The Ascon Family: Lightweight Authenticated Encryption, Hashing, and More

Christoph Dobraunig, Maria Eichlseder,
Florian Mendel, Martin Schläffer

Ascon Team

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

The Ascon family

- **Authenticated encryption** (CAESAR, 2014)
  - Ascon-128
  - Ascon-128a
- **Hashing** (NIST, 2019)
  - Ascon-Hash/Xof
  - Ascon-Hasha/Xofa
- **Extensions** (ePrint, 2021)
  - Ascon-Mac/Prf
  - Ascon-PrfShort

The Ascon design basics

- **Permutation based**
  - Single 320-bit permutation (all)

- **Sponge based**
  - Absorb/squeeze (Hash, XOF)
  - Duplex-mode (AEAD)
  - High-rate absorption (MAC, PRF)

- **Keyed initialization/finalization**
  - Increases robustness (AEAD)

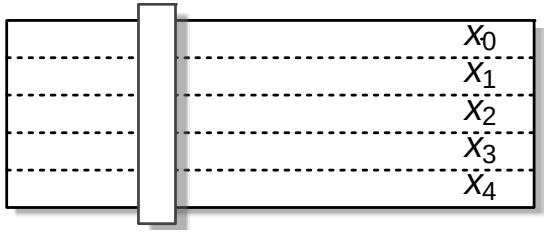
Main design goals

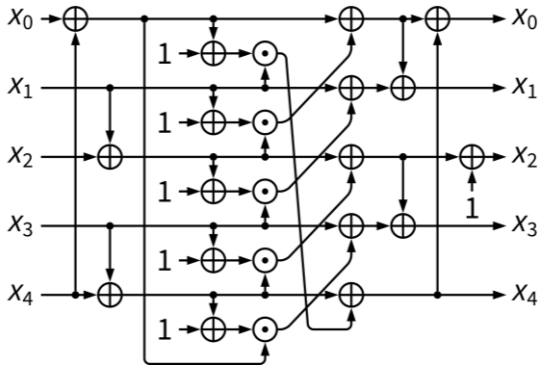
- Security
- Efficiency
- Simplicity
- Scalability
- Online
- Single pass
- Lightweight
- Robustness (SCA, misuse)

Ascon: Authenticated Encryption

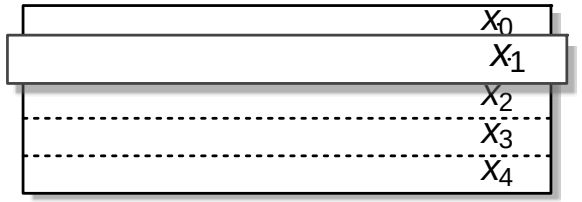
The permutation: 6/8/12 rounds

S-box layer





Linear layer

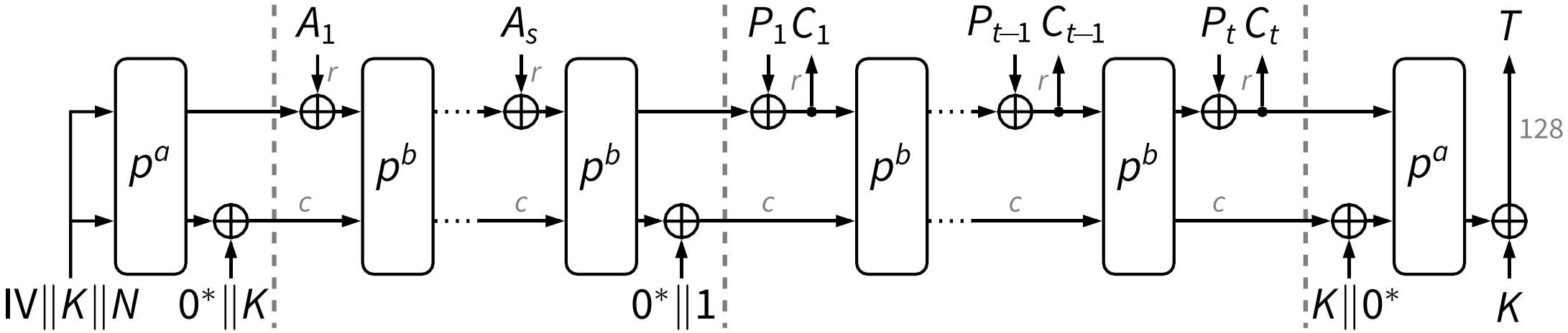


$$
\begin{aligned}
x_0 &= x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) \\
x_1 &= x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39) \\
x_2 &= x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) \\
x_3 &= x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) \\
x_4 &= x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)
\end{aligned}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

