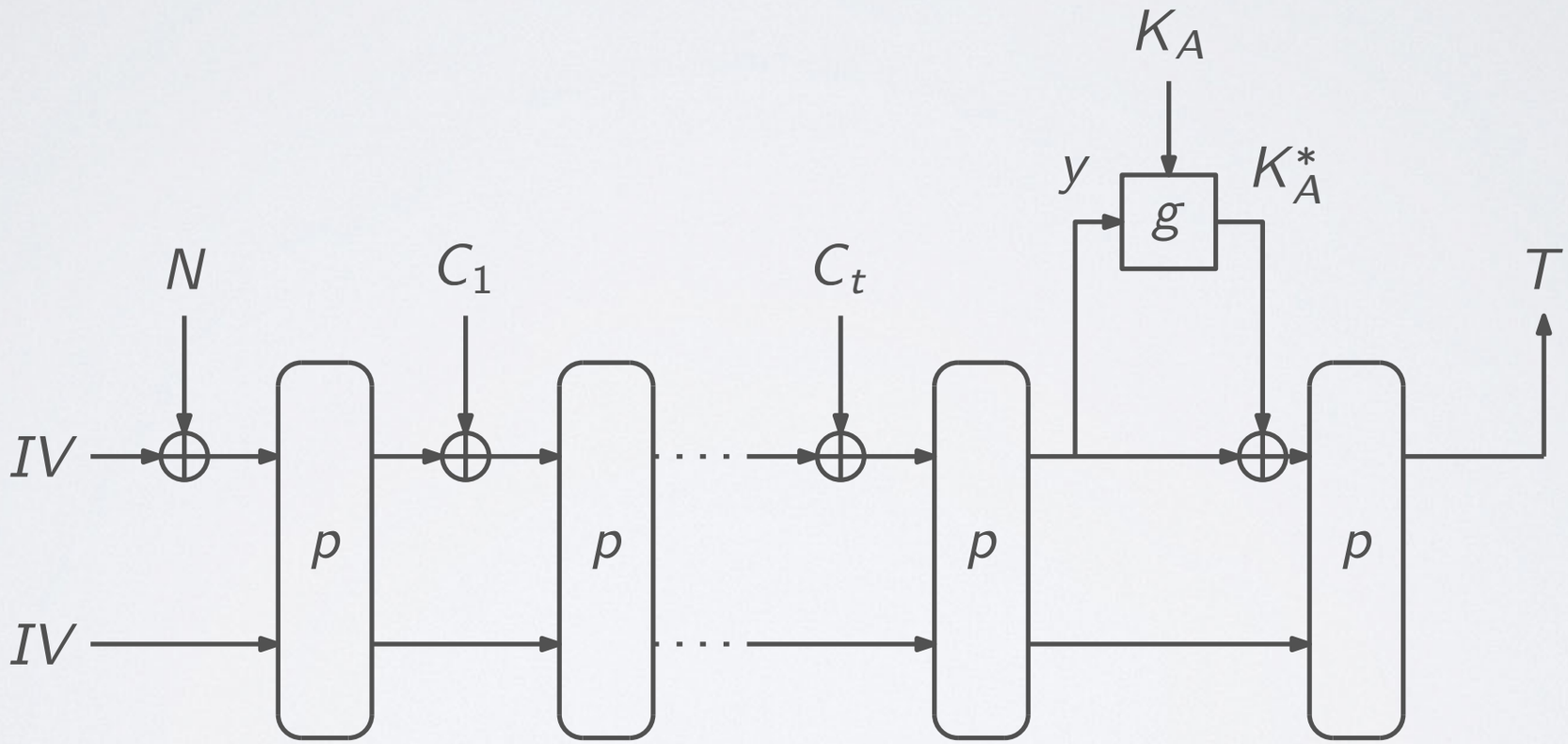
BENEFITS OF SPONGES

- Well-studied and analyzed
- Allows to implement a wide range of primitives
- No inverse building blocks (permutation) needed
- No key schedule, key is injected once
- Simple way to model side-channel-leakage

