Update on the Security Analysis of AsCON

Christoph Dobranyin    Maria Eichlseder    Johannes Erlacher    Florian Mendel    Martin Schläffer

NIST LWC Workshop 2022 – 11 May 2022

https://ascon.iaik.tugraz.at
The Ascon Family

- Designed in 2014 [DEMS16]
- Selected in CAESAR portfolio as first choice for lightweight AEAD in 2019
- Published in Journal of Cryptology in 2021 [DEMS21c]
- Extensive published third-party cryptanalysis confirming its security margin

⭐ This talk: Overview of recent third-party cryptanalysis results & our own work on new security bounds [EME22]
Ascon’s Mode for Authenticated Encryption

- **Doubly-keyed** initialization/finalization for higher robustness under misuse
- **Duplex sponge** mode using a $5 \times 64 = 320$-bit permutation
Ascon Permutation: $a = 12$, $b \in \{6, 8\}$ Rounds

S-box layer

Linear layer

\[
\begin{align*}
x_0 & := x_0 \oplus (x_0 \gg 19) \oplus (x_0 \gg 28) \\
x_1 & := x_1 \oplus (x_1 \gg 61) \oplus (x_1 \gg 39) \\
x_2 & := x_2 \oplus (x_2 \gg 1) \oplus (x_2 \gg 6) \\
x_3 & := x_3 \oplus (x_3 \gg 10) \oplus (x_3 \gg 17) \\
x_4 & := x_4 \oplus (x_4 \gg 7) \oplus (x_4 \gg 41)
\end{align*}
\]
# Analysis of AsCON

<table>
<thead>
<tr>
<th>Key recovery</th>
<th>AsCON initialization</th>
<th>7 / 12</th>
<th>$2^{97}$</th>
<th>☒️</th>
<th>Cube-like</th>
<th>[LZWW17]</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsCON initialization</td>
<td>7 / 12</td>
<td>$2^{104}$</td>
<td>☒️</td>
<td>Cube-like</td>
<td>[LDW17]</td>
<td></td>
</tr>
<tr>
<td>AsCON initialization</td>
<td>7 / 12</td>
<td>$2^{123}$</td>
<td>✔️</td>
<td>Cube</td>
<td>[RHSS21]</td>
<td></td>
</tr>
<tr>
<td>AsCON initialization</td>
<td>6 / 12</td>
<td>$2^{74}$</td>
<td>☒️</td>
<td>Cond. HDL</td>
<td>[HP22]</td>
<td></td>
</tr>
<tr>
<td>AsCON initialization</td>
<td>5 / 12</td>
<td>$2^{31}$</td>
<td>✔️</td>
<td>Diff.-linear</td>
<td>[Tez20]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128a iteration</td>
<td>7 / 8</td>
<td>$2^{118}$</td>
<td>☒️</td>
<td>Cond. cube</td>
<td>[CKT22]</td>
<td></td>
</tr>
<tr>
<td>AsCON-80pq iteration</td>
<td>6 / 6</td>
<td>$2^{130}$</td>
<td>☒️</td>
<td>Cond. cube</td>
<td>[CHK22]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forgery</th>
<th>AsCON-128 finalization</th>
<th>6 / 12</th>
<th>$2^{33}$</th>
<th>☒️</th>
<th>Cube tester</th>
<th>[LZWW17]</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsCON-128 finalization</td>
<td>4 / 12</td>
<td>$2^{102}$</td>
<td>☒️</td>
<td>Differential</td>
<td>[DEMS15]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128 finalization</td>
<td>4 / 12</td>
<td>$2^{97}$</td>
<td>☒️</td>
<td>Differential</td>
<td>[GPT21]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128a finalization</td>
<td>3 / 12</td>
<td>$2^{20}$</td>
<td>✔️</td>
<td>Differential</td>
<td>[GPT21]</td>
<td></td>
</tr>
</tbody>
</table>

= nonce misuse  = exceeds data limit of $2^{64}$ blocks  = time exceeds $2^{128}$ weak-key variants omitted
Analysis of AsCON: (Partial*) state recovery