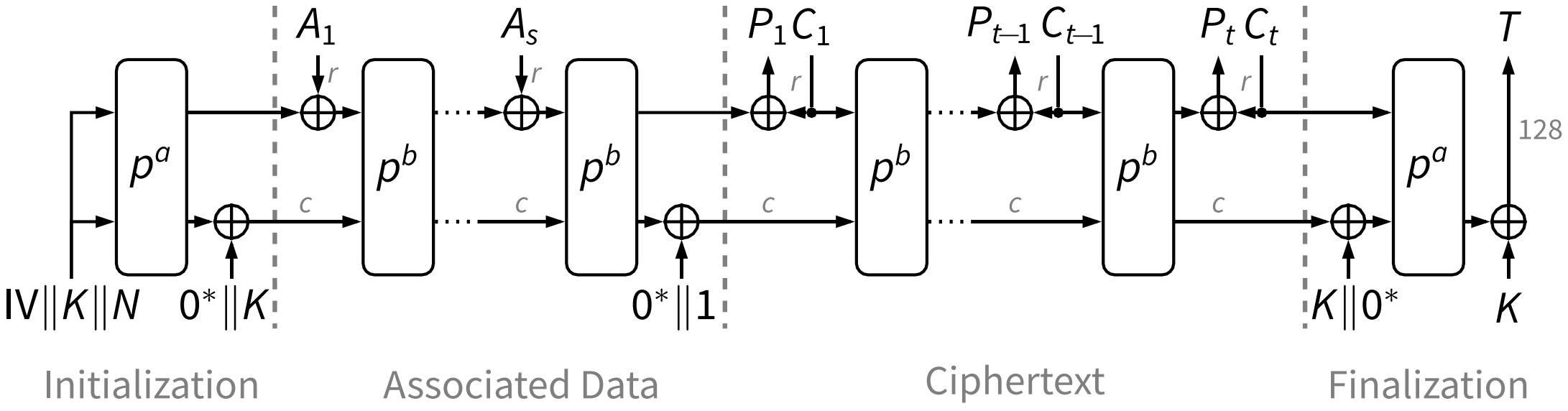
Properties of the permutation

- Simplicity
  - Small 320-bit state size
  - Defined on 5 64-bit words
  - Using bitwise Boolean functions
- Fast in Software
  - Up to 5 instructions in parallel
  - Bit-sliced S-box (64 in parallel)
  - Bit-interleaving on 32-bit processors
- Flexible in hardware
  - Small area to high speed
- Easy integration of side-channel countermeasures
  - No look-up tables
  - Low degree S-box
- High diffusion and proven bounds

Ascon AEAD: Encryption



Ascon AEAD: Decryption



AEAD instances

Nonce-based AEAD, duplex sponge-based with keyed initialization and finalization

	Ascon-128	Ascon-128a	Ascon-80pq
Security [bits]	128	128	128
Key k [bits]	128	128	160
Rate r [bits]	64	128	64
Capacity c [bits]	256	192	256
Rounds (a, b)	(12, 6)	(12, 8)	(12, 6)

Ascon-128 vs Ascon-128a

- Same security, different trade-off (block size vs. number of rounds)
- Both scrutinized for years in cryptographic competitions
- Most security analysis can be applied to both algorithms
- Tight security proof for Ascon (https://eprint.iacr.org/2023/775)

$$\frac{T}{2^{\min\{\kappa,c\}}} + \frac{D}{2^{\min\{\tau,c\}}} + \frac{TD}{2^b}$$