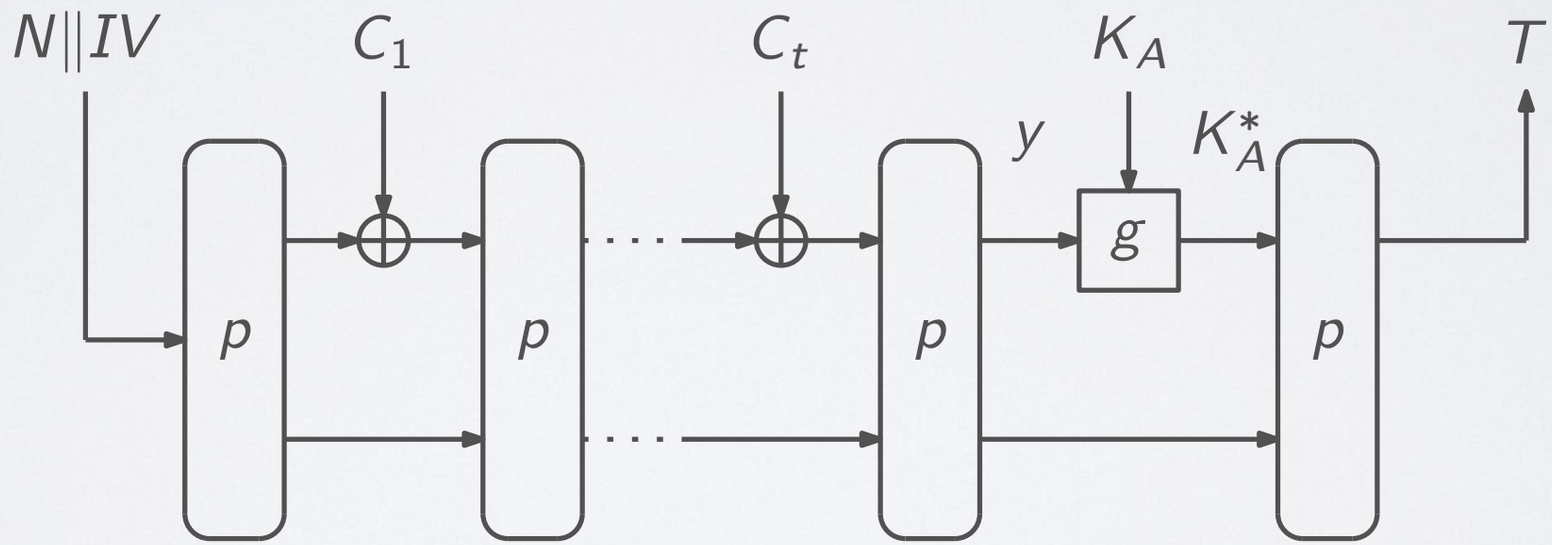
AUTHENTICATION / VERIFICATION



AUTHENTICATION / VERIFICATION



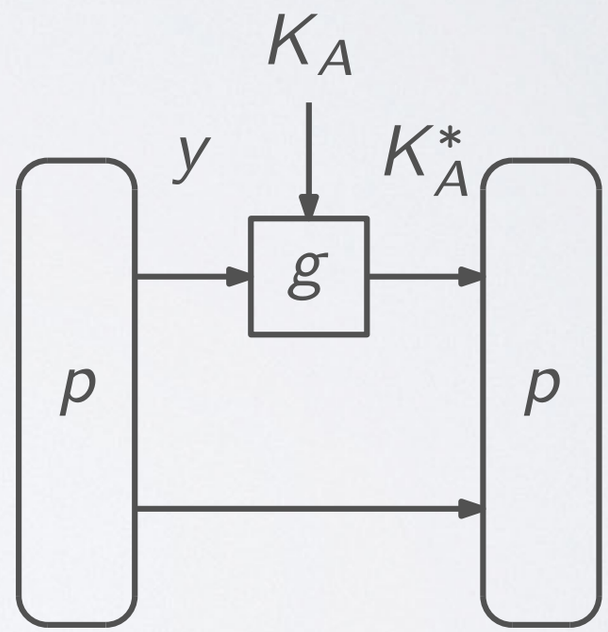
AUTHENTICATION / VERIFICATION



- Use suffix MAC instead of hash-then-MAC

ABSORBING THE KEY

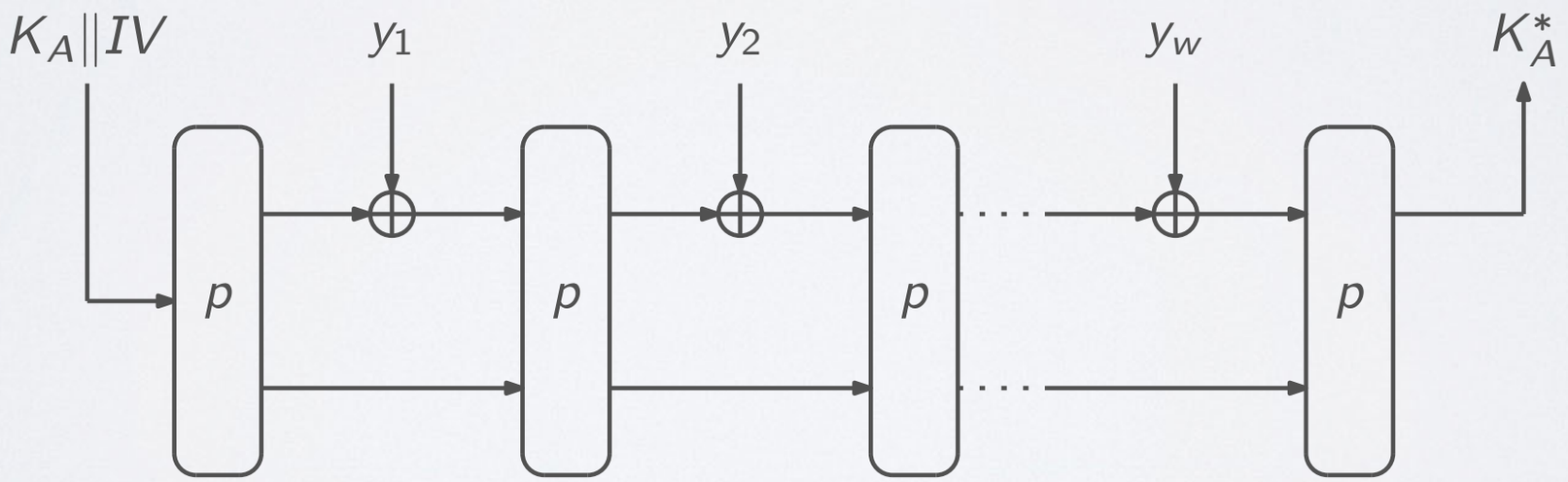
- Modular multiplication
- LPL and LWE
- Sponges