<table>
<thead>
<tr>
<th>State recovery</th>
<th>AsCON-128 iteration</th>
<th>6 / 6</th>
<th>$2^{40}$</th>
<th>No</th>
<th>Cond. cube</th>
<th>[BCP22]</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsCON-128 iteration*</td>
<td>6 / 6</td>
<td>$2^{45}$</td>
<td>No</td>
<td>Cond. cube</td>
<td>[CHK22]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128 iteration</td>
<td>5 / 6</td>
<td>$2^{66}$</td>
<td>No</td>
<td>Cube-like</td>
<td>[LZWW17]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128a iteration</td>
<td>7 / 8</td>
<td>$2^{118}$</td>
<td>No</td>
<td>Cond. cube</td>
<td>[CKT22]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128a iteration</td>
<td>3 / 8</td>
<td>$2^{117}$</td>
<td>Yes</td>
<td>Differential</td>
<td>[GPT21]</td>
<td></td>
</tr>
<tr>
<td>AsCON-128a iteration</td>
<td>2 / 8</td>
<td>–</td>
<td>Yes</td>
<td>Sat-Solver</td>
<td>[DKM+17]</td>
<td></td>
</tr>
</tbody>
</table>

= nonce misuse = exceeds data limit of $2^{64}$ blocks
weak-key variants omitted
## Analysis of ASCON-HASH and ASCON-XOF

<table>
<thead>
<tr>
<th>Type</th>
<th>Target</th>
<th>Output size</th>
<th>Rounds</th>
<th>Time</th>
<th>Method</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preimage</td>
<td>ASCON-XOF</td>
<td>64</td>
<td>6 / 12</td>
<td>$2^{63.3}$</td>
<td>Algebraic</td>
<td>[DEMS19]</td>
</tr>
<tr>
<td></td>
<td>ASCON-XOF</td>
<td>64</td>
<td>2 / 12</td>
<td>$2^{39}$</td>
<td>Cube-like</td>
<td>[DEMS19]</td>
</tr>
<tr>
<td>Collision</td>
<td>ASCON-XOF</td>
<td>all</td>
<td>4 / 12</td>
<td>–</td>
<td>Differential</td>
<td>[DEMS19]</td>
</tr>
<tr>
<td></td>
<td>ASCON-XOF</td>
<td>64</td>
<td>2 / 12</td>
<td>$2^{15}$</td>
<td>Differential</td>
<td>[ZDW19]</td>
</tr>
<tr>
<td></td>
<td>ASCON-HASH</td>
<td>256</td>
<td>2 / 12</td>
<td>$2^{125}$</td>
<td>Differential</td>
<td>[ZDW19]</td>
</tr>
<tr>
<td></td>
<td>ASCON-HASH</td>
<td>256</td>
<td>2 / 12</td>
<td>$2^{103}$</td>
<td>Differential</td>
<td>[GPT21]</td>
</tr>
</tbody>
</table>

(การออกแบบ IV)
## Analysis of AsCON’s Permutation

<table>
<thead>
<tr>
<th>Distinguisher</th>
<th>Permutation</th>
<th>$n/D$</th>
<th>$2^k$</th>
<th>Property</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permutation</td>
<td>12 / 12</td>
<td>$2^{55}$</td>
<td>Zero-sum</td>
<td>[HP22]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>11 / 12</td>
<td>$2^{85}$</td>
<td>Zero-sum</td>
<td>[DEMS21a]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>8 / 12</td>
<td>$2^{46}$</td>
<td>Integral</td>
<td>[HP22]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>7 / 12</td>
<td>$2^{65}$</td>
<td>Integral</td>
<td>[Tod15]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>7 / 12</td>
<td>$2^{60}$</td>
<td>Integral</td>
<td>[RHSS21]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>7 / 12</td>
<td>$2^{34}$</td>
<td>Limited-Birthday</td>
<td>[GPT21]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>5 / 12</td>
<td>$2^{109}$</td>
<td>Truncated Differential</td>
<td>[Tez16]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>5 / 12</td>
<td>$2^{80}$</td>
<td>Rectangle</td>
<td>[GPT21]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>5 / 12</td>
<td>$2^{109}$</td>
<td>Zero-Correlation</td>
<td>[DEMS21a]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>5 / 12</td>
<td>$2^{109}$</td>
<td>Impossible Differential</td>
<td>[DEMS21a]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>4 / 12</td>
<td>$2^{107}$</td>
<td>Differential</td>
<td>[DEMS21a]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>4 / 12</td>
<td>$2^{101}$</td>
<td>Linear</td>
<td>[DEM15a]</td>
<td></td>
</tr>
<tr>
<td>Permutation</td>
<td>3 / 12</td>
<td>$2^{101}$</td>
<td>Subspace Trails</td>
<td>[LTW18]</td>
<td></td>
</tr>
</tbody>
</table>

