ASCON

Submission to the CAESAR Competition

Christoph Dobraunig, Maria Eichlseder,
Florian Mendel, Martin Schläffer

This work was supported in part by the Austrian Government through the
research projects SePAG (FIT-IT 835919) and SeCoS (FFG/SFG 836628)

TU Graz

Our Team

- Christoph Dobraunig

- Maria Eichlseder

- Florian Mendel

- Martin Schläffer

ASCON

Main Design Goals

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

ASCON

General Overview

- Nonce-based AE scheme
- Sponge inspired

	ASCON-128	ASCON-96
Security	128 bits	96 bits
State size (b)	320 bits	320 bits
Capacity (c)	256 bits	192 bits
Rate (r)	64 bits	128 bits

ASCON

Working Principle

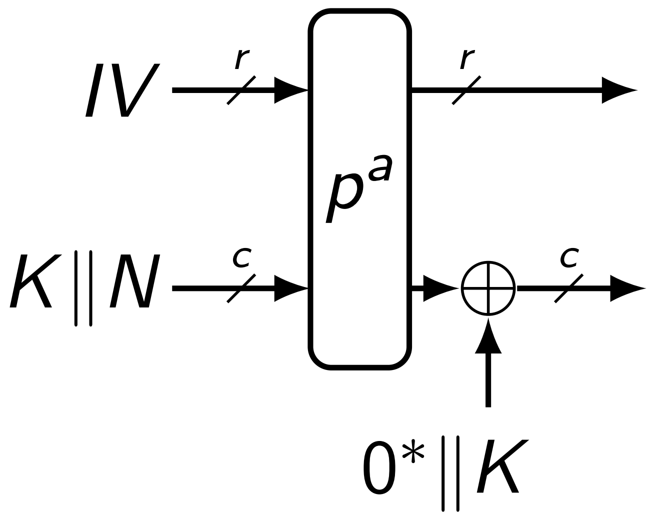
The encryption process is split into four phases:

- Initialization
- Associated Data Processing
- Plaintext Processing
- Finalization

ASCON

Initialization

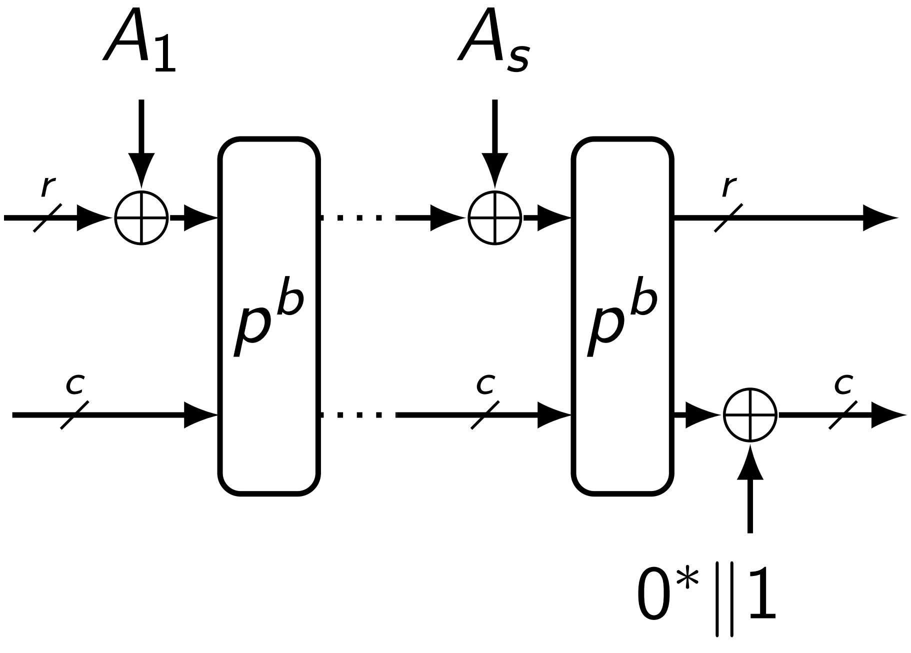
- **Initialization:** updates the 320-bit state with the key K and nonce N



