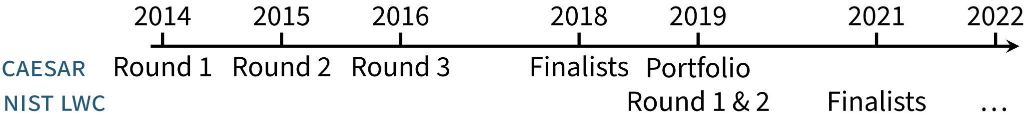
Update on the Security Analysis of Ascon

Christoph Dobraunig **Maria Eichlseder** Johannes Erlacher Florian Mendel Martin Schläffer

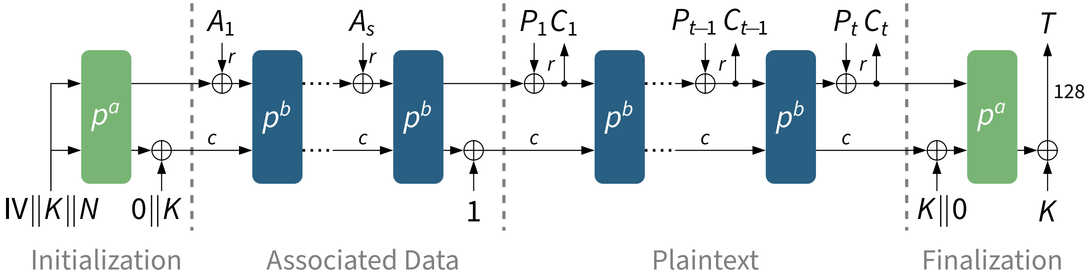
NIST LWC Workshop 2022 – 11 May 2022

The Ascon Family

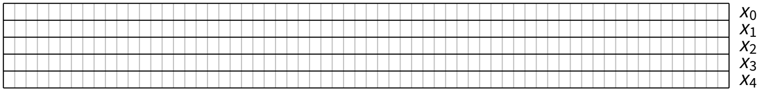
- Designed in 2014 [DEMS16]
- Selected in CAESAR portfolio as first choice for lightweight AEAD in 2019
- Published in Journal of Cryptology in 2021 [DEMS21c]
- Extensive published third-party cryptanalysis confirming its security margin
- **This talk**: Overview of recent third-party cryptanalysis results & our own work on new security bounds [EME22]



Ascon's Mode for Authenticated Encryption

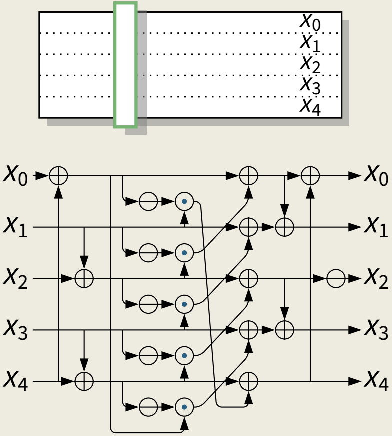


- **Doubly-keyed** initialization/finalization for higher robustness under misuse
- **Duplex sponge** mode using a $5 \times 64 = 320$-bit permutation