- Ascon-128a: 33% more performance, more rounds, larger rate
- Ascon-128: higher robustness in case of state recovery (https://eprint.iacr.org/2023/796)

→ We are in favor of standardizing both a fast and a more robust version

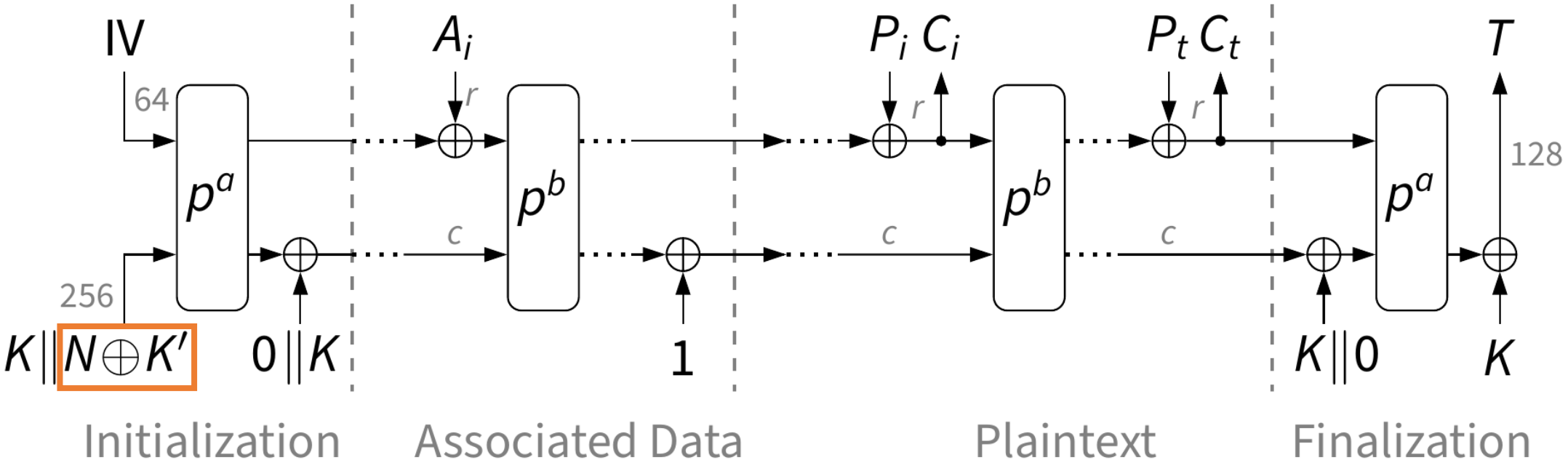
Larger nonce, shorter tags

- Support for shorter tags is useful
  - Recommend e.g., 64, 96 and 128 bits
- We would recommend to encode the size of the tag in the IV.
- In addition, we think that if shorter tags are supported, a strict limit on verification fails should be imposed by the application.
- Otherwise, for short tags, one ends up in attack scenarios resembling return of unverified plaintext which might be a problem for the application.

Larger nonce, shorter tags

- We do not see the immediate need to support larger nonce, considering the limit on messages that can be encrypted under a single key.
- In case someone would like to use a fixed prefix in the nonce, we suggest to put this prefix into the associated data instead.

Secret nonce, larger keys



Secret nonce, larger keys

- Also done in AES-GCM in TLS (RFC 8446)
- Increases key size to 256 bits, security level remains at 128 bits
- Improves multi-user security (https://eprint.iacr.org/2023/924)

