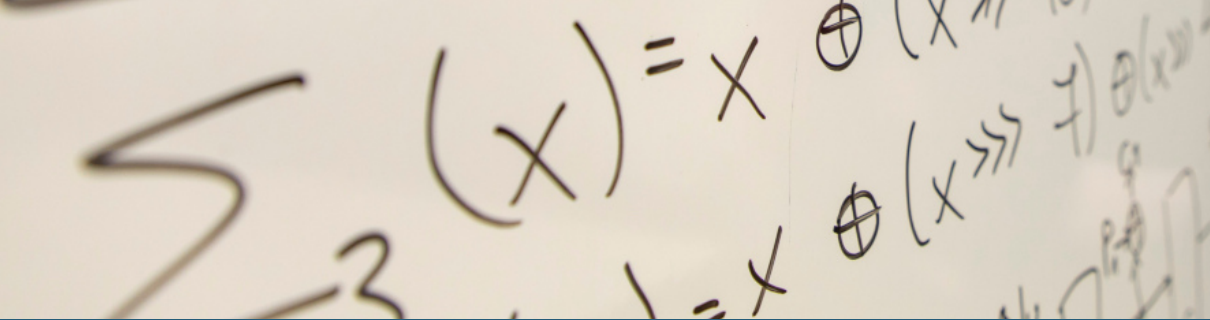


The Ascon Family for Lightweight Cryptography

Christoph Dobraunig · **Maria Eichlseder** · Florian Mendel · Martin Schläffer

- PBC 2023
- Lyon · 23 April 2023

TU Graz

› https://ascon.iaik.tugraz.at

Motivation

Lightweight Cryptography

Need lightweight authenticated encryption and hashing algorithms

Low **area** · Low **energy** · Low **power** · Low **latency**

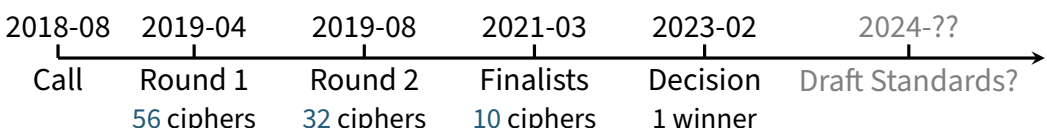
for efficient, secure, robust implementations on constrained devices

National Institute of Standards and Technology
U.S. Department of Commerce

LWC Competition – Standardizing LightWeight Crypto

- Standardize lightweight authenticated encryption and hashing algorithms
- Organized by NIST (US National Institute of Standards and Technology)