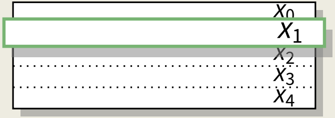


Ascon Permutation: $a = 12,\ b \in \{6, 8\}$ Rounds

S-box layer



Linear layer



$$x_0 := x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$

$$x_1 := x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$

$$x_2 := x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$$

$$x_3 := x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$

$$x_4 := x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$$

Analysis of Ascon

Key recovery	Ascon initialization	7 / 12	2^{97} ⊘	Cube-like	[LZWW17]
	Ascon initialization	7 / 12	2^{104}	Cube-like	[LDW17]
	Ascon initialization	7 / 12	2^{123} ✓	Cube	[RHSS21]
	Ascon initialization	6 / 12	2^{74}	Cond. HDL	[HP22]
	Ascon initialization	5 / 12	2^{31} ✓	Diff.-linear	[Tez20]
	Ascon-128a iteration	7 / 8	2^{118} ⊘	Cond. cube	[CKT22]
	Ascon-80pq iteration	6 / 6	2^{130} ⊘ ⌛	Cond. cube	[CHK22]
Forgery	Ascon-128 finalization	6 / 12	2^{33} ⊘	Cube tester	[LZWW17]
	Ascon-128 finalization	4 / 12	2^{102}	Differential	[DEMS15]
	Ascon-128 finalization	4 / 12	2^{97}	Differential	[GPT21]
	Ascon-128a finalization	3 / 12	2^{20} ✓	Differential	[GPT21]

⊘ = nonce misuse = exceeds data limit of 2^{64} blocks ⌛ = time exceeds 2^{128}

weak-key variants omitted

Analysis of Ascon: (Partial*) state recovery

State recovery	Ascon-128 iteration	6 / 6	2^{40}	⊘	Cond. cube	[BCP22]
	Ascon-128 iteration*	6 / 6	2^{45}	⊘	Cond. cube	[CHK22]
	Ascon-128 iteration	5 / 6	2^{66}	⊘	Cube-like	[LZWW17]
	Ascon-128a iteration	7 / 8	2^{118}	⊘ ⊗	Cond. cube	[CKT22]
	Ascon-128a iteration	3 / 8	2^{117}	✓	Differential	[GPT21]
	Ascon-128a iteration	2 / 8	—	✓	Sat-Solver	[DKM+17]

⊘ = nonce misuse ⊗ = exceeds data limit of 2^{64} blocks
weak-key variants omitted

Analysis of Ascon-Hash and Ascon-Xof

Type	Target	Output size	Rounds	Time	Method	Reference
Preimage	Ascon-Xof	64	6 / 12	$2^{63.3}$	Algebraic	[DEMS19]
	Ascon-Xof	64	2 / 12	2^{39}	Cube-like	[DEMS19]
Collision	Ascon-Xof	all	4 / 12	– ⊘	Differential	[DEMS19]
	Ascon-Xof	64	2 / 12	2^{15}	Differential	[ZDW19]
	Ascon-Hash	256	2 / 12	2^{125}	Differential	[ZDW19]
	Ascon-Hash	256	2 / 12	2^{103}	Differential	[GPT21]

(⊘ = chosen IV)

Analysis of Ascon's Permutation

Distinguisher	Permutation	12 / 12	2^{55} 👁	Zero-sum	[HP22]
	Permutation	11 / 12	2^{85} 👁	Zero-sum	[DEMS21a]
	Permutation	8 / 12	2^{46}	Integral	[HP22]
	Permutation	7 / 12	2^{65}	Integral	[Tod15]
	Permutation	7 / 12	2^{60}	Integral	[RHSS21]
	Permutation	7 / 12	2^{34} 👁	Limited-Birthday	[GPT21]
	Permutation	5 / 12	2^{109}	Truncated Differential	[Tez16]
	Permutation	5 / 12	2^{80}	Rectangle	[GPT21]
	Permutation	5 / 12	–	Zero-Correlation	[DEMS21a]
	Permutation	5 / 12	–	Impossible Differential	[DEMS21a]
	Permutation	4 / 12	2^{107}	Differential	[DEMS21a]
	Permutation	4 / 12	2^{101}	Linear	[DEM15a]
	Permutation	3 / 12	–	Subspace Trails	[LTW18]

(👁 = 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[1], Kai Hu[2,5], Sumanta Sarkar[3] and Siwei Sun[4,6]

[1] Univ Rennes, Centre National de la Recherche Scientifique (CNRS), Institut de Recherche en

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

Diving Deep into the Weak Keys of Round Reduced Ascon

Raghvendra Rohit[1] and Santanu Sarkar[2,3]

[1] Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE

[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 Gerault[1,2], Thomas Peyrin[1] and Quan Quan Tan[1]

[1] Nanyang Technological University, Singapore, Singapore

[GPT21] investigate the applicability of **differential distinguishers for forgeries and collisions**.

