ASCON

AUTHENTICATED ENCRYPTION AND HASHING

Christoph Dobraunig, Maria Eichlseder,
Florian Mendel, Martin Schläffer

ASCON TEAM

- Christoph Dobraunig
- Maria Eichlseder
- Florian Mendel
- Martin Schläffer



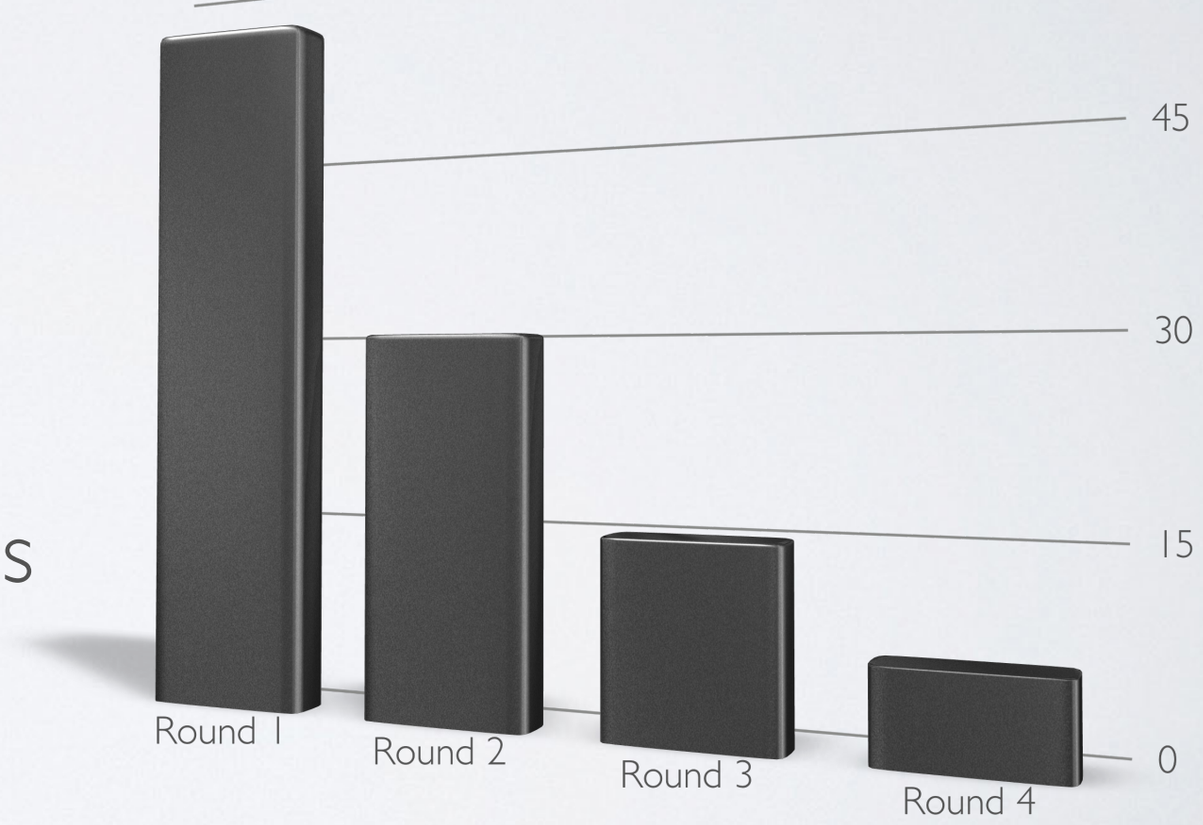

CAESAR

Goal: Select portfolio of authenticated ciphers

Timeline: 2014 - 2019, 4 rounds

Categories:

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



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 inspired

	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

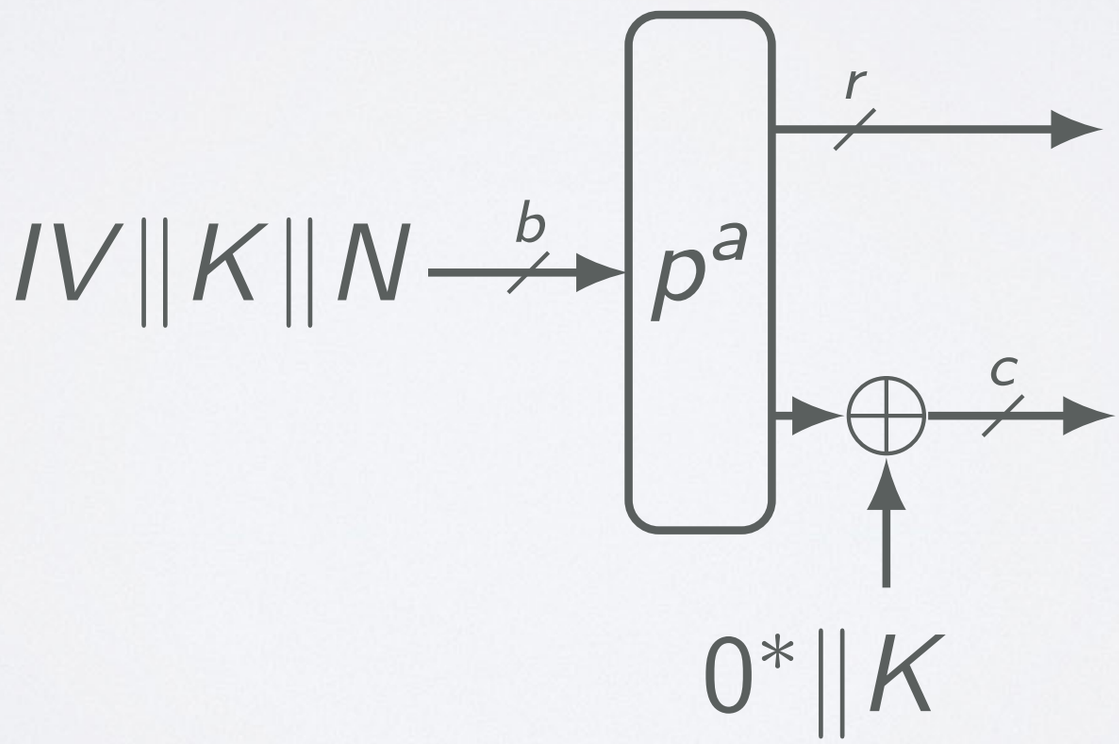
WORKING PRINCIPLE

The encryption process is split into four phases:

- Initialization
- Associated Data Processing
- Plaintext Processing
- Finalization