(.eye_open$=$ non-black-box distinguisher)
Analysis of Round-Reduced Ascon

Recent third-party analysis
Improvements to 7-Round Cube Attacks

Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon

Raghvendra Rohit\textsuperscript{1}, Kai Hu\textsuperscript{2,5}, Sumanta Sarkar\textsuperscript{3} and Siwei Sun\textsuperscript{4,6}

\textsuperscript{1} Univ Rennes, Centre National de la Recherche Scientifique (CNRS), Institut de Recherche en...

[Diving Deep into the Weak Keys of Round Reduced Ascon]

Raghvendra Rohit\textsuperscript{1} and Santanu Sarkar\textsuperscript{2,3}

\textsuperscript{1} Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE

\[\text{[RHSS21]}\] slightly reduced the data complexity of 7-round attacks to stay below the limit of \(2^{64}\) blocks.

\[\text{[RS21]}\] investigated classes of “weak keys” which permit slightly better cube attacks for 7 rounds.
Refined Results for Differential Attacks

Exploring Differential-Based Distinguishers and Forgeries for ASCON

David Gerauld\textsuperscript{1,2}, Thomas Peyrin\textsuperscript{1} and Quan Quan Tan\textsuperscript{1}

\textsuperscript{1} Nanyang Technological University, Singapore, Singapore

\[ \text{[GPT21]} \] investigate the applicability of \textbf{differential distinguishers} for forgeries and collisions.

\[ \text{[MR22]} \] find characteristics with \textbf{fewer active S-boxes} for 4 rounds (44 $\rightarrow$ 43) and 5 rounds (78 $\rightarrow$ 72).
[CT22] provide experiments on differential-linear cryptanalysis to refine previous results on 7 rounds.

[HP22] investigate higher-order DL distinguishers and find 8-round permutation distinguishers in a dedicated setting and 6-round key-recovery attacks.
Other Distinguishers

Simplified MITM Modeling for Permutations: New (Quantum) Attacks
André Schrottenloher and Marc Stevens
Cryptology Group, CWI, Amsterdam, The Netherlands
firstname.lastname@cwi.nl

(SS22a; SS22b) show that structural MitM attacks can find a fixpoint $x = P(x)$ for up to 2.5 rounds with complexity $2^{272}$.

Exploring Differential-Based Distinguishers and Forgeries for ASCON
David Gerault¹,², Thomas Peyrin¹ and Quan Quan Tan¹

¹ Nanyang Technological University, Singapore, Singapore

(GPT21) find limited-birthday distinguishers up to 7 rounds.
Misuse Analysis of Ascon

Recent third-party analysis
Analysis of Ascon in Misuse Settings

- Cryptanalysis in standard settings has only lead to small improvements in the last years
- Cryptanalysts increasingly consider misuse settings:
  - Nonce misuse
  - Decryption misuse
  - Implementation attacks
Analysis of Duplex Sponges in Misuse Settings

Generic nonce-misuse attacks on duplex designs include

- **Confidentiality break**
  with $1 + 1$ misuse query per block of the challenge message.

- **State recovery**
  with $D$ misuse queries, $T \cdot D = 2^c$.
  - Does not lead to trivial key recovery in Ascon

With more massive nonce misuse, some dedicated attacks are possible:
Conditional Cube Attacks on Ascon in Misuse Settings

Practical cube-attack against nonce-misused Ascon†
Jules Baudrin, Anne Canteaut and Léo Perrin
Inria, France

[BCP22] find conditional cube attacks with nonce misuse for the full 6 encryption rounds of Ascon-128.

Ascon-80pq in a Nonce-misuse Setting
Donghoon Chang1,2, Deukjo Hong1,3, and Jinkeon Kang1

[CHK22] find similar results and KR attacks for Ascon-80pq (> 2^{128}).