[MR22] find characteristics with **fewer active S-boxes** for 4 rounds ($44 \rightarrow 43$) and 5 rounds ($78 \rightarrow 72$).

(Higher-Order) Differential-Linear Distinguishers

Differential-linear Attacks on Permutation Ciphers Revisited: Experiments on Ascon and DryGASCON

Aslı Başak Civek[a] and Cihangir Tezcan[b]
…tics Institute, Department of Cyber Security, CyDeS Laboratory, Middle East Technical University, Ankara

Revisiting Higher-Order Differential(-Linear) Attacks from an Algebraic Perspective

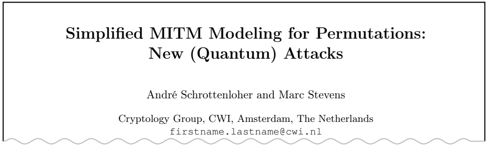
Applications to Ascon, Grain v1, Xoodoo, and ChaCha

Kai Hu and Thomas Peyrin

[CT22] provide experiments on **differential-linear cryptanalysis** to refine previous results on 7 rounds.

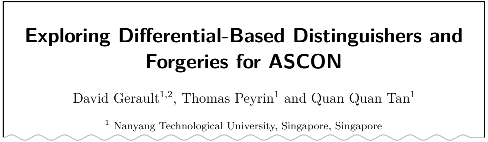
[HP22] investigate **higher-order DL distinguishers** and find 8-round permutation distinguishers in a dedicated setting and 6-round key-recovery attacks.

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


Exploring Differential-Based Distinguishers and Forgeries for ASCON

David Gerault[1,2], Thomas Peyrin[1] and Quan Quan Tan[1]

[1] Nanyang Technological University, Singapore, Singapore

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

[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 Chang[1,2], Deukjo Hong[1,3], and Jinkeon Kang[1]

[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 Chang[1,2], Jinkeon Kang[1] and Meltem Sönmez Turan[1]

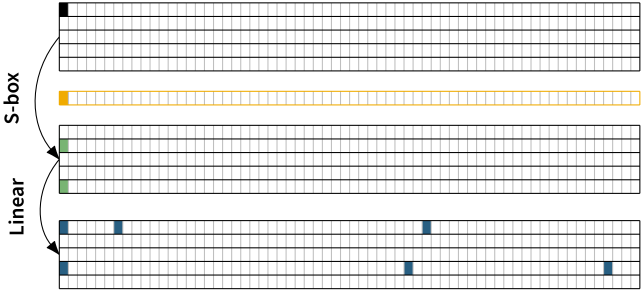
[CKT22] find conditional cube attacks with nonce misuse for 7 of 8 round in Ascon-128a and a key-recovery attack.

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** $\rightarrow$ proving bounds is challenging, need bitwise model



Bounds and Best Known Characteristics

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

	R	min #S-boxes (provable)	min #S-boxes (best known)	max Probability (provable)	max Probability (best known)	Methods
Differential	1	1	1	2^{-2}	2^{-2}	DDT
	2	4	4	2^{-8}	2^{-8}	DDT
	3	15	15	$\leq 2^{-30}$	2^{-40}	SMT, `nldtool`
	4	-	44	-	2^{-107}	`nldtool`
	5	-	78	-	2^{-190}	CP
	6	-	-	-	-	

Bounds and Best Known Characteristics

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

	R	min #S-boxes		max Probability		Methods
Differential	1	1	1	2^{-2}	2^{-2}	DDT
	2	4	4	2^{-8}	2^{-8}	DDT
	3	15	15	$\leq 2^{-30}$	2^{-40}	SMT, `nldtool`
	4	$\geq$ **36**	43	$\leq 2^{-\mathbf{72}}$	2^{-107}	`nldtool`, SAT
	5	-	72	-	2^{-190}	CP, SAT
	6	$\geq$ **54**	-	$\leq 2^{-\mathbf{108}}$	-	