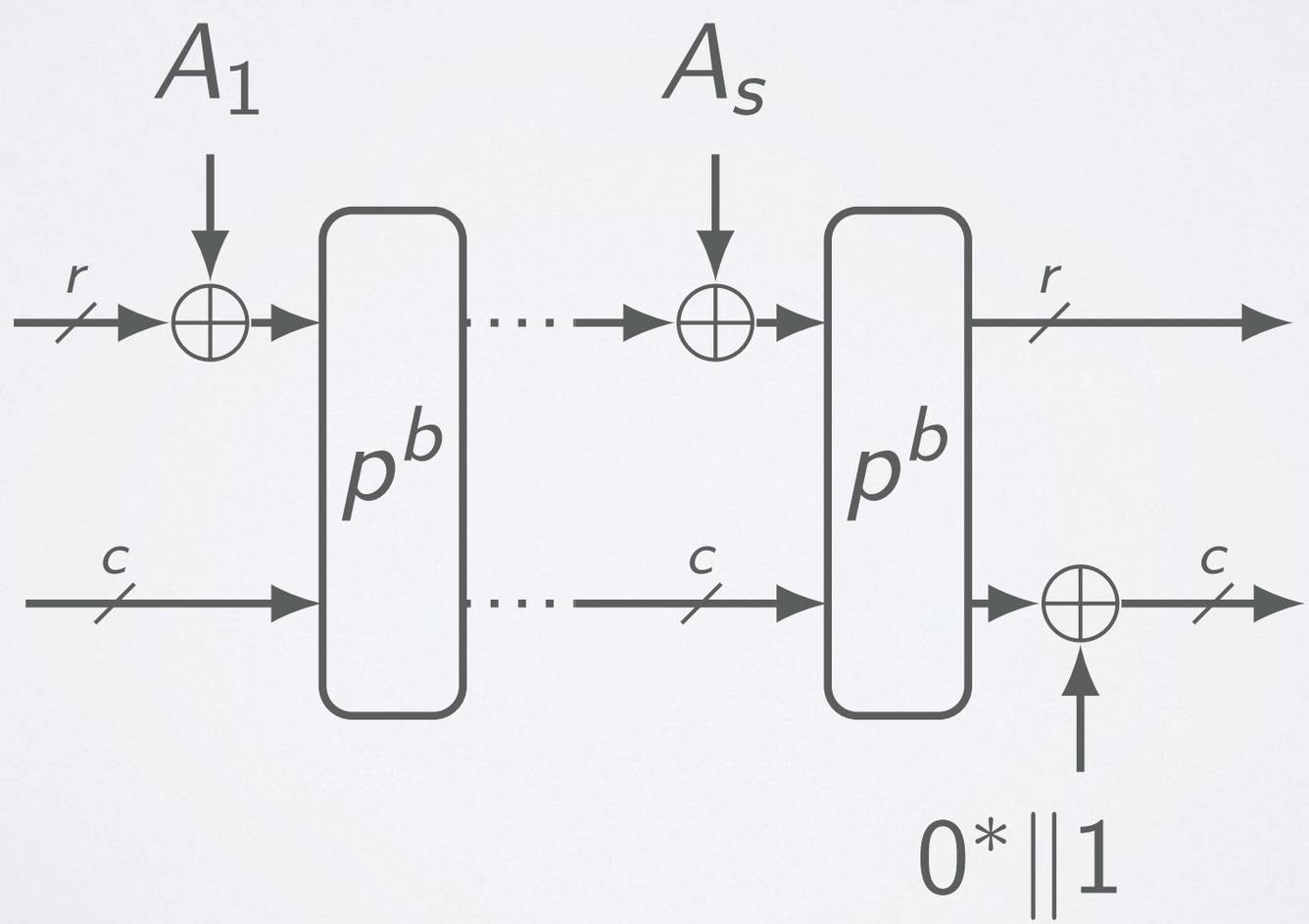
INITIALIZATION

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



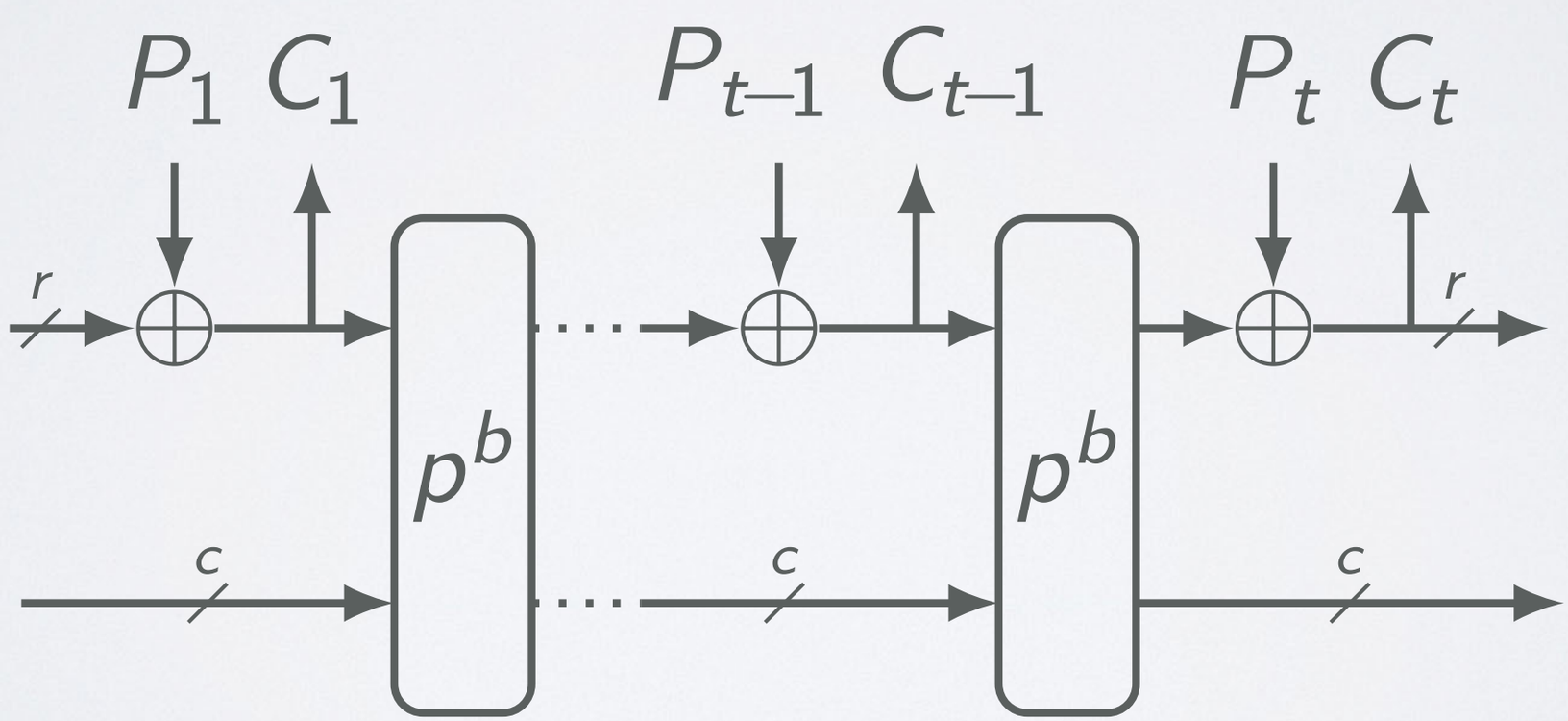
ASSOCIATED DATA