https://csrc.nist.gov/projects/lightweight-cryptography



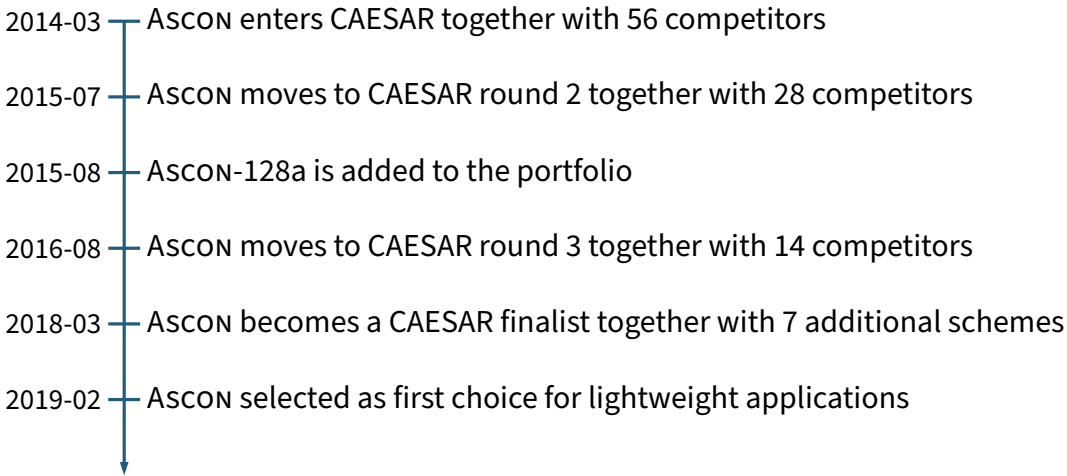
Designing the Ascon Family

The Ascon Team

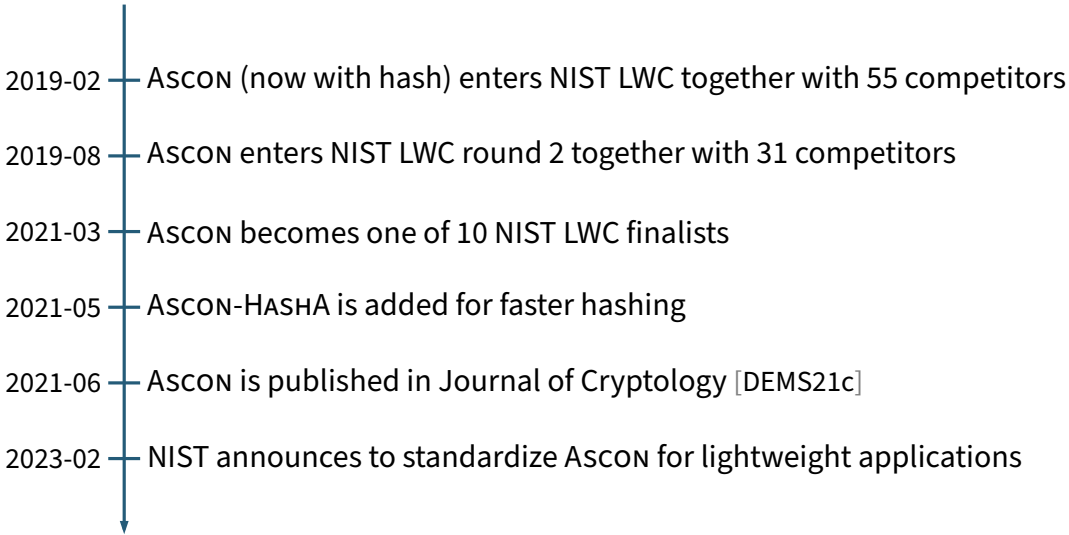
- Martin Schläffer
- Florian Mendel
- Christoph Dobraunig
- Maria Eichlseder

(c) Lunghammer, TU Graz

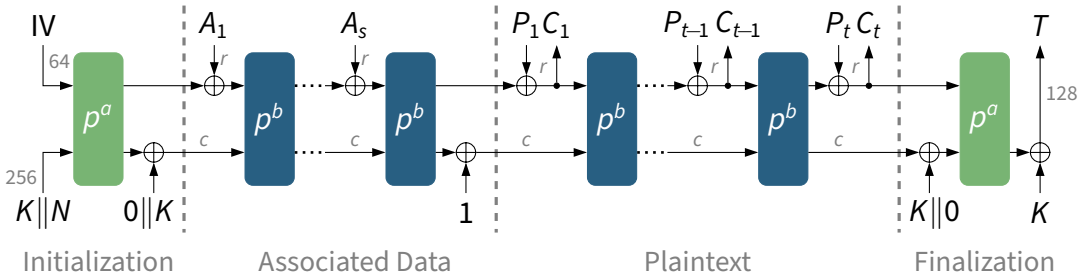
History I


2014-03
Ascon enters CAESAR together with 56 competitors
2015-07
Ascon moves to CAESAR round 2 together with 28 competitors
2015-08
Ascon-128a is added to the portfolio
2016-08
Ascon moves to CAESAR round 3 together with 14 competitors
2018-03
Ascon becomes a CAESAR finalist together with 7 additional schemes
2019-02
Ascon selected as first choice for lightweight applications