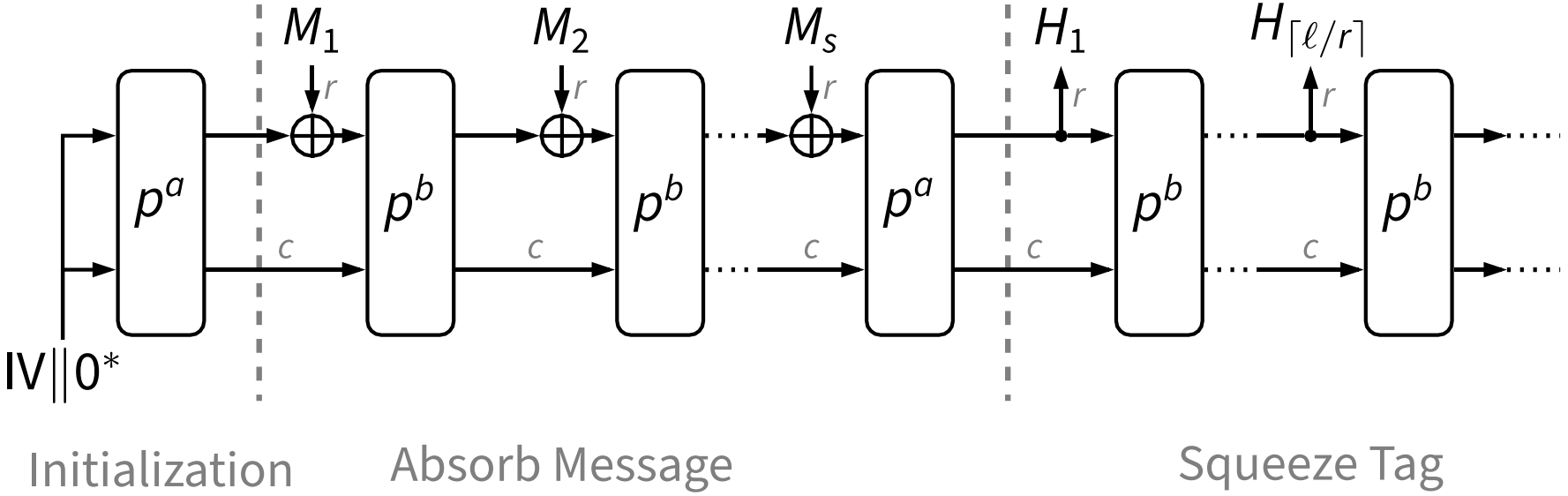
Ascon-80pq

- Instead of Ascon-80pq we prefer to add support for larger keys, secret nonce to increase multi-user security and also resistance against Grover's algorithm.
- By dropping Ascon-80pq we can extend the IV to 64 bits again which gives use some options for encoding additional information such as tag sizes etc.
- Reduce number of variants in the standard.

Ascon: Hashing and XOF

Ascon Hash / XOF

- Similar structure, same permutation(s) as AEAD



- Hash: Fixed output size (ℓ=256)
- Xof: Variable output size

Hash / XOF instances

- Uses the sponge construction, different number of rounds for init/final and absorb/squeeze

	Ascon-Hash/Xof	Ascon-Hasha/Xofa
Security [bits]	128	128
Rate r [bits]	64	64
Capacity c [bits]	256	256
Rounds (a, b)	(12, 12)	(12, 8)