- 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]:

	R	min #S-boxes (provable)	min #S-boxes (best known)	max Square Corr. (provable)	max Square Corr. (best known)	Methods
Linear	1	1	1	2^{-2}	2^{-2}	LAT
	2	4	4	2^{-8}	2^{-8}	LAT
	3	13	13	$\leq 2^{-26}$	2^{-28}	SMT, `lineartrails`
	4	-	43	-	2^{-98}	`lineartrails`
	5	-	67	-	2^{-186}	`lineartrails`
	6	-	-	-	-	

- 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]:

	R	min #S-boxes		max Square Corr.		Methods
Linear	1	1	1	2^{-2}	2^{-2}	LAT
	2	4	4	2^{-8}	2^{-8}	LAT
	3	13	13	$\leq 2^{-26}$	2^{-28}	SMT, `lineartrails`
	4	**$\geq$ 36**	43	$\leq 2^{-72}$	2^{-98}	`lineartrails`, SAT
	5	-	67	-	2^{-186}	`lineartrails`
	6	**$\geq$ 54**	-	$\leq 2^{-108}$	-	SAT

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

Approach for SAT Model to Prove Bounds

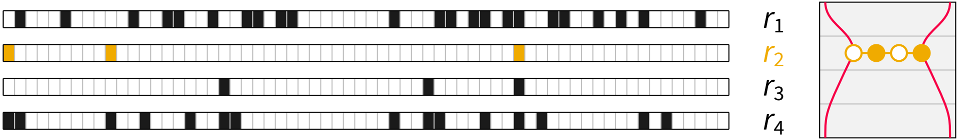
- **Optimized** SAT model
  - **SAT encoding** for **characteristics** by Sun et al. [SWW21; SWW18]
  - Different **counter encodings**

Approach for SAT Model to Prove Bounds

- **Optimized** SAT model
  - **SAT encoding** for **characteristics** by Sun et al. [SWW21; SWW18]
  - Different **counter encodings**
- **Parallelization**
  - Solver-based [HKWB11; HFB20; BSS15; SS21]
  - Manual partitioning

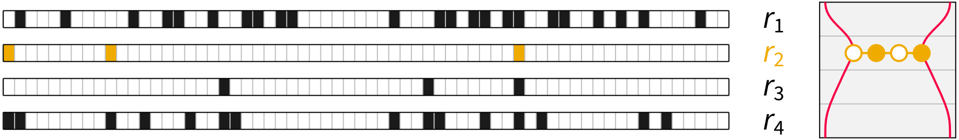
Manual parallelization approach

- **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**

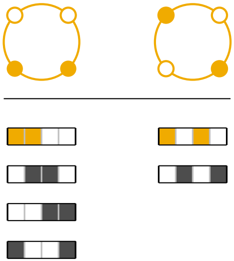


- **Reduce** the number of subproblems to be solved
- **Optimize** the individual SAT models

Manual parallelization approach

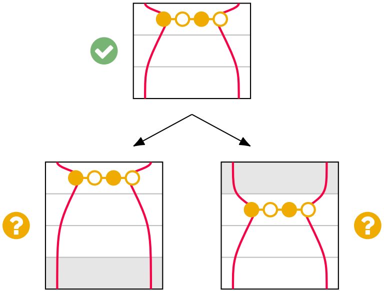
Consider **rotational symmetries**

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



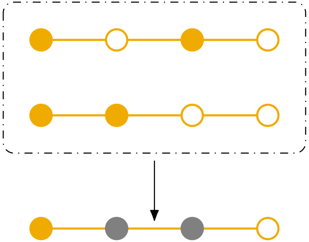
Manual parallelization approach

- 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**
  - $\geq$ **36 active S-boxes**
  - Runtime $\approx$ 600 CPU days

