ASCON: A Submission to CAESAR

Ch. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer
Graz University of Technology

CECC 2015

The Team

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

Overview

- CAESAR
- Design of ASCON
- Security analysis
- Implementations

CAESAR

- CAESAR: Competition for Authenticated Encryption – Security, Applicability, and Robustness
  - http://competitions.cr.yp.to/caesar.html
- Inspired by
  - AES
  - SHA-3
  - eStream

CAESAR – Candidates

ACORN	++AE	AEGIS	AES-CMCC
AES-COBRA	AES-COPA	AES-CPFB	AES-JAMBU
AES-OTR	AEZ	Artemia	Ascon
AVALANCHE	Calico	CBA	CBEAM
CLOC	Deoxys	ELmD	Enchilada
FASER	HKC	HS1-SIV	ICEPOLE
iFeed[AES]	Joltik	Julius	Ketje
Keyak	KIASU	LAC	Marble
McMambo	Minalpher	MORUS	NORX
OCB	OMD	PAEQ	PAES
PANDA	π-Cipher	POET	POLAWIS
PRIMATEs	Prøst	Raviyoyla	Sablier
SCREAM	SHELL	SILC	Silver
STRIBOB	Tiaoxin	TriviA-ck	Wheesht
YAES			

CAESAR – Candidates

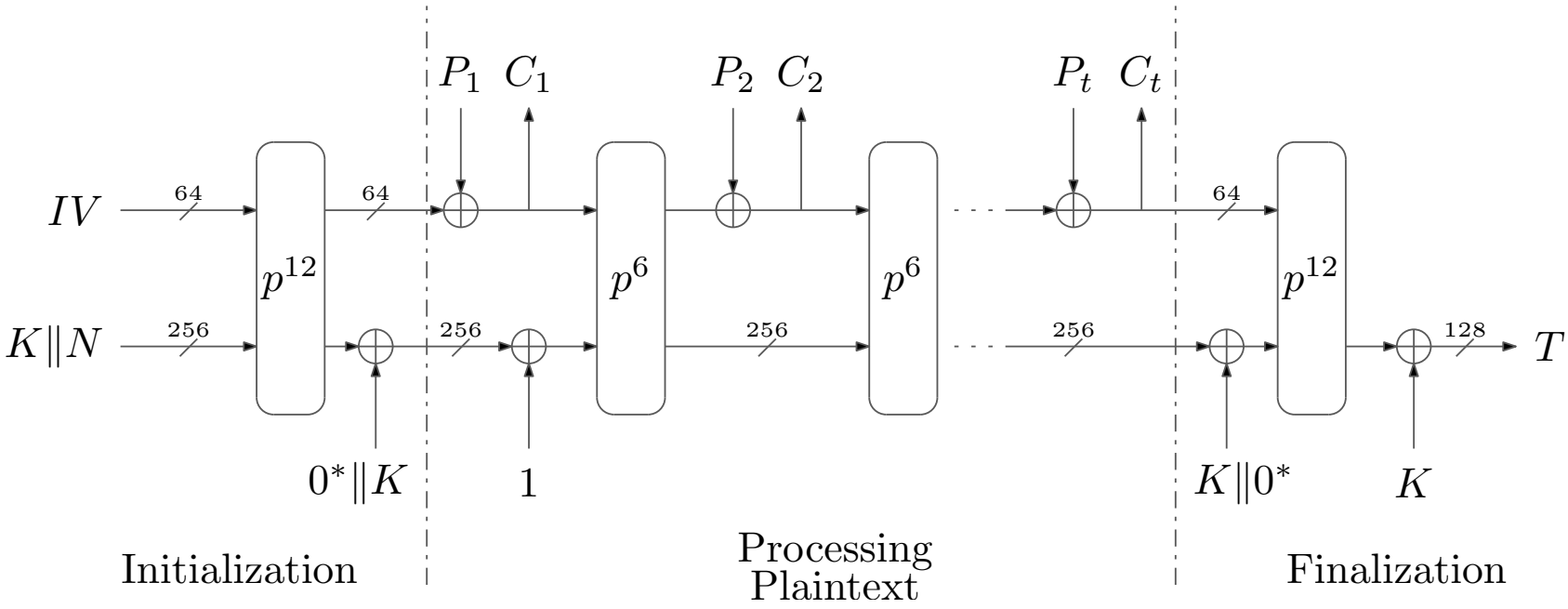
ACORN	~~++AE~~	AEGIS	~~AES-GMGC~~
~~AES-COBRA~~	AES-COPA	~~AES-CPFB~~	AES-JAMBU
AES-OTR	AEZ	~~Artemia~~	Ascon
~~AVALANCHE~~	~~Calico~~	~~CBA~~	~~CBEAM~~
CLOC	Deoxys	ELmD	~~Enchilada~~
~~FASER~~	~~HKC~~	HS1-SIV	ICEPOLE
~~iFeed[AES]~~	Joltik	~~Julius~~	Ketje
Keyak	~~KIASU~~	~~LAC~~	~~Marble~~
~~McMambo~~	Minalpher	MORUS	NORX
OCB	OMD	PAEQ	~~PAES~~
~~PANDA~~	π-Cipher	POET	~~POLAWIS~~
PRIMATEs	~~Prøst~~	~~Raviyoyla~~	~~Sablier~~
SCREAM	SHELL	SILC	~~Silver~~
STRIBOB	Tiaoxin	TriviA-ck	~~Wheesht~~
~~YAES~~			