→ We are in favor of standardizing XOF

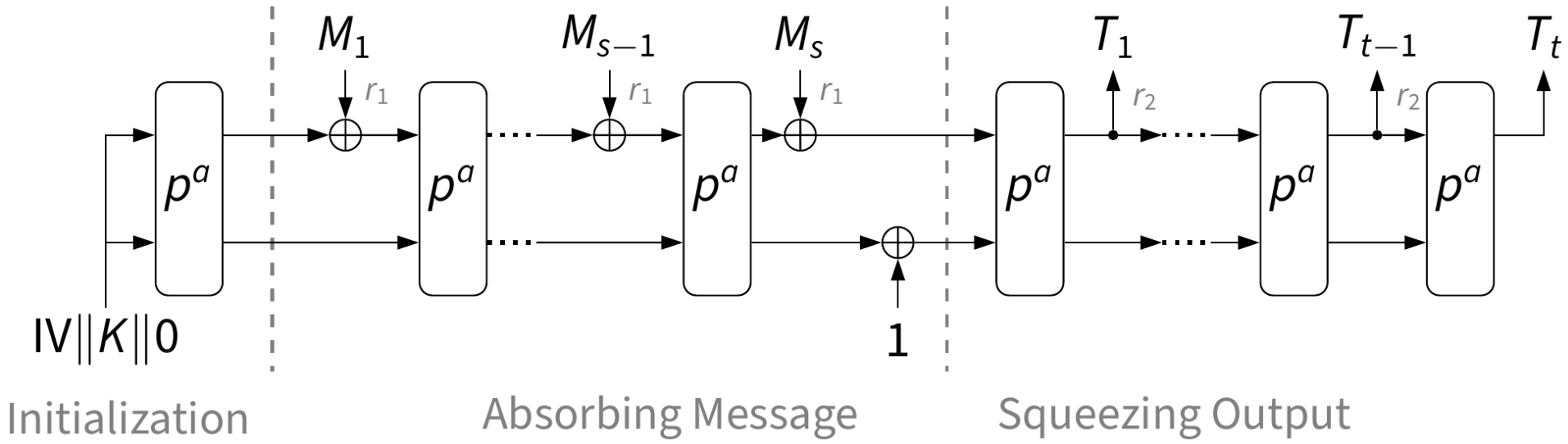
Ascon: PRF and MAC

Ascon PRF / MAC

- We see the requirement for having efficient PRFs that can be used as, e.g., MACs or stream ciphers from an industry point of view.
- Efficient constructions exists for Ascon with low implementation overhead (https://eprint.iacr.org/2021/1574)
- Alternative constructions based on HMAC or KMAC are not as efficient and not our preferred option.

Ascon PRF and MAC

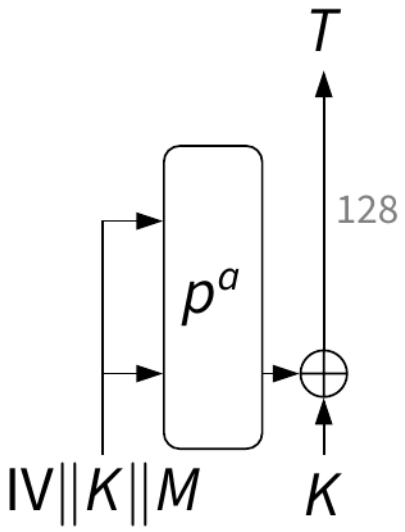
- Initialization with key, 12 rounds in p^a
- Absorb message with $r_1 = 256$ (4x more efficient than Ascon-KMAC)
- Squeeze tag with $r_2 = 128$



Ascon PRF-Short

- Initialization of Ascon-128 (with different IV)
- Nonce replaced by message (m ≤ 128 bits)
- Generates tag (t ≤ 128 bits)

- Applications:
  - Symmetric authentication (challenge-response)
  - Efficient key derivation
  - Pointer Authentication
  - …



Security

Analysis of AEAD

- Nonce respecting, within data limit 2^{64} and time limit 2^{128}

Type	Target	Rounds	Time	Method	Reference
Key recovery	Ascon initialization	7 / 12	2^{123}	Cube	[RHSS21]
	Ascon initialization	6 / 12	2^{40}	Cube-like	[LDW17]
	Ascon initialization	5 / 12	2^{31}	Diff.-linear	[Tez20]
Forgery	Ascon finalization	3 / 12	2^{20}	Differential	[GPT21]
State recovery	Ascon-128a iteration	3 / 8	2^{117}	Differential	[GPT21]
	Ascon-128a iteration	2 / 8	—	Sat-Solver	[DKM+17]

Analysis of AEAD (misuse settings)

- Generic nonce-misuse on duplex designs result in:
  - Confidentiality break with 1+1 misuse queries per block
  - State recovery with D misuse queries where $T \cdot D = 2^c$
- State recovery does not lead to trivial key recovery (in Ascon)
- Nonce-misuse attacks do not trivially break authenticity (in Ascon)
- Many interesting results published which analyze Ascon in misuse settings
  - Exceeding data limit of 2^{64}
  - Exceeding time limit of 2^{128}
  - Using (massive) nonce-misuse