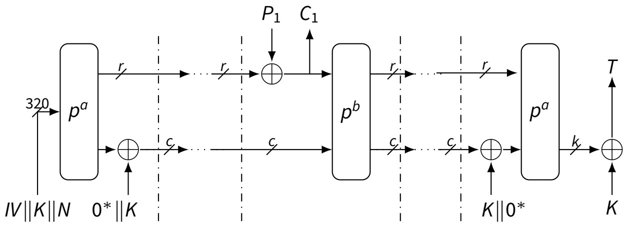
New Bounds

- 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

New Bounds

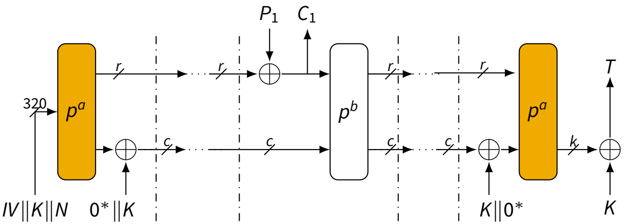
- Single characteristic for **4-round Ascon**
  - $\geq$ **36 active S-boxes**
  - Runtime $\approx$ 600 CPU days
- Single characteristic for **6-round Ascon**
  - $\geq$ **54 active S-boxes**
  - Runtime $\approx$ 60 CPU days
  - Utilizing intermediate results from our 4 round bound
- Almost certainly not tight, but good enough to support trust in the permutation

Implications for Ascon



R	min #S	Probability
6	$\geq$ 54	$\leq 2^{-108}$
8	$\geq$ 72	$\leq 2^{-144}$
12	$\geq$ 108	$\leq 2^{-216}$

Implications for ASCON

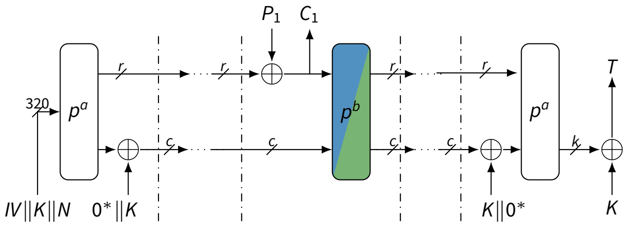


R	min #S	Probability
6	$\geq$ 54	$\leq 2^{-108}$
8	$\geq$ 72	$\leq 2^{-144}$
12	$\geq$ 108	$\leq 2^{-216}$

Authenticated Encryption: Initialization and Finalization

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

Implications for Ascon

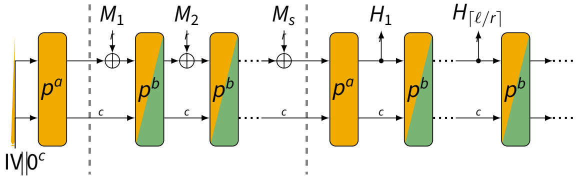


R	min #S	Probability
6	$\geq$ 54	$\leq 2^{-108}$
8	$\geq$ 72	$\leq 2^{-144}$
12	$\geq$ 108	$\leq 2^{-216}$

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

Implications for Ascon



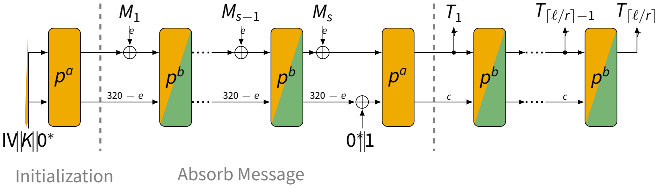
R	min #S	Probability
6	$\geq$ 54	$\leq 2^{-108}$
8	$\geq$ 72	$\leq 2^{-144}$
12	$\geq$ 108	$\leq 2^{-216}$