ASCON – Design Goals

- Security
- Efficiency
- Lightweight
- Simplicity
- Online
- Single pass
- Scalability
- Side-Channel Robustness

ASCON – General Overview

- Nonce-based AE scheme
- Sponge inspired

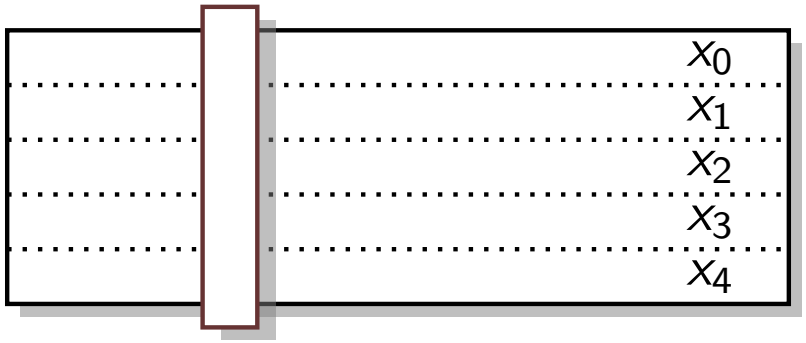


ASCON – Permutation

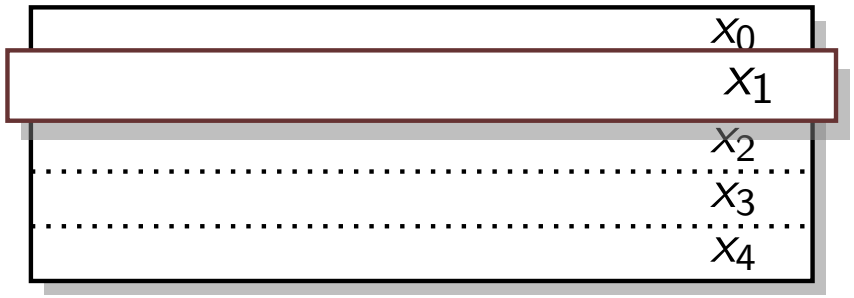
- Iterative application of round function
- One round
  - Constant addition
  - Substitution layer
  - Linear layer

ASCON – Round

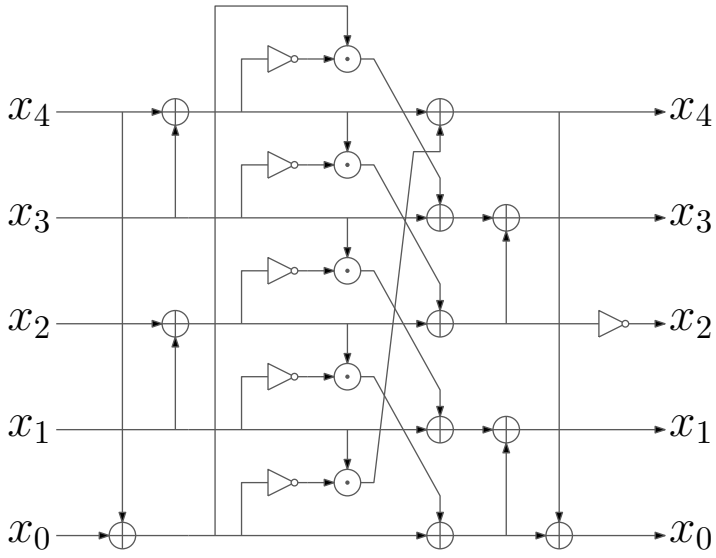
- Substitution layer



- Linear layer



ASCON – Round



S-box

$$x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41) \rightarrow x_4$$

$$x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) \rightarrow x_3$$

$$x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) \rightarrow x_2$$

$$x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39) \rightarrow x_1$$

$$x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) \rightarrow x_0$$

Linear transformation

Analysis – ASCON [DEMS15]

- Attacks on round-reduced versions of ASCON-128
  - Key-recovery
  - Forgery
- Analysis of the building blocks
  - Permutation

Key-recovery – Idea

- Target initialization
- Choose nonce
- Observe key-stream
- Deduce information about the secret key