Analysis of AEAD

- D. Chang, D. Hong, J. Kang. **Conditional Cube Attacks on Ascon-128 and Ascon-80pq in a Nonce-misuse Setting**. IACR Cryptology ePrint Archive 2022.
- D. Chang, J. Kang, M. S. Turan. **A New Conditional Cube Attack on Reduced-Round Ascon-128a in a Nonce-misuse Setting**. NIST LWC Workshop 2022.
- C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer. **Cryptanalysis of Ascon**. CT-RSA 2015.
- D. Gérault, T. Peyrin, Q. Q. Tan. **Exploring Differential-Based Distinguishers and Forgeries for Ascon**. IACR Transactions on Symmetric Cryptology 2021.
- K. Hu,T. Peyrin. **Revisiting Higher-Order Differential(-Linear) Attacks from an Algebraic Perspective: Applications to Ascon, Grain v1, Xoodoo, and ChaCha**. NIST LWC Workshop 2022.
- Z. Li, X. Dong, X. Wang**. Conditional Cube Attack on Round-Reduced Ascon**. IACR Transactions on Symmetric Cryptology 2017.

Analysis of AEAD

- Y. Li, G. Zhang, W. Wang, M. Wang. **Cryptanalysis of round-reduced Ascon**. SCIENCE CHINA Information Sciences 2017.
- R. Rohit, K. Hu, S. Sarkar, S. Sun. **Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon**. IACR Transactions of Symmetric Cryptology 2021.
- C. Tezcan. **Analysis of Ascon, DryGASCON, and Shamash Permutations**. Information Security Science 2020.

Analysis of Hash / XOF

Type	Target	Output	Rounds	Time	Method	Reference
Preimage	Ascon-Xof(a) final.	64	6 / 12	$2^{63.3}$	Algebraic	[DEMS19]
	Ascon-Xof(a) final.	256	3 / 12	$2^{114.5}$	MitM	[QZH+23]
	Ascon-Xof(a) final.	64	2 / 12	2^{39}	Cube-like	[DEMS19]
Collision	Ascon-Hash(a) final.	256	4 / 12	$2^{126.8}$	MitM	[QZH+23]
	Ascon-Xof(a) final.	64	2 / 12	2^{15}	Differential	[ZDW19]
	Ascon-Hash(a) iteration	256	2 / 12(8)	$2^{62.6}$	Differential	[YLW+23]

Analysis of Hash / XOF

- C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer. **Preliminary Analysis of Ascon-Xof and Ascon-Hash**. Technical Report. 2019.
- D. Gérault, T. Peyrin, Q. Q. Tan. **Exploring Differential-Based Distinguishers and Forgeries for Ascon**. IACR Transactions on Symmetric Cryptology 2021.
- R. Zong, X. Dong, X. Wang. **Collision Attacks on Round-Reduced Gimli-Hash/Ascon-Xof/Ascon-Hash**. IACR Cryptology ePrint Archive 2019.
- L. Qin, B. Zhao, J. Hua, X. Dong, X. Wang. **Weak-Diffusion Structure: Meet-in-the-Middle Attacks on Sponge-based Hashing Revisited**. IACR Cryptology ePrint Archive 2023.
- X. Yu, F. Liu, G. Wang, S. Sun, W. Meier. **A Closer Look at the S-box: Deeper Analysis of Round-Reduced ASCON-HASH.** IACR Cryptology ePrint Archive 2023.

Security properties of the permutation

- Ascon does not require ideal properties of the permutation
  - Non-random properties are known
  - Detailed overview of analysis in final NIST status update
- Properties of S-box:
  - Algebraic degree 2
  - Differential/linear branch number 3
  - Max. differential probability 2^{-2}, max. squared correlation 2^{-2}
- Properties of linear layer:
  - Differential/linear branch number 4
  - Efficient diffusion due to weak alignment