Ascon-Hash and Ascon-Xof

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

➔ 12 round bound $< 2^{-192}$

Implications for Ascon

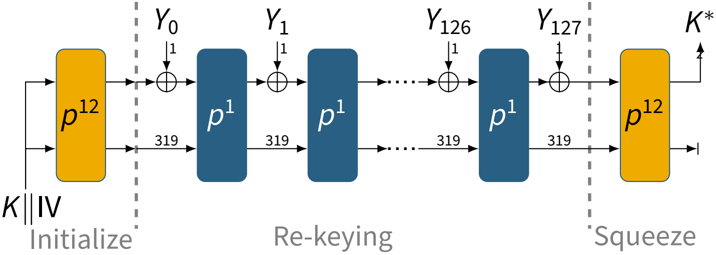


R	min #S	Probability
6	$\geq$ 54	$\leq 2^{-108}$
8	$\geq$ 72	$\leq 2^{-144}$
12	$\geq$ 108	$\leq 2^{-216}$

Ascon-Mac and Ascon-Prf [DEMS21b]

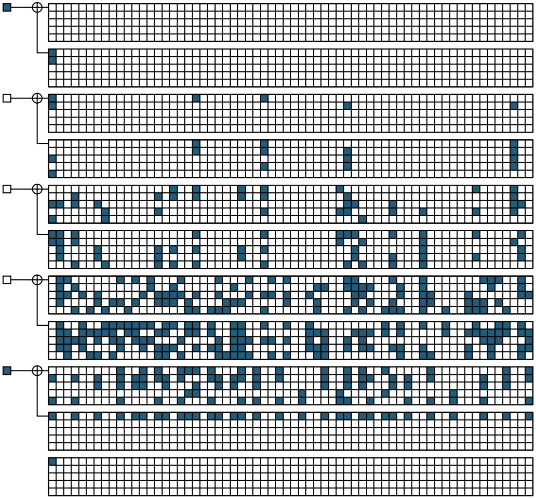
- Ascon-Mac, Ascon-Prf: **12 rounds**
- Ascon-MacA, Ascon-PrfA: **8 rounds**

Bounds for ISAP



- **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 I

[BCP22] Jules Baudrin, Anne Canteaut, and Léo Perrin. **Practical cube-attack against nonce-misused Ascon**. FSE 2022 Rump Session. 2022. URL: https://youtu.be/avBHsIM_5DA?t=2582.

[BSS15] Tomás Balyo, Peter Sanders, and Carsten Sinz. **HordeSat: A Massively Parallel Portfolio**. Theory and Applications of Satisfiability Testing – SAT 2015. Vol. 9340. LNCS. Springer, 2015, pp. 156–172. DOI: 10.1007/978-3-319-24318-4_12.

[CHK22] Donghoon Chang, Deukjo Hong, and Jinkeon Kang. **Conditional Cube Attacks on Ascon-128 and Ascon-80pq in a Nonce-misuse Setting**. IACR Cryptology ePrint Archive, Report 2022/544. 2022. URL: https://eprint.iacr.org/2022/544.

[CKT22] Donghoon Chang, Jinkeon Kang, and Meltem Sönmez Turan. **A New Conditional Cube Attack on Reduced-Round Ascon-128a in a Nonce-misuse Setting**. NIST LWC Workshop 2022. 2022.

Bibliography II

[CT22] Aslí Basak Civek and Cihangir Tezcan. **Differential-linear Attacks on Permutation Ciphers Revisited: Experiments on Ascon and DryGASCON.** Information Systems Security and Privacy – ICISSP 2022. SCITEPRESS, 2022, pp. 202–209. DOI: 10.5220/0010982600003120.

[DEM15a] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. **Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates.** ASIACRYPT 2015. Vol. 9453. LNCS. Springer, 2015, pp. 490–509. DOI: 10.1007/978-3-662-48800-3_20.

