# ASCON

## Submission to the CAESAR Competition

Christoph Dobraunig, Maria Eichlseder,
Florian Mendel, Martin Schläffer

# Our Team

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

# ASCON

## Main Design Goals

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

# ASCON

## General Overview

- Nonce-based AE scheme
- Sponge inspired

| | ASCON-128 | ASCON-961a |
|---|---|---|
| **Security** | 128 bits | 96 bits |
| **Rate (r)** | 64 bits | 128 bits |
| **Capacity (c)** | 256 bits | 192 bits |
| **State size (b)** | 320 bits | 320 bits |

# ASCON

## General Overview

- Nonce-based AE scheme
- Sponge inspired

| | ASCON-128 | ASCON-961a |
|---|---|---|
| **Security** | 128 bits | 128 bits |
| **Rate (r)** | 64 bits | 128 bits |
| **Capacity (c)** | 256 bits | 192 bits |
| **State size (b)** | 320 bits | 320 bits |

# ASCON

## General Overview

- Nonce-based AE scheme
- Sponge inspired

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

# ASCON

## Working Principle

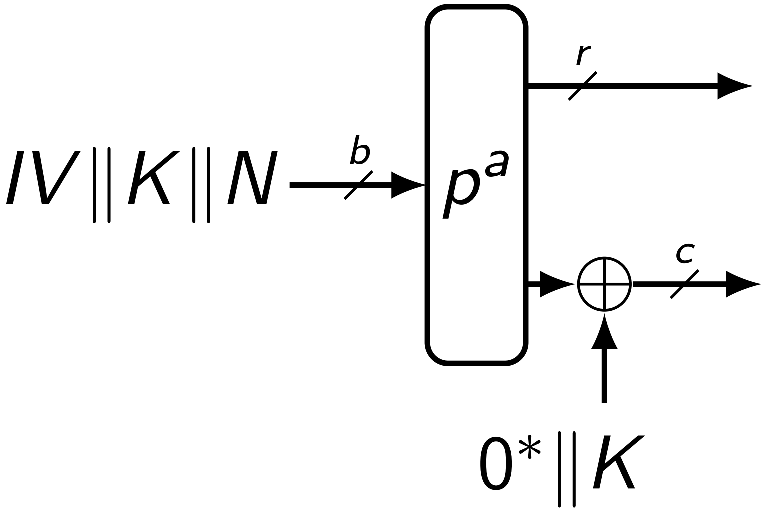
The encryption process is split into four phases:

- Initialization
- Associated Data Processing
- Plaintext Processing
- Finalization

# ASCON

## Initialization

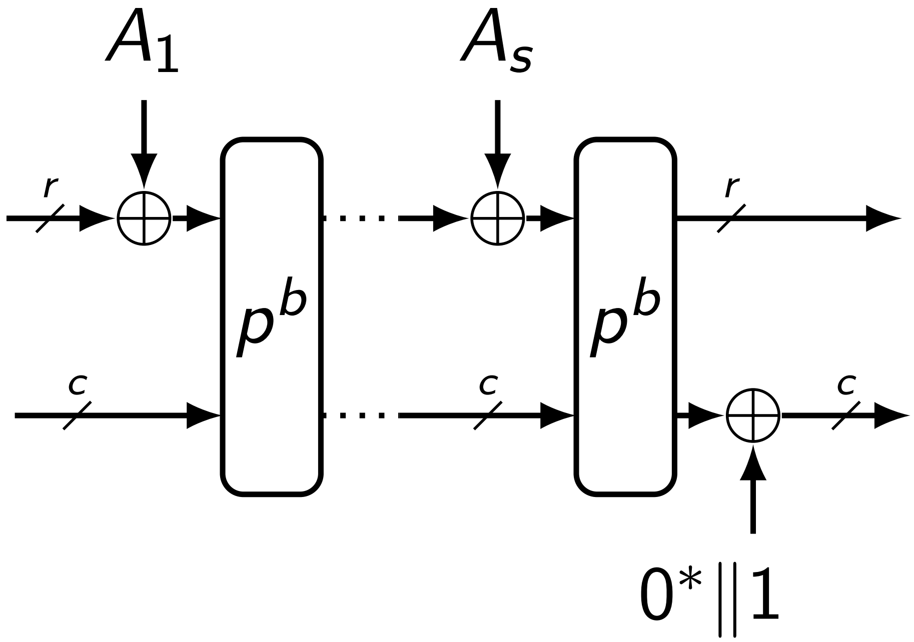
- **Initialization:** updates the 320-bit state with the key K and nonce N



# ASCON

## Associated Data

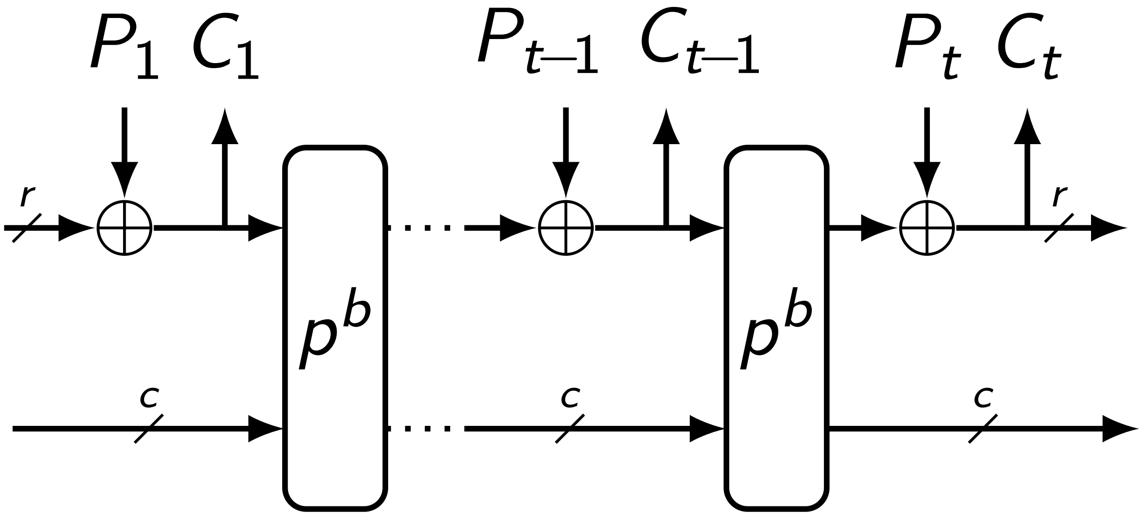
- **Associated Data Processing**: updating the 320-bit state with associated data blocks $A_i$



# ASCON

## Encryption

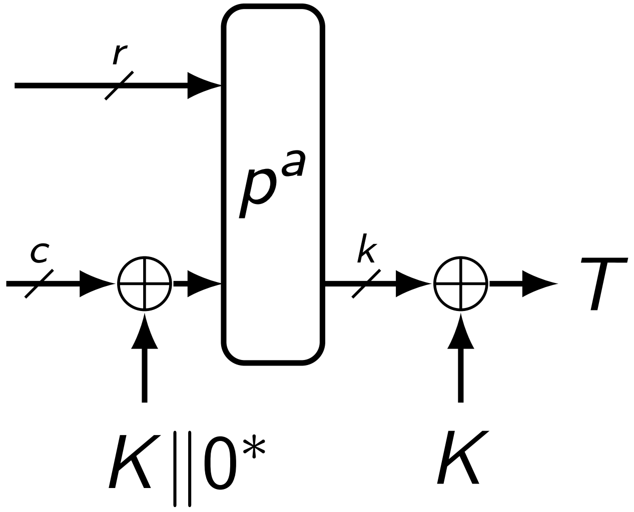
- **Plaintext Processing**: inject plaintext blocks $P_i$ in the state and extract ciphertext blocks $C_i$



# ASCON

## Finalization

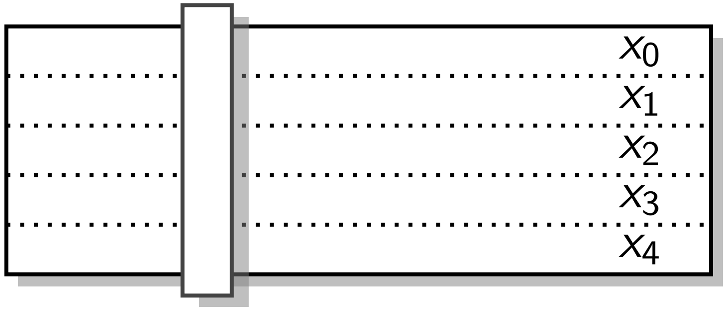
- **Finalization:** inject the key K and extracts a tag T for authentication



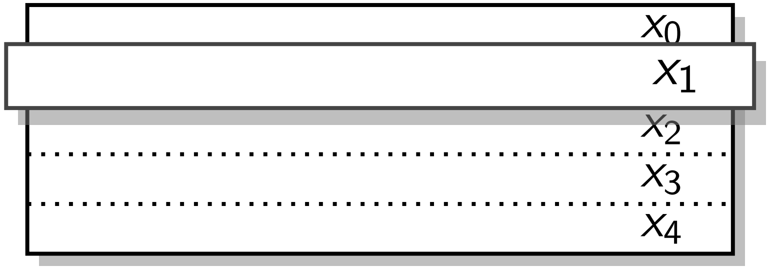
# ASCON

## Permutation

- SP-Network:
  - S-Layer:



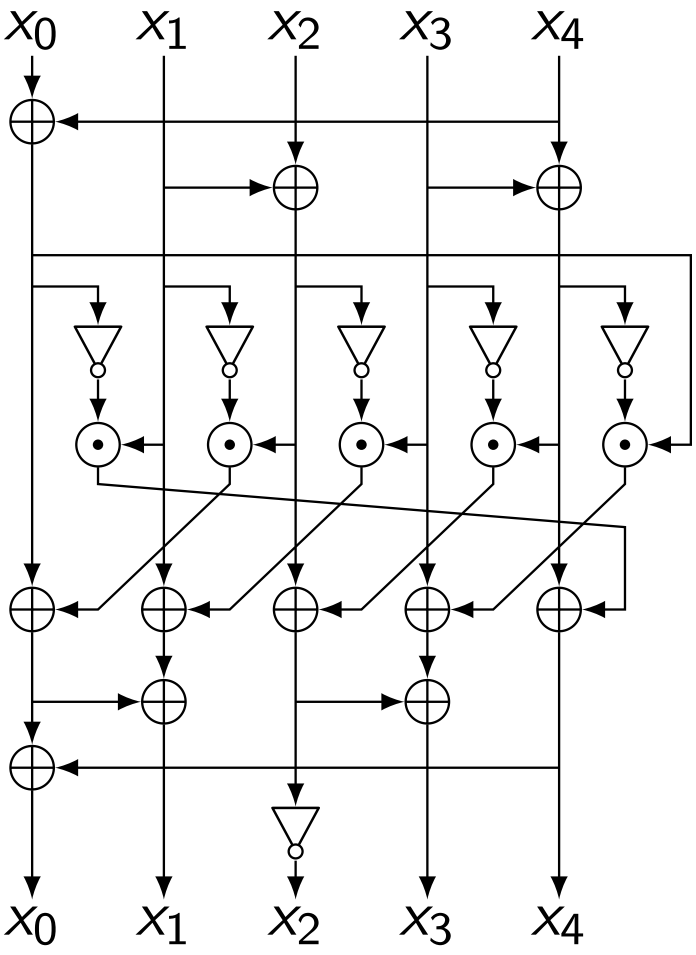
  - P-Layer:



# 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

$$
\begin{aligned}
\Sigma_0(x_0) &= x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)\\
\Sigma_1(x_1) &= x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)\\
\Sigma_2(x_2) &= x_2 \oplus (x_2 \ggg \phantom{0}1) \oplus (x_2 \ggg \phantom{0}6)\\
\Sigma_3(x_3) &= x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)\\
\Sigma_4(x_4) &= x_4 \oplus (x_4 \ggg \phantom{0}7) \oplus (x_4 \ggg 41)
\end{aligned}
$$

# ASCON

## Security Analysis

- Differential and Linear Cryptanalysis

| Rounds | Differential | Linear |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 4 | 4 |
| 3 | 15 | 13 |
| 4 | 44 | 43 |
| ≥ 5 | > 64 | > 64 |

ASIACRYPT 2015

# ASCON

## Security Analysis

- Differential and Linear Cryptanalysis

| Rounds | Differential | Linear |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 4 | 4 |
| 3 | 15 | 13 |
| 4 | 44 | 43 |
| ≥ 5 | > 64 | > 64 |

ASIACRYPT 2015

# ASCON

## Security Analysis

- Analysis of round-reduced versions

| Method | Rounds | Complexity |
|---|---|---|
| **cube-like** | 5/12 | $2^{35}$ |
| | 6/12 | $2^{66}$ |
| **differential-linear** | 4/12 | $2^{18}$ |
| | 5/12 | $2^{36}$ |

CT-RSA 2015

# 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**<br>**(cycles/byte)** | 22.0 | 15.9 | 15.6 | **15.2** |
| **ASCON-128a**<br>**(cycles/byte)** | 17.7 | 11.0 | 10.5 | **10.3** |

Dobraunig, Schläffer

# ASCON

## Software Implementation

- Intel Haswell (four message per core)

| | 64 | 512 | 1024 | 4096 |
|---|---|---|---|---|
| **ASCON-128**<br>**(cycles/byte)** | 10.5 | 7.3 | 7.1 | **6.9** |
| **ASCON-128a**<br>**(cycles/byte)** | 8.5 | 5.3 | 5.0 | **4.8** |

Dobraunig, Senfter

# ASCON

## Hardware Implementation

- Unprotected Implementations

| | Variant 1 | Variant 2 | Variant 3 |
|---|---|---|---|
| **Area**<br>**(kGE)** | 7.1 | 24.9 | **2.6** |
| **Throughput**<br>**(Mbps)** | 5 524 | **13 218** | 14 |

Gross, Wenger, Dobraunig, Ehrenhöfer

# ASCON

## Hardware Implementation

- Threshold Implementations

| | Variant 1 | Variant 2 | Variant 3 |
|---|---|---|---|
| **Area**<br>**(kGE)** | 28.6 | 123.5 | **7.9** |
| **Throughput**<br>**(Mbps)** | 3 774 | **9 018** | 14 |

Gross, Wenger, Dobraunig, Ehrenhöfer

# Thank you!

http://ascon.iaik.tugraz.at

# References

- Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer.
  **Cryptanalysis of Ascon.**
  CT-RSA 2015.
- Christoph Dobraunig, Maria Eichlseder, Florian Mendel.
  **Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates.**
  ASIACRYPT 2015
- Hannes Groß, Erich Wenger, Christoph Dobraunig, Christoph Ehrenhöfer.
  **Suit up! Made-to-Measure Hardware Implementations of Ascon.**
  DSD 2015
- Philipp Jovanovic, Atul Luykx, Bart Mennink.
  **Beyond 2^(c/2) Security in Sponge-Based Authenticated Encryption Modes.**
  ASIACRYPT 2014.
- Elena Andreeva, Joan Daemen, Bart Mennink, Gilles Van Assche.
  **Security of Keyed Sponge Constructions Using a Modular Proof Approach.**
  FSE 2015
- Yosuke Todo.
  **Structural Evaluation by Generalized Integral Property.**
  EUROCRYPT 2015.