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



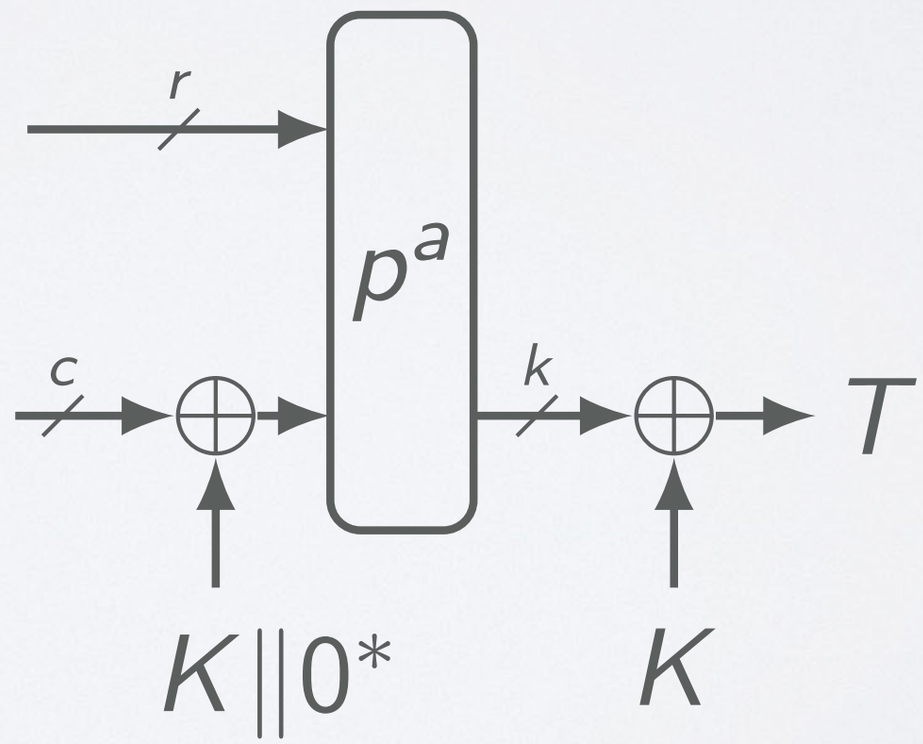
ENCRYPTION

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