ASCON

Associated Data

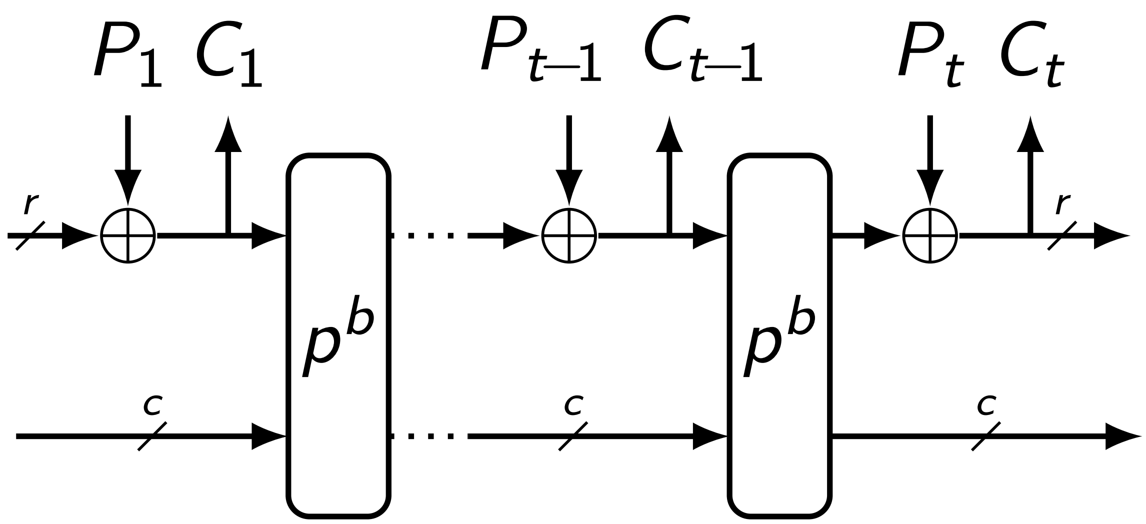
- **Associated Data Processing**: updating the 320-bit state with associated data blocks A_i



ASCON

Encryption

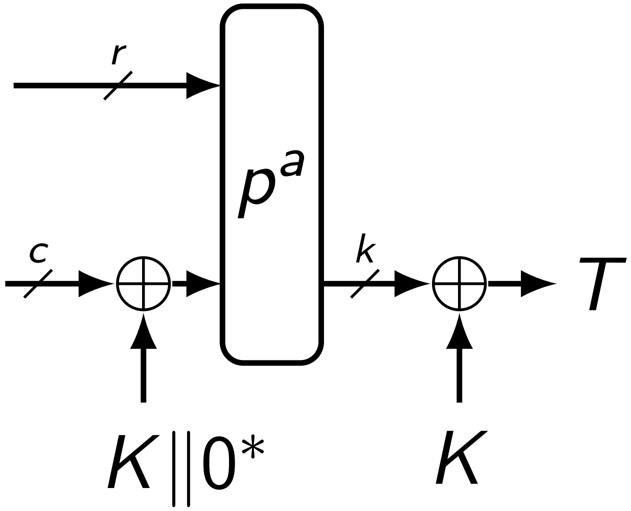
- **Plaintext Processing**: inject plaintext blocks P_i in the state and extract ciphertext blocks C_i



ASCON

Finalization

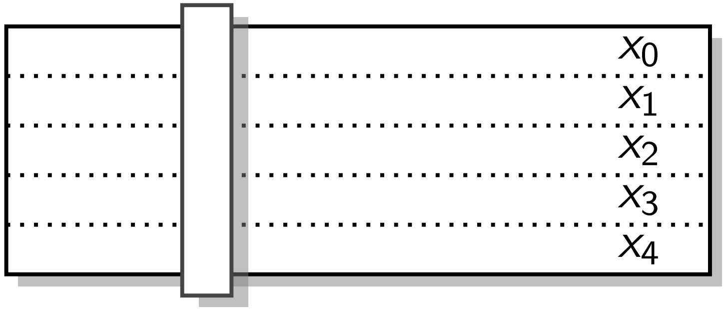
- **Finalization:** inject the key K and extracts a tag T for authentication



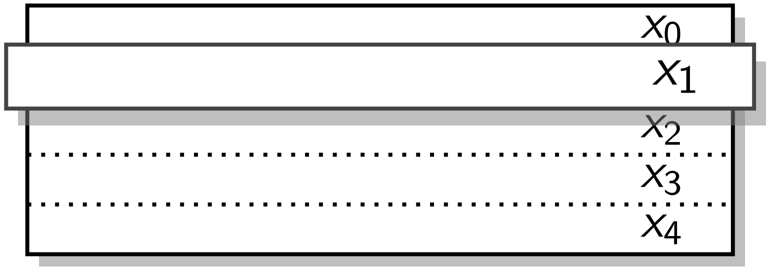
ASCON

Permutation

- SP-Network:
  - S-Layer:



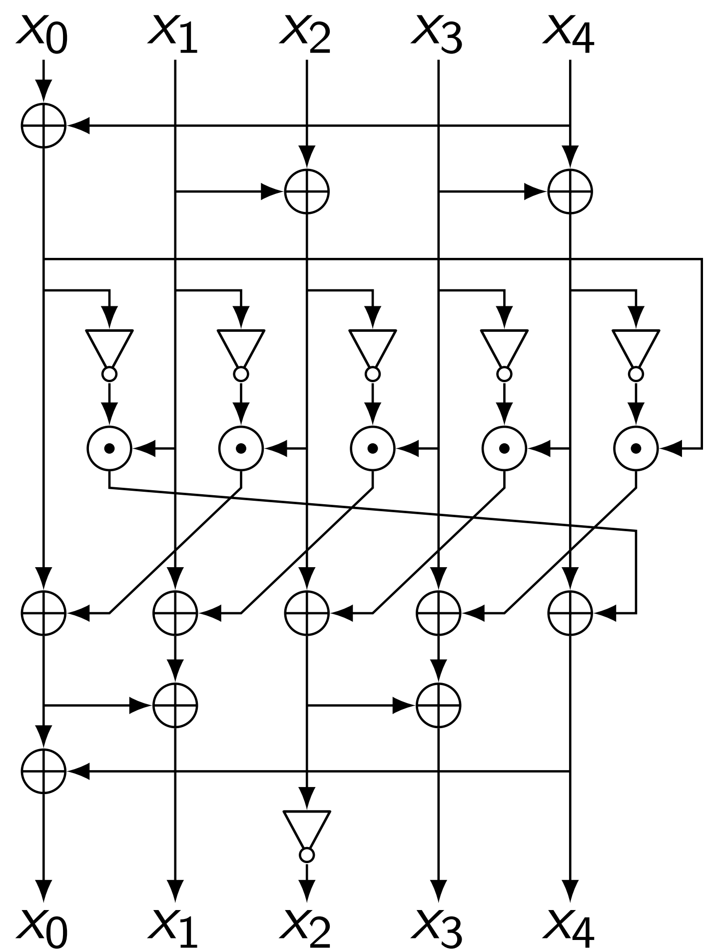
  - P-Layer:



ASCON

Permutation: S-Layer

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



ASCON

Permutation: P-Layer

- Branch Number 4

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

ASCON

Security Analysis

- Differential Cryptanalysis
  - 5 rounds: > 64 active Sboxes
- Impossible Differential
  - up to 5 rounds
- Linear Cryptanalysis
  - 5 rounds: > 64 active Sboxes

ASCON

Security Analysis

- Differential Cryptanalysis

Rounds	Active Sboxes	Probability
1	1	2^{-2}
2	4	2^{-8}
3	15	2^{-30}
4	44	2^{-88}
5	74	2^{-148}

ASCON

Security Analysis

- Linear Cryptanalysis

Rounds	Active Sboxes	Correlation
1	1	2^{-2}
2	4	2^{-8}
3	13	2^{-26}
4	43	2^{-86}
5	70	2^{-140}

ASCON

Implementation/Performance

- Software
  - Intel Core2 Duo
  - ARM Cortex-A8
- Hardware
  - High-speed
  - Low-area

ASCON

Software Implementation

- Intel Core2 Duo

	64	512	1024	4096
ASCON-128 **(cycles/byte)**	22.0	15.9	15.6	**15.2**
ASCON-96 **(cycles/byte)**	17.7	11.0	10.5	**10.3**

ASCON

Hardware Implementation

- ASCON-128

	Variant 1	Variant 2
Area (kGE)	8.9	4
Throughput (MByte/s)	400	1

H. Gross, E. Wenger

Threshold implementation coming soon!

ASCON

Choice of Parameters

- Now: (c,r) = (256, 64)
  - Conservative choice
- Proposed: (c,r) = (192,128) [BDPV12]
  - Significant speedup (factor 2)
  - Limit on data complexity 2^{64}
- Proposed: (c,r) = (128,192) [JLM14]
  - Significant speedup (factor 3)
  - More analysis needed

ASCON

General Information

Home Specification Implementation Analysis Resources Contact

ASCON

Interesting Links

ASCON Resources

- Specification [v1.0]
- Submission document [v1.0]
- GitHub repositories with implementations [git collection]
  - C (reference / optimized) [git] [zip]
  - Python [git] [py]
  - Java [git] [zip]
  - Hardware [git] [zip]

http://ascon.iaik.tugraz.at

Thank you!

http://ascon.iaik.tugraz.at