A New Conditional Cube Attack on Reduced-Round Ascon-128a in a Nonce-misuse Setting
Donghoon Chang1,2, Jinkeon Kang and Meltem Sönmez Turan1

[CKT22] find conditional cube attacks with nonce misuse for 7 of 8 round in Ascon-128A and a key-recovery attack.
Differential & Linear Cryptanalysis: New Bounds

ToSC 2022/1
Differential and Linear Characteristics of ASCON

- **S-box** has max. differential probability $2^{-2}$, max. squared correlation $2^{-2}$
- Goal: Prove lower bound on number of active S-boxes of characteristics
- **Weak alignment** → proving bounds is challenging, need bitwise model
**Bounds and Best Known Characteristics**

Gap of **provable bounds** vs. **best known characteristics** [DEMS15; DEM15b; GPT21]:

<table>
<thead>
<tr>
<th>Differential</th>
<th>R</th>
<th>min #S-boxes</th>
<th>max Probability</th>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>$2^{-2}$</td>
<td>DDT</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>$2^{-8}$</td>
<td>DDT</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>15</td>
<td>$\leq 2^{-30}$</td>
<td>SMT, nldtool</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>nldtool</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>CP</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
## Bounds and Best Known Characteristics

The gap of **provable bounds vs. best known characteristics** [DEMS15; DEM15b; GPT21]:

<table>
<thead>
<tr>
<th>Differential</th>
<th>$R$</th>
<th>$\text{min #S-boxes}$</th>
<th>$\text{max Probability}$</th>
<th>$\text{Methods}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>$2^{-2}$</td>
<td>$2^{-2}$</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td>$2^{-8}$</td>
<td>$2^{-8}$</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>15</td>
<td>$\leq 2^{-30}$</td>
<td>$2^{-40}$</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>$\geq 36$</td>
<td>$\leq 2^{-72}$</td>
<td>$2^{-107}$</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>$2^{-190}$</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>$\geq 54$</td>
<td>$\leq 2^{-108}$</td>
<td>-</td>
</tr>
</tbody>
</table>

- **New lower bounds for 4 and 6 rounds** [EME22]
- **Slightly better characteristics** [MR22]
### Bounds and Best Known Characteristics

Gap of **provable bounds** vs. **best known characteristics** [DEMS15; DEM15b; GPT21]:

<table>
<thead>
<tr>
<th>R</th>
<th>min #S-boxes</th>
<th>max Square Corr.</th>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$2^{-2}$</td>
<td>LAT</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$2^{-8}$</td>
<td>LAT</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>$\leq 2^{-26}$</td>
<td>SMT, lineartrails</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>lineartrails</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>lineartrails</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- **New lower bounds for 4 and 6 rounds** [EME22]
- **Slightly better characteristics** [MR22]
Bounds and Best Known Characteristics

Gap of **provable bounds** vs. **best known characteristics** [DEMS15; DEM15b; GPT21]:

<table>
<thead>
<tr>
<th>R</th>
<th>min #S-boxes</th>
<th>max Square Corr.</th>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$2^{-2}$</td>
<td>$2^{-2}$</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$2^{-8}$</td>
<td>$2^{-8}$</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>$\leq 2^{-26}$</td>
<td>$2^{-28}$</td>
</tr>
<tr>
<td>4</td>
<td>$\geq 36$</td>
<td>$\leq 2^{-72}$</td>
<td>$2^{-98}$</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>$2^{-186}$</td>
</tr>
<tr>
<td>6</td>
<td>$\geq 54$</td>
<td>$\leq 2^{-108}$</td>
<td>-</td>
</tr>
</tbody>
</table>

- New lower bounds for 4 and 6 rounds [EME22]
- Slightly better characteristics [MR22]
Approach for SAT Model to Prove Bounds

- **Optimized SAT model**
  - SAT encoding for characteristics by Sun et al. [SWW21; SWW18]
  - Different counter encodings
Approach for SAT Model to Prove Bounds

**Optimizer** SAT model

- SAT encoding for characteristics by Sun et al. [SWW21; SWW18]
- Different counter encodings

**Parallelization**

- Solver-based [HKWB11; HFB20; BSS15; SS21]
- Manual partitioning
Manual parallelization approach

Partition the search space into many independent problems

Categorize characteristics based on “girdle patterns”