Analysis of the permutation

- C. Dobraunig, M. Eichlseder, F. Mendel. **Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates**. ASIACRYPT 2015.
- D. Gérault, T. Peyrin, Q. Q. Tan. **Exploring Differential-Based Distinguishers and Forgeries for Ascon**. IACR Transactions on Symmetric Cryptology 2021.
- K. Hu,T. Peyrin. **Revisiting Higher-Order Differential(-Linear) Attacks from an Algebraic Perspective: Applications to Ascon, Grain v1, Xoodoo, and ChaCha**. NIST LWC Workshop 2022.
- G. Leander, C. Tezcan, F. Wiemer. **Searching for Subspace Trails and Truncated Differentials**. IACR Transactions on Symmetric Cryptology 2018.
- R. Rohit, K. Hu, S. Sarkar, S. Sun. **Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon**. IACR Transactions of Symmetric Cryptology 2021.
- C. Tezcan. **Truncated, Impossible, and Improbable Differential Analysis of Ascon**. ICISSP 2016.
- Y. Todo. **Structural Evaluation by Generalized Integral Property**. EUROCRYPT 2015.

Bounds and characteristics

- C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer. **Cryptanalysis of Ascon**. CT-RSA 2015.
- C. Dobraunig, M. Eichlseder, F. Mendel. **Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates**. ASIACRYPT 2015.
- D. Gérault, T. Peyrin, Q. Q. Tan. **Exploring Differential-Based Distinguishers and Forgeries for Ascon**. IACR Transactions on Symmetric Cryptology 2021.
- R. H. Makarim, R. Rohit. **Towards Tight Differential Bounds of Ascon**. FSE 2022 Rump Session. 2022.
- J. Erlacher, F. Mendel, M. Eichlseder. **Bounds for the Security of Ascon against Differential and Linear Cryptanalysis**. IACR Transactions on Symmetric Cryptology 2022.
- S. El Hirch, S. Mella, A. Mehrdad, J. Daemen. **Improved Differential and Linear Trail Bounds for Ascon**. IACR Trans. Symmetric Cryptol. 2022.

Bounds and characteristics

- Best known characteristics and bounds for up to 6 rounds of the Ascon permutation (https://eprint.iacr.org/2022/1377)

Rounds	Differential		Linear	
1	2^{-2}	2^{-2}	2^{-2}	2^{-2}
2	2^{-8}	2^{-8}	2^{-8}	2^{-8}
3	2^{-40}	2^{-40}	2^{-28}	2^{-28}
4	2^{-107}	$\leq 2^{-86}$	2^{-98}	$\leq 2^{-88}$
5	2^{-190}	$\leq 2^{-100}$	2^{-186}	$\leq 2^{-96}$
6	-	$\leq 2^{-129}$	-	$\leq 2^{-132}$

Implementations

FPGA benchmarks

	Throughput	Area	Throughput / Area
ASCON-128a	6297.6	2410	2.61
ASCON-128	3744.0	2126	1.76
AES128-GCM	2700.8	3270	0.83

Xilinx Artix-7

	Throughput	Area	Throughput / Area
ASCON-128a	3031.0	4552	0.67
ASCON-128	2157.0	3215	0.67
AES128-GCM	1548.3	8754	0.18

Intel Cyclone 10 LP

	Throughput	Area	Throughput / Area
ASCON-128a	2158.1	5909	0.37
ASCON-128	1427.5	3764	0.38
AES128-GCM	1384.4	6740	0.21

Lattice ECP5

https://eprint.iacr.org/2020/1207

Your costs and results may vary.

ASIC benchmarks

	Throughput	Area	Throughput / Area
Ascon-128a	25.60	1.49	17.18
Ascon-128	16.00	1.56	10.25
AES128-GCM	11.63	2.75	4.22

https://eprint.iacr.org/2021/049

Your costs and results may vary.

Embedded SW implementations

Time to process NIST testvectors in [µs] on embedded devices

	Uno	F1	ESP	F7	R5
Ascon-128a	1981	66.4	18.4	11.8	7.3
Ascon-128	2337	76.7	22.3	13.8	8.5
AES128-GCM	-	332.8	67.2	35.8	23.7

https://lwc.las3.de/

Code size in [bytes] on embedded devices

	Uno	F1	ESP	F7	R5
Ascon-128a	2544	2252	1200	1240	1792
Ascon-128	2552	2157	1120	1180	1792
AES128-GCM	-	9908	14832	9836	14272

https://lwc.las3.de/

Your costs and results may vary.