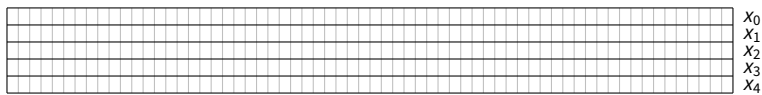
History II


2019-02
Ascon (now with hash) enters NIST LWC together with 55 competitors
2019-08
Ascon enters NIST LWC round 2 together with 31 competitors
2021-03
Ascon becomes one of 10 NIST LWC finalists
2021-05
Ascon-Hasha is added for faster hashing
2021-06
Ascon is published in Journal of Cryptology [DEMS21c]
2023-02
NIST announces to standardize Ascon for lightweight applications

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

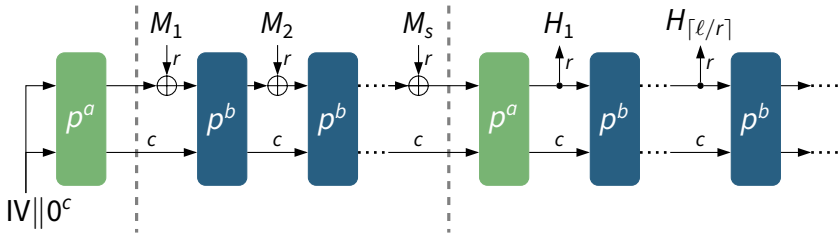


AEAD Family

Name	Algorithms	Bit size of				Rounds	
		key	nonce	tag	data block	p^a	p^b
Ascon-128	$\mathcal{E}, \mathcal{D}_{128,64,12,6}$	128	128	128	64	12	6
Ascon-128a	$\mathcal{E}, \mathcal{D}_{128,128,12,8}$	128	128	128	128	12	8
Ascon-80pq	$\mathcal{E}, \mathcal{D}_{160,64,12,6}$	160	128	128	64	12	6

- **Ascon-128**: Primary recommendation
- **Ascon-128a**: Same security, 33 % faster (more rounds but larger rate)
- **Ascon-80pq**: Same classical security, higher PQ security

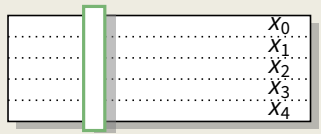
Ascon Hashing

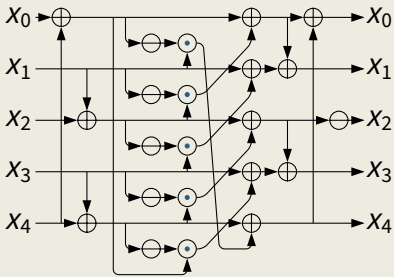


Name	Algorithm	Bit size of		Rounds	
		hash	data block	p^a	p^b
Ascon-Hash	$\mathcal{X}_{256,64,12,12}$ with $\ell = 256$	256	64	12	12
Ascon-Hasha	$\mathcal{X}_{256,64,12,8}$ with $\ell = 256$	256	64	12	8

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

S-box layer





Linear layer

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

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

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

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

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

Security

When used correctly (nonce-respecting, etc.):

Requirement	Security in bits			
	Ascon-128 Ascon-128a	Ascon-80pq	Ascon-Hash Ascon-Hasha	Ascon-Xof Ascon-Xofa
Confidentiality of M	128	128		
Integrity of M, A, N	128	128		
Collision resistance			128	$\min(128, \ell/2)$
Pre-image resistance			128	$\min(128, \ell)$

In case of nonce misuse or other misuse (side-channels, …):
Aim to keep damage “local” to misused setting (resilience)