[DEM15b] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. **Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates.** Advances in Cryptology – ASIACRYPT 2015. Vol. 9453. LNCS. Springer, 2015, pp. 490–509. DOI: 10.1007/978-3-662-48800-3_20.

Bibliography III

[DEMS15] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Cryptanalysis of Ascon.** Topics in Cryptology – CT-RSA 2015. Vol. 9048. LNCS. Springer, 2015, pp. 371–387. DOI: 10.1007/978-3-319-16715-2_20.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Ascon v1.2.** CAESAR Competition. 2016. URL: https://competitions.cr.yp.to/caesar-submissions.html.

[DEMS19] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Preliminary Analysis of Ascon-Xof and Ascon-Hash.** Technical Report. 2019. URL: https://ascon.iaik.tugraz.at.

[DEMS21a] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Ascon.** Submission as a Finalist to the NIST Lightweight Crypto Standardization Process. 2021. URL: https://csrc.nist.gov/Projects/lightweight-cryptography/finalists.

Bibliography IV

[DEMS21b] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Ascon PRF, MAC, and Short-Input MAC.** IACR Cryptology ePrint Archive, Report 2021/1574. 2021. URL: https://ia.cr/2021/1574.

[DEMS21c] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Ascon v1.2: Lightweight Authenticated Encryption and Hashing.** Journal of Cryptology 34.3 (2021), p. 33. DOI: 10.1007/s00145-021-09398-9.

[DKM+17] Ashutosh Dhar Dwivedi, Miloš Klouček, Pawel Morawiecki, Ivica Nikolič, Josef Pieprzyk, and Sebastian Wójtowicz. **SAT-based Cryptanalysis of Authenticated Ciphers from the CAESAR Competition.** SECRYPT ICETE 2017. SciTePress, 2017, pp. 237–246. DOI: 10.5220/0006387302370246.

[EME22] Johannes Erlacher, Florian Mendel, and Maria Eichlseder. **Bounds for the Security of Ascon against Differential and Linear Cryptanalysis.** IACR Transactions on Symmetric Cryptology 2022.1 (2022), pp. 64–87. DOI: 10.46586/tosc.v2022.i1.64-87.

Bibliography V

[GPT21] David Gérault, Thomas Peyrin, and Quan Quan Tan. **Exploring Differential-Based Distinguishers and Forgeries for ASCON.** IACR Transactions on Symmetric Cryptology 2021.3 (2021), pp. 102–136. DOI: 10.46586/tosc.v2021.i3.102-136.

[HFB20] Maximilian Heisinger, Mathias Fleury, and Armin Biere. **Distributed Cube and Conquer with Paracooba.** Theory and Applications of Satisfiability Testing – SAT 2020. Vol. 12178. LNCS. Springer, 2020, pp. 114–122. DOI: 10.1007/978-3-030-51825-7_9.

[HKWB11] Marijn Heule, Oliver Kullmann, Siert Wieringa, and Armin Biere. **Cube and Conquer: Guiding CDCL SAT Solvers by Lookaheads.** Hardware and Software: Verification and Testing Conference – HVC 2011. Vol. 7261. LNCS. Springer, 2011, pp. 50–65. DOI: 10.1007/978-3-642-34188-5_8.

Bibliography VI

[HP22] Kai Hu and Thomas Peyrin. **Revisiting Higher-Order Differential(-Linear) Attacks from an Algebraic Perspective: Applications to Ascon, Grain v1, Xoodoo, and ChaCha**. NIST LWC Workshop 2022. 2022.

[LDW17] Zheng Li, Xiaoyang Dong, and Xiaoyun Wang. **Conditional Cube Attack on Round-Reduced ASCON**. IACR Transactions on Symmetric Cryptology 2017.1 (2017), pp. 175–202. ISSN: 2519-173X. DOI: 10.13154/tosc.v2017.i1.175-202. URL: https://github.com/lizhengcn/Ascon_test.