- S-box activity within the round with fewest active S-boxes
Manual parallelization approach

- Partition the search space into **many independent problems**
- Categorize characteristics based on “**girdle patterns**”
  - S-box activity within the **round with fewest active S-boxes**
  - ![Diagram showing girdle patterns with S-boxes highlighted](image)
- **Reduce** the number of subproblems to be solved
- **Optimize** the individual SAT models
Manual parallelization approach

Consider rotational symmetries

- Use necklace theory to eliminate redundant checks [Mor72]
Manual parallelization approach

Consider rotational symmetries

- Use necklace theory to eliminate redundant checks [Mor72]

Prefilter individual problems

- Reduces model complexity
Manual parallelization approach

Consider **rotational symmetries**
- Use **necklace theory** to eliminate redundant checks [Mor72]

**Prefilter** individual problems
- Reduces model complexity

**Pooling** individual problems
- Reduces overhead
New Bounds

- Single characteristic for **4-round Ascon**
  - ≥ 36 active S-boxes
  - Runtime ≈ 600 CPU days
New Bounds

- Single characteristic for **4-round Ascon**
  - ≥ 36 active S-boxes
  - Runtime ≈ 600 CPU days

- Single characteristic for **6-round Ascon**
  - ≥ 54 active S-boxes
  - Runtime ≈ 60 CPU days
  - Utilizing intermediate results from our 4 round bound
New Bounds

- Single characteristic for **4-round Ascon**
  - $\geq 36$ active S-boxes
  - Runtime $\approx 600$ CPU days

- Single characteristic for **6-round Ascon**
  - $\geq 54$ active S-boxes
  - Runtime $\approx 60$ CPU days
  - Utilizing intermediate results from our 4 round bound

- Almost certainly not tight, but good enough to support trust in the permutation
Implications for Ascon

<table>
<thead>
<tr>
<th>R</th>
<th>min #S</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>≥ 54</td>
<td>≤ $2^{-108}$</td>
</tr>
<tr>
<td>8</td>
<td>≥ 72</td>
<td>≤ $2^{-144}$</td>
</tr>
<tr>
<td>12</td>
<td>≥ 108</td>
<td>≤ $2^{-216}$</td>
</tr>
</tbody>
</table>
Implications for ASCON

Authenticated Encryption: Initialization and Finalization

- **12 round** configuration
- Ample security margin for **128-bit security**
Implications for ASCON

Authenticated Encryption: Data processing

- ASCON-128: 6 rounds
- ASCON-128A: 8 rounds
- Data limit of $2^{64}$ encrypted blocks
- Goal: Find better (tighter) 6-round bound

<table>
<thead>
<tr>
<th>R</th>
<th>min #S</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$\geq 54$</td>
<td>$\leq 2^{-108}$</td>
</tr>
<tr>
<td>8</td>
<td>$\geq 72$</td>
<td>$\leq 2^{-144}$</td>
</tr>
<tr>
<td>12</td>
<td>$\geq 108$</td>
<td>$\leq 2^{-216}$</td>
</tr>
</tbody>
</table>
Implications for Ascon

**Ascon-Hash and Ascon-Xof**

- Difficult to evaluate unkeyed modes based on probability
- Assumption: $2^{-128}$ (attempts) $\times$ $2^{-64}$ (degrees of freedom)

$\Rightarrow$ **12 round bound** $< 2^{-192}$
Implications for AsCON

AsCON-Mac and AsCON-PRF [DEMS21b]

- AsCON-Mac, AsCON-PRF: **12 rounds**
- AsCON-MacA, AsCON-PRFaA: **8 rounds**
**Scenario:** Create collision based on 1-bit absorption

- For 1 to 4 rounds (consecutive bits), **no solution exists**
- For 5 rounds, collision-producing characteristic with 105 active S-boxes exists
- General bound: For 3+ final rounds in any collision-producing characteristic with 1-bit rate, there are at least 64 active S-boxes
Bounds for ISAP – 5-round characteristic
Conclusion

Ascon has received a lot of attention by cryptanalysts
- during CAESAR and during NIST LWC

Main results: Optimizations of 7-round cube attack; Misuse attacks
- No cryptanalytic breakthroughs
- Improved bounds


Bibliography IX