High-end SW performance

	AMD Ryzen 9	ARM Cortex-A72
Ascon-128a	5.6	7.0
Ascon-128	8.1	10.5
AES128-GCM	1.1*	30.6

*with AES-NI

https://bench.cr.yp.to/

Your costs and results may vary.

Ascon hardware extensions/instructions

- A Fast and Compact RISC-V Accelerator (for RV32, also ARM)
  - RI5CY Ascon with **4.7kGE**: speedup factor **50x**
  - Reuse 10 registers of CPU register file
  - https://eprint.iacr.org/2020/1083.pdf

- ARM Custom Datapath Extension, RISC-V Bitmanip Extension, ...
  - 32-bit funnel shift instructions (RV32B: FSRI, ESP32: SRC)
  - 32-bit interleaving instructions (RV32B: ZIP/UNZIP, ARM CDE: CX3)
  - Fused AND/XOR, BIC/XOR instructions (ARM A64: BCAX, ARM CDE: CX3A)
  - SHA-2 like Sigma instructions (ARM CDE: CX3DA)

Your costs and results may vary.

Implementation summary

- Often much more efficient than AES128-GCM
  - Up to **3x to 5x speed** on microcontrollers (https://lwc.las3.de/)
  - Up to **2x throughput** with **0.5x energy** in hardware (https://eprint.iacr.org/2021/049)

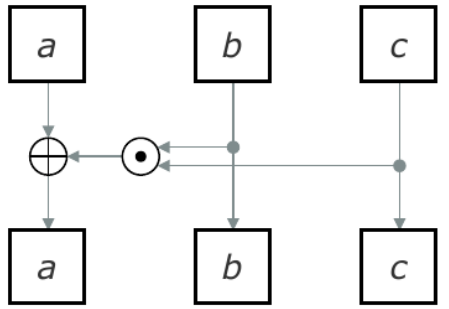
- Designed to ease protection against physical attacks

Your costs and results may vary.

Side-channel protected implementations

Ascon: Designed with SCA in mind

- Algebraic degree 2 of S-box (more efficient masking)
- Masking using invertible Toffoli gate
  - Fewer (no) fresh randomness needed
  - Better protection against SIFA attacks
- Limited damage if state is recovered
- Leveled implementations
  - Higher protection order for Init/Final (key)
  - Lower protection order for AD/PT/CT processing (data)



Masked hardware implementations

- Masked DOM implementations of Ascon-128 (CHES2017)

Protection Order	[kGE]	[Mbps]	[kGE]	[Mbps]
1	10.86	108	28.89	2246
2	16.19	108	53.00	1896
3	21.59	110	81.21	1903
…	…	…	…	…

- Additional first and second-order masked hardware implementations:
  - Implementation: https://github.com/ascon/ascon-hardware-sca
  - Evaluation: https://cryptography.gmu.edu/athena/index.php?id=LWC

Your costs and results may vary.

Masked software implementations

- Masked Toffoli/leveled implementations of Ascon-128

impl./shares flags	armv6	C -O2	C -Os	2 -O2	2 -Os	3 -O2	3 -Os
ARM1176JZF	58	70	85	260	343	524	703
STM32F415	59	84	90	320	378	650	669

Performance in cycles/byte (green: evaluated)

- First and second-order masked software implementations:
  - Implementation: https://github.com/ascon/ascon-c
  - Evaluations: https://cryptography.gmu.edu/athena/index.php?id=LWC
    https://github.com/ascon/simpleserial-ascon

Your costs and results may vary.

Summary

- **Security**
  - Well analyzed/understood
  - High number of external analysis
  - Large security margin
- **Efficiency**
  - Efficient on constraint devices in HW and SW
  - Easier side-channel protection
  - Fast on modern CPUs
- **Flexibility**
  - Additional constructions like XOF, MAC, PRF, …

Thank you!