[LTW18] Gregor Leander, Cihangir Tezcan, and Friedrich Wiemer. **Searching for Subspace Trails and Truncated Differentials**. IACR Transactions on Symmetric Cryptology 2018.1 (2018), pp. 74–100. DOI: 10.13154/tosc.v2018.i1.74-100.

[LZWW17] Yanbin Li, Guoyan Zhang, Wei Wang, and Meiqin Wang. **Cryptanalysis of round-reduced ASCON**. SCIENCE CHINA Information Sciences 60.3 (2017), p. 38102. DOI: 10.1007/s11432-016-0283-3.

Bibliography VII

[Mor72] C. Moreau. **Sur les permutations circulaires distinctes.** fr. Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale 2e série, 11 (1872), pp. 309–314. URL: http://www.numdam.org/item/NAM_1872_2_11__309_0/.

[MR22] Rusydi H. Makarim and Raghvendra Rohit. **Towards Tight Differential Bounds of Ascon.** FSE 2022 Rump Session. 2022. URL: https://youtu.be/avBHsIM_5DA?t=2091.

[RHSS21] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. **Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon.** IACR Transactions of Symmetric Cryptology 2021.1 (2021), pp. 130–155. DOI: 10.46586/tosc.v2021.i1.130-155.

[RS21] Raghvendra Rohit and Santanu Sarkar. **Diving Deep into the Weak Keys of Round Reduced Ascon.** IACR Transactions on Symmetric Cryptology 2021.4 (2021), pp. 74–99. DOI: 10.46586/tosc.v2021.i4.74-99.

Bibliography VIII

[SS21] Dominik Schreiber and Peter Sanders. **Scalable SAT Solving in the Cloud.** Theory and Applications of Satisfiability Testing – SAT 2021. Vol. 12831. LNCS. Springer, 2021, pp. 518–534. DOI: 10.1007/978-3-030-80223-3_35.

[SS22a] André Schrottenloher and Marc Stevens. **MitM Attacks on Ascon.** Personal communication. 2022.

[SS22b] André Schrottenloher and Marc Stevens. **Simplified MITM Modeling for Permutations: New (Quantum) Attacks.** Dagstuhl Seminar 22141 Symmetric Cryptology. 2022. URL: https://eprint.iacr.org/2022/189.

[SWW18] Ling Sun, Wei Wang, and Meiqin Wang. **More Accurate Differential Properties of LED64 and Midori64.** IACR Transactions on Symmetric Cryptology 2018.3 (2018), pp. 93–123. DOI: 10.13154/tosc.v2018.i3.93-123.

Bibliography IX

[SWW21] Ling Sun, Wei Wang, and Meiqin Wang. **Accelerating the Search of Differential and Linear Characteristics with the SAT Method.** IACR Transactions on Symmetric Cryptology 2021.1 (2021), pp. 269–315. DOI: 10.46586/tosc.v2021.i1.269-315.

[Tez16] Cihangir Tezcan. **Truncated, Impossible, and Improbable Differential Analysis of Ascon.** ICISSP 2016. SciTePress, 2016, pp. 325–332. DOI: 10.5220/0005689903250332.

[Tez20] Cihangir Tezcan. **Analysis of Ascon, DryGASCON, and Shamash Permutations.** International Journal of Information Security Science 9.3 (2020), pp. 172–187. URL: https://www.ijiss.org/ijiss/index.php/ijiss/article/view/762.

[Tod15] Yosuke Todo. **Structural Evaluation by Generalized Integral Property.** EUROCRYPT 2015. Vol. 9056. LNCS. Springer, 2015, pp. 287–314. DOI: 10.1007/978-3-662-46800-5_12.

Bibliography X

[ZDW19] Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. **Collision Attacks on Round-Reduced Gimli-Hash/Ascon-Xof/Ascon-Hash.** IACR Cryptology ePrint Archive, Report 2019/1115. 2019.