Implementing Ascon

Ascon Permutation Properties

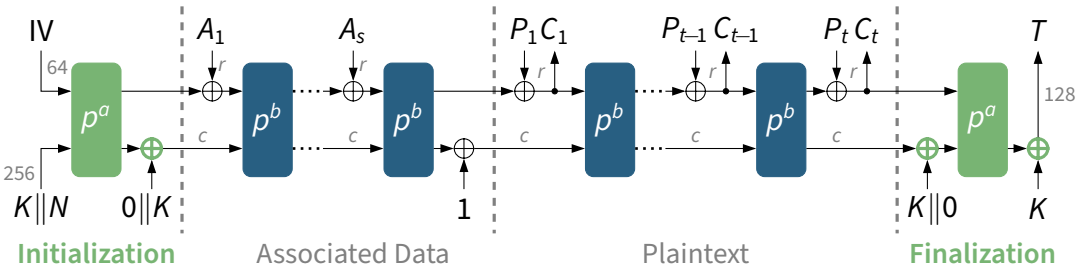
- **Simplicity**
  - Low 320-bit state size
  - Bitwise Boolean functions defined on 64-bit words
- **Bitsliced in Software**
  - 64-bit words
  - Up to 5 instructions in parallel
  - Minimal temporary registers
- **Flexible in Hardware**
  - Small area
  - High speed
- **Easy to integrate side-channel countermeasures**
  - No look-up tables
  - Low-degree S-boxes
  - Easy to mask

Ascon Performance Characteristics

- Often much more efficient than AES-GCM
  - Up to **3x to 5x speed on microcontrollers** (from `https://lwc.las3.de`)
  - Up to **2x throughput** with **0.5x energy** in hardware (from `https://ia.cr/2021/049`)
- Designed for ease of protection against physical attacks

Protecting against Implementation Attacks

- Robustness: Limited damage if state recovered through some misuse
- **Mode**: **Levelled Implementation** [BBC+20]: only **Init/Final** need full protection



- **Primitive**: Efficient masking (e.g., using Toffoli gate [DDE+20])

Analyzing Ascon

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)

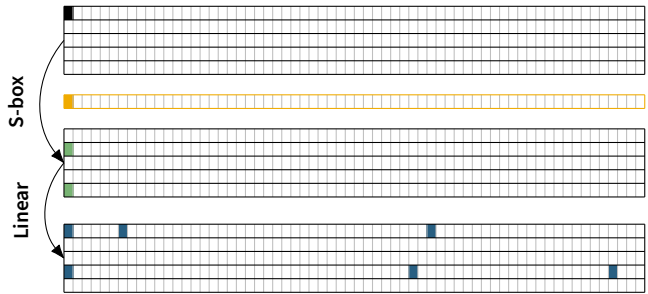
Analysis of Ascon in Misuse Settings

- Cryptanalysts increasingly consider misuse settings:
  Nonce misuse · Decryption misuse · Implementation attacks
- 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

Differential and Linear Characteristics of Ascon

- Goal: Prove lower bound on number of **active S-boxes** of characteristics
- **S-box** has max. differential probability 2^{-2}, max. squared correlation 2^{-2}
- **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		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	-	44	-	2^{-107}	`nldtool`, SAT
	5	-	78	-	2^{-190}	CP, SAT
	6	-	-	-	-	

- New lower bounds for **4** and **6** rounds [EME22; HMMD22]
- 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 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	≥ 36	43	$\leq 2^{-86}$	2^{-107}	`nldtool`, [HMMD22]
	5	-	72	$\leq 2^{-100}$	2^{-190}	CP, [HMMD22]
	6	≥ 54	-	$\leq 2^{-129}$	-	

- New lower bounds for **4** and **6** rounds [EME22; HMMD22]
- Slightly better characteristics [MR22]

Bounds and Best Known Characteristics

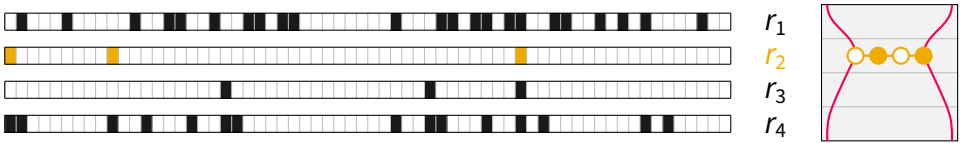
Gap of **provable bounds** vs. **best known characteristics** [DEMS15; DEM15b; GPT21]:

	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	2^{-28}	2^{-28}	SMT, `lineartrails`, [HMMD22]
	4	≥ 36	43	$\leq 2^{-88}$	2^{-98}	`lineartrails`, [HMMD22]
	5	-	67	$\leq 2^{-96}$	2^{-186}	`lineartrails`, [HMMD22]
	6	≥ 54	-	$\leq 2^{-132}$	-	[HMMD22]

- New lower bounds for **4** and **6** rounds [EME22; HMMD22]
- Slightly better characteristics [MR22]

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

Shaping & Extending the Ascon Family

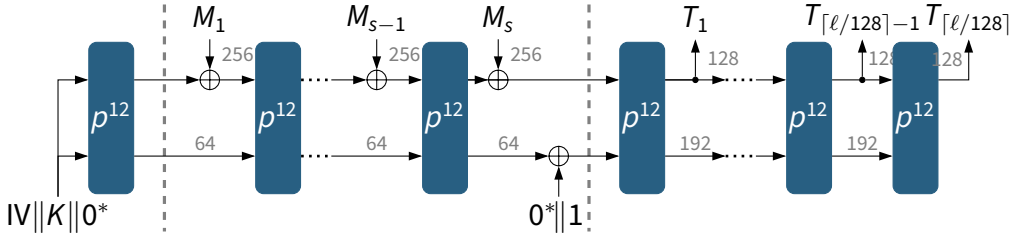
What's Next?

NIST will …

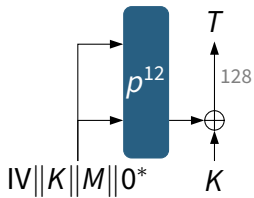
- publish a report (NIST IR 8454) with details on the competition process
- work with the Ascon team to draft the new standard for public comments
- host a workshop (June 21–22) to discuss various aspects of the process

Open discussion: Potential extensions based on requests from community (MAC/PRF, key/tag sizes, sessions, …)

Potential Extensions for MAC/PRF/KDF: Ascon-PRF [DEMS21b]



Ascon-PRFshort:



Conclusion

- NIST announced selection of Ascon as new lightweight cryptography standard
- Ascon has received a lot of attention by cryptanalysts (CAESAR, LWC)
- Many implementations for different platforms available

- Many decisions to be made for final standard (variants, extensions)
- Now is the perfect time for comments and suggestions

Bibliography I

[BBC+20] Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. **Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography – A Practical Guide Through the Leakage-Resistance Jungle**. Advances in Cryptology – CRYPTO 2020. Vol. 12170. LNCS. Springer, 2020, pp. 369–400. DOI: 10.1007/978-3-030-56784-2_13.

[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

[DDE+20] Joan Daemen, Christoph Dobraunig, Maria Eichlseder, Hannes Groß, Florian Mendel, and Robert Primas. **Protecting against Statistical Ineffective Fault Attacks**. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020.3 (2020), pp. 508–543.

[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.

[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.

Bibliography III

[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.

[DEMS21b] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. **Ascon PRF, MAC, and Short-Input MAC**. IACR Cryptol. ePrint Arch., Report 2021/1574. 2021. URL: https://eprint.iacr.org/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 IV

[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.

[HMMD22] Solane El Hirch, Silvia Mella, Alireza Mehrdad, and Joan Daemen. **Improved Differential and Linear Trail Bounds for ASCON**. IACR Trans. Symmetric Cryptol. 2022.4 (2022), pp. 145–178. DOI: 10.46586/tosc.v2022.i4.145-178.

[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.

Bibliography V

[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.

[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.

Bibliography VI

[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.

[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.

[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 VII

[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.