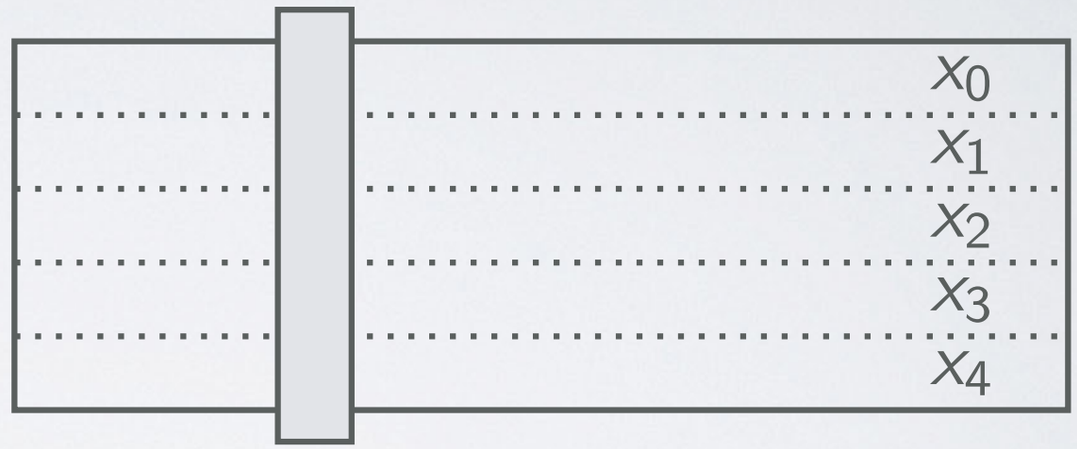
FINALIZATION

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

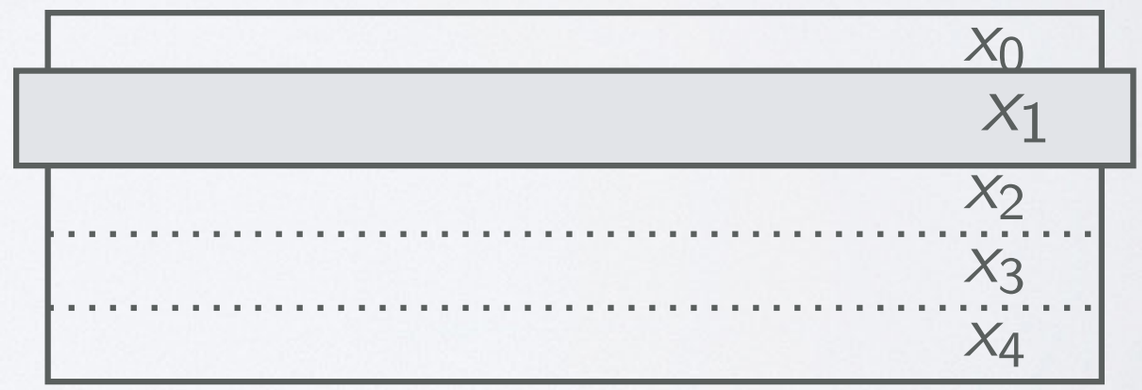


PERMUTATION

- SP-Network:
  - S-Layer:

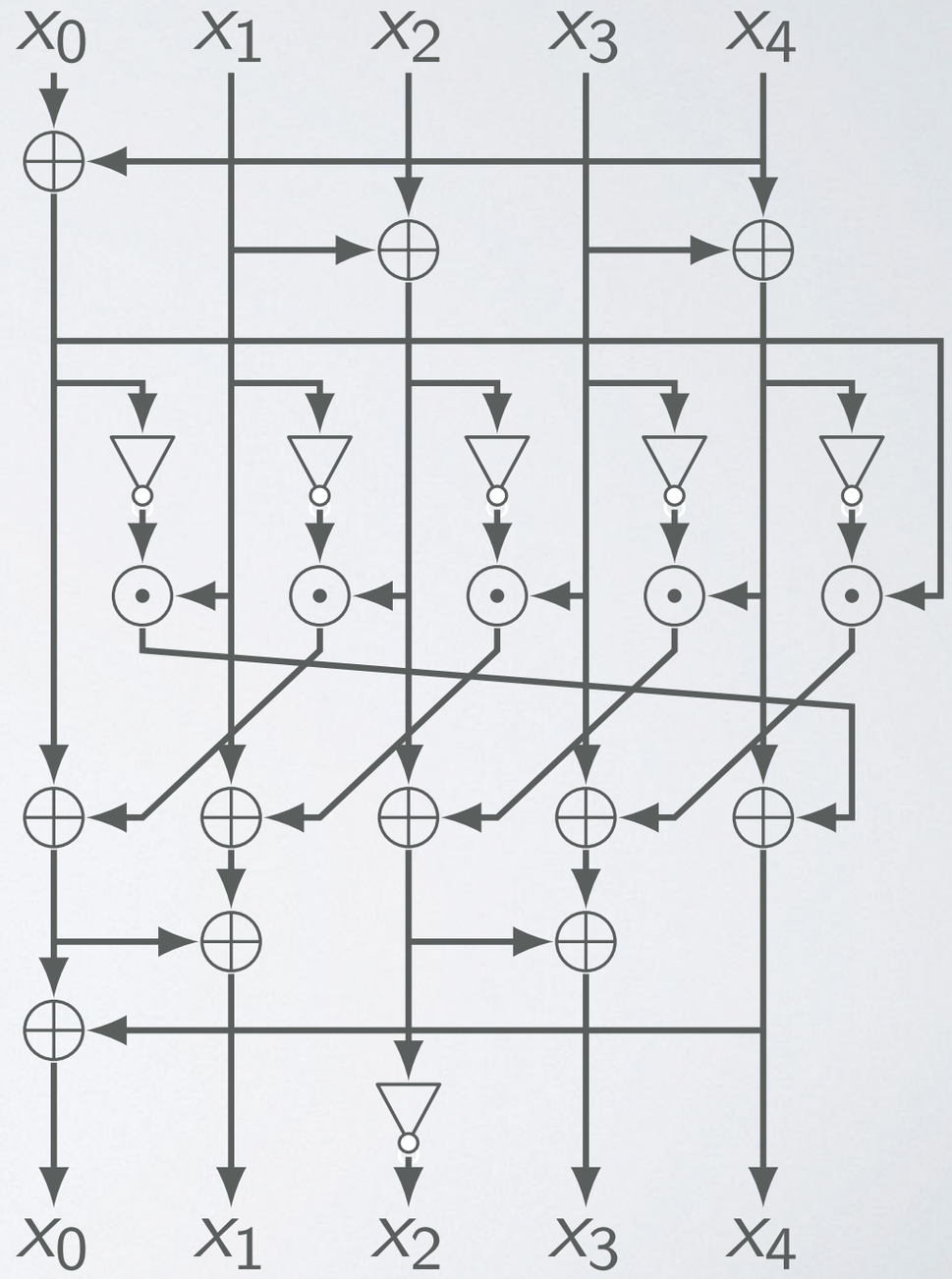


  - P-Layer:



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

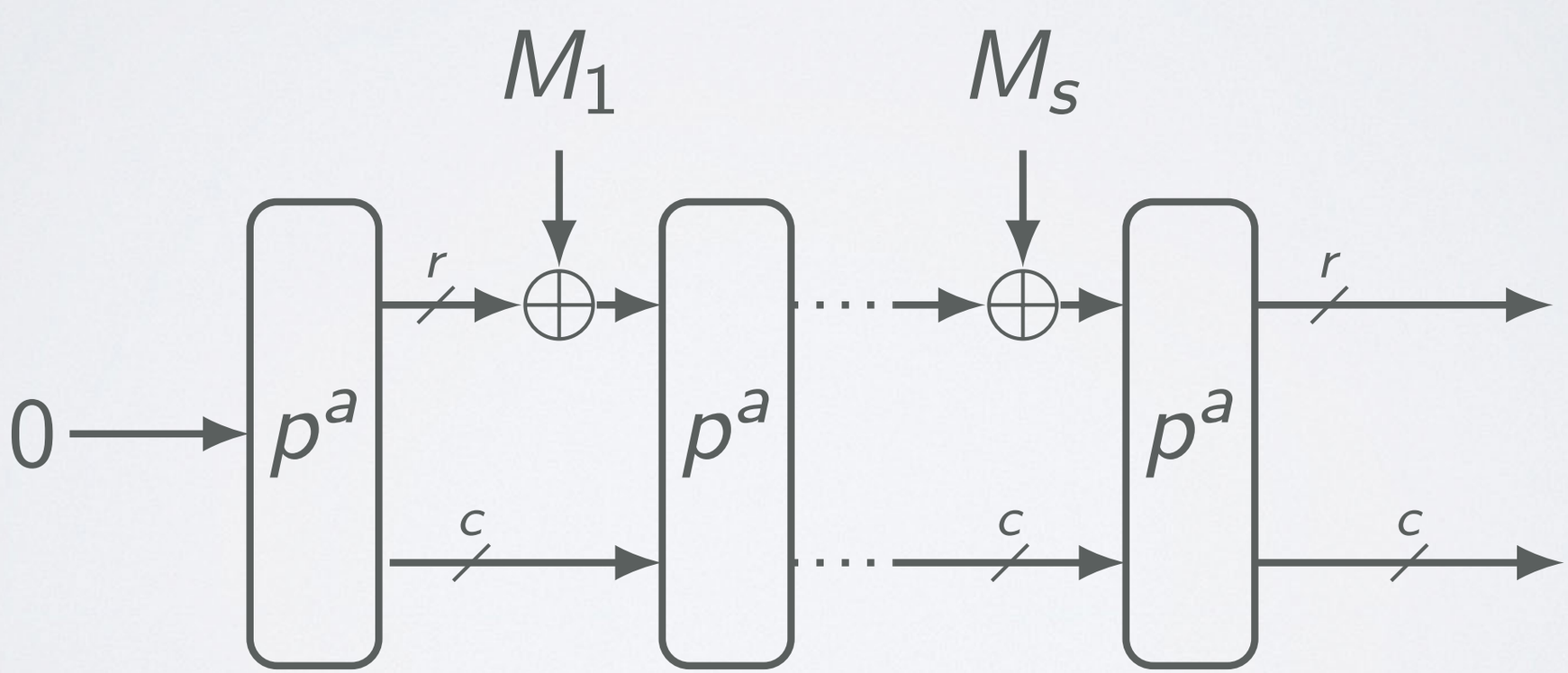
HASHING

- 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

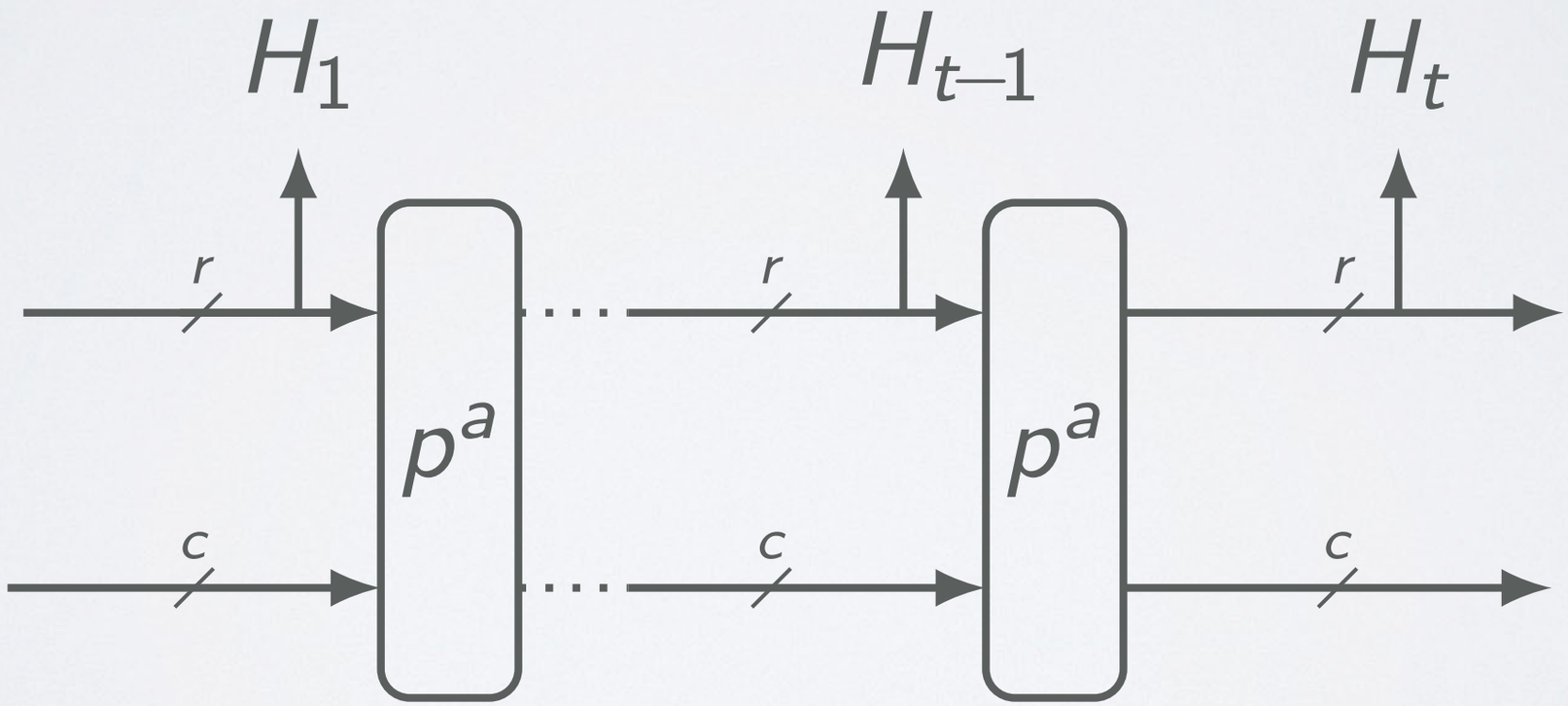
HASHING

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

HARDWARE

- Threshold Implementations

	Variant	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

TU Graz

Infineon

Radboud University

IN·DEI·NOMINE·FELICITER