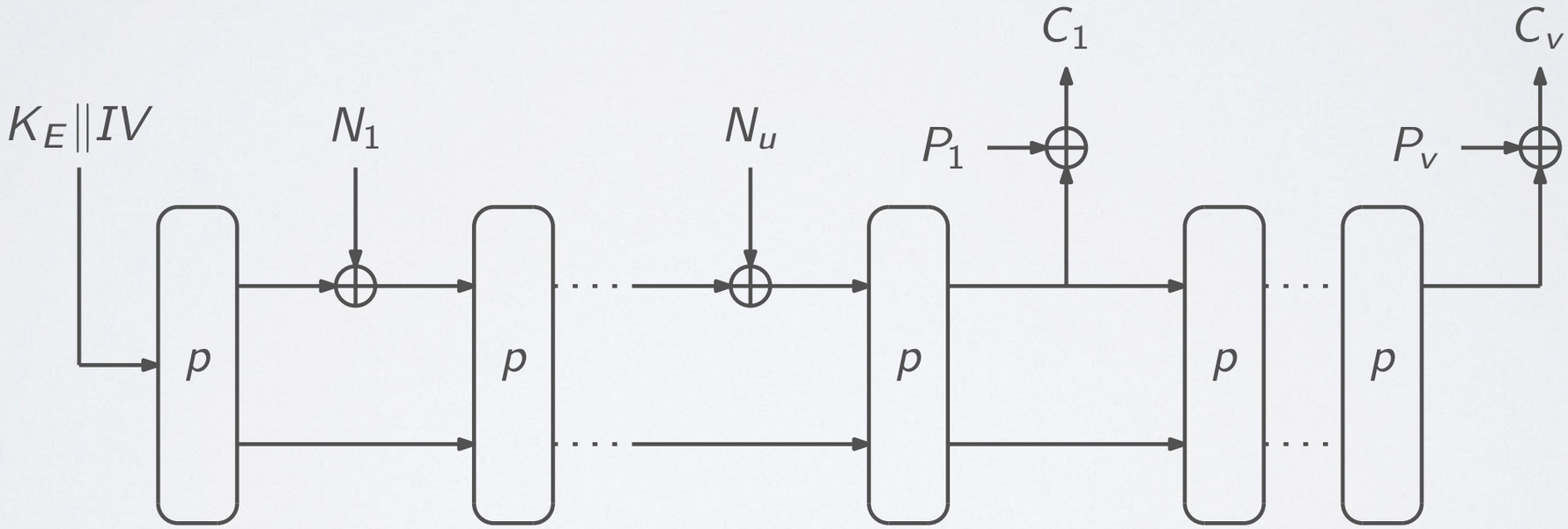
ABSORBING THE KEY

Idea: Reduce rate to a minimum

Related to the classical GGM construction



ENCRYPTION / DECRYPTION

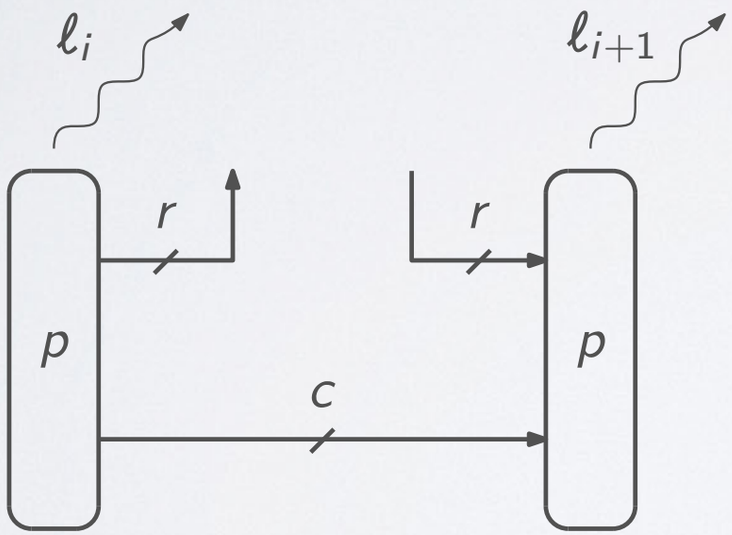


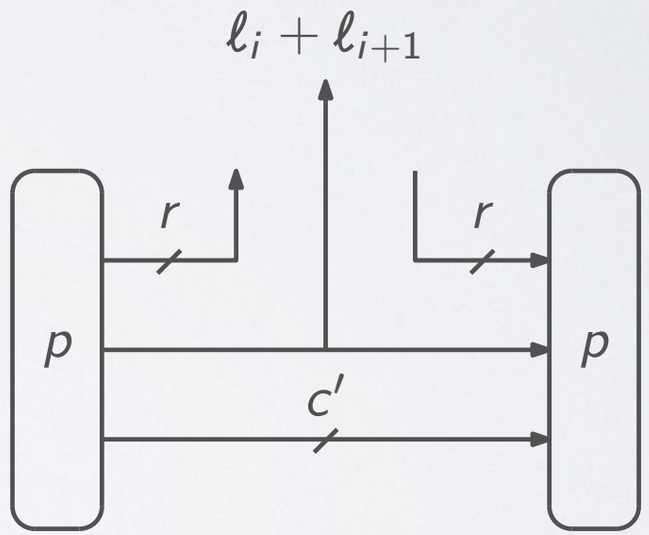
BENEFITS OF SPONGES

- Well-studied and analyzed
- Allows to implement a wide range of primitives
- No inverse building blocks (permutation) needed
- No key schedule, key is injected once
- **Simple way to model side-channel-leakage**

SIDE-CHANNEL LEAKAGE

- Modelling side-channel leakage in sponges





LEAKAGE RESILIENCE

- C. Dobraunig and B. Mennink: Leakage Resilience of the Duplex Construction. ASIACRYPT 2019
- J.-P. Degabriele, C. Janson and P. Struck: Sponges Resist Leakage - The Case of Authenticated Encryption. ASIACRYPT 2019
- C. Guo, O. Pereira, T. Peters and F.-X. Standaert: Towards Low-Energy Leakage-Resistant Authenticated Encryption from the Duplex Sponge Construction. FSE 2020
- C. Dobraunig and B. Mennink: Security of the Suffix Keyed Sponge. FSE 2020
- C. Dobraunig and B. Mennink: Leakage Resilience of the ISAP Mode - A Vulgarized Summary. NIST Lightweight Cryptography Workshop 2019

INSTANCES

- **Keccak-p[400]**
  - ISAP-K-128A
  - ISAP-K-128
- **Ascon**
  - ISAP-A-128A
  - ISAP-A-128

SUMMARY

- AE scheme following the NIST call
- Provides robustness against DPA on algorithmic level
- Enables several use-cases
  - Multiple decryption of stored data
  - Unidirectional/Broadcast communication

FURTHER INFORMATION

https://isap.iaik.tugraz.at