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

<table>
<thead>
<tr>
<th></th>
<th>ASCON-128</th>
<th>ASCON-128a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>State size</td>
<td>320 bits</td>
<td>320 bits</td>
</tr>
<tr>
<td>Capacity</td>
<td>256 bits</td>
<td>192 bits</td>
</tr>
<tr>
<td>Rate (r)</td>
<td>64 bits</td>
<td>128 bits</td>
</tr>
</tbody>
</table>
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 $A_i$
• **Plaintext Processing:** inject plaintext blocks $P_i$ in the state and extract ciphertext blocks $C_i$
• **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

\[
\begin{align*}
\Sigma_0(x_0) &= x_0 \oplus (x_0 \gg 19) \oplus (x_0 \gg 28) \\
\Sigma_1(x_1) &= x_1 \oplus (x_1 \gg 61) \oplus (x_1 \gg 39) \\
\Sigma_2(x_2) &= x_2 \oplus (x_2 \gg 1) \oplus (x_2 \gg 6) \\
\Sigma_3(x_3) &= x_3 \oplus (x_3 \gg 10) \oplus (x_3 \gg 17) \\
\Sigma_4(x_4) &= x_4 \oplus (x_4 \gg 7) \oplus (x_4 \gg 41)
\end{align*}
\]
SECURITY ANALYSIS

- Differential and Linear Cryptanalysis

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Differential</th>
<th>Linear</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>44</td>
<td>43</td>
</tr>
<tr>
<td>...</td>
<td>&gt;64</td>
<td>&gt;64</td>
</tr>
</tbody>
</table>

Asiacrypt 2015
## SECURITY ANALYSIS

- Analysis of round-reduced versions

<table>
<thead>
<tr>
<th>Method</th>
<th>Rounds</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>cube-like</td>
<td>6/12</td>
<td>$2^{66}$</td>
</tr>
<tr>
<td></td>
<td>7/12</td>
<td>$2^{104}$</td>
</tr>
<tr>
<td>Differential-Linear</td>
<td>4/12</td>
<td>$2^{18}$</td>
</tr>
<tr>
<td></td>
<td>5/12</td>
<td>$2^{36}$</td>
</tr>
</tbody>
</table>

CT-RSA 2015, FSE 2017
OTHER ANALYSIS


- 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


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

<table>
<thead>
<tr>
<th></th>
<th>ASCON-Hash</th>
<th>ASCON-Xof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash size</td>
<td>256 bits</td>
<td>variable</td>
</tr>
<tr>
<td>State size (b)</td>
<td>320 bits</td>
<td>320 bits</td>
</tr>
<tr>
<td>Capacity (c)</td>
<td>256 bits</td>
<td>256 bits</td>
</tr>
<tr>
<td>Rate (r)</td>
<td>64 bits</td>
<td>64 bits</td>
</tr>
</tbody>
</table>
• **Absorbing**: updates the 320-bit state with the data block $M_i$
• **Squeezing**: extracts the final hash value
## SECURITY ANALYSIS

<table>
<thead>
<tr>
<th></th>
<th>Rounds</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascon-Hash</td>
<td>2/12</td>
<td>$2^{105}$</td>
</tr>
<tr>
<td>Ascon-Xof</td>
<td>2/12</td>
<td>$2^{15}$</td>
</tr>
<tr>
<td>(64 bits)</td>
<td>6/12</td>
<td>$2^{63.3}$</td>
</tr>
</tbody>
</table>

- Christoph Dobrânig, Maria Eichlseder, Florian Mendel, Martin Schläffer. Preliminary Analysis of Ascon-Xof and Ascon-Hash. 2019
IMPLEMENTATION

- Software
  - Intel Xeon
  - ARM Cortex-A53

- Hardware
  - High-speed
  - Low-area
SOFTWARE

• Intel Xeon

<table>
<thead>
<tr>
<th></th>
<th>64</th>
<th>512</th>
<th>1024</th>
<th>4096</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASCON-128</strong></td>
<td>17.3</td>
<td>12.9</td>
<td>10.8</td>
<td>10.5</td>
</tr>
<tr>
<td>(cycles/byte)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ASCON-128a</strong></td>
<td>14.1</td>
<td>9.7</td>
<td>7.3</td>
<td>6.9</td>
</tr>
<tr>
<td>(cycles/byte)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SOFTWARE

- ARM Cortex-A53

<table>
<thead>
<tr>
<th></th>
<th>64</th>
<th>512</th>
<th>1024</th>
<th>4096</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASCON-128</strong></td>
<td>18.3</td>
<td>14.4</td>
<td>11.3</td>
<td>11.0</td>
</tr>
<tr>
<td>(cycles/byte)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ASCON-128a</strong></td>
<td>15.1</td>
<td>11.2</td>
<td>7.6</td>
<td>7.3</td>
</tr>
<tr>
<td>(cycles/byte)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HARDWARE

- Unprotected Implementations

<table>
<thead>
<tr>
<th></th>
<th>Variant 1</th>
<th>Variant 2</th>
<th>Variant 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td>7.1</td>
<td>24.9</td>
<td>2.6</td>
</tr>
<tr>
<td><strong>Throughput</strong></td>
<td>5524</td>
<td>13218</td>
<td>14</td>
</tr>
</tbody>
</table>
HARDWARE

- Threshold Implementations

<table>
<thead>
<tr>
<th></th>
<th>Variant 1</th>
<th>Variant 2</th>
<th>Variant 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong> (kGE)</td>
<td>28.6</td>
<td>123.5</td>
<td>7.9</td>
</tr>
<tr>
<td><strong>Throughput</strong> (MByte/s)</td>
<td>3 774</td>
<td>9 018</td>
<td>14</td>
</tr>
</tbody>
</table>
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
FURTHER INFORMATION

https://ascon.iaik.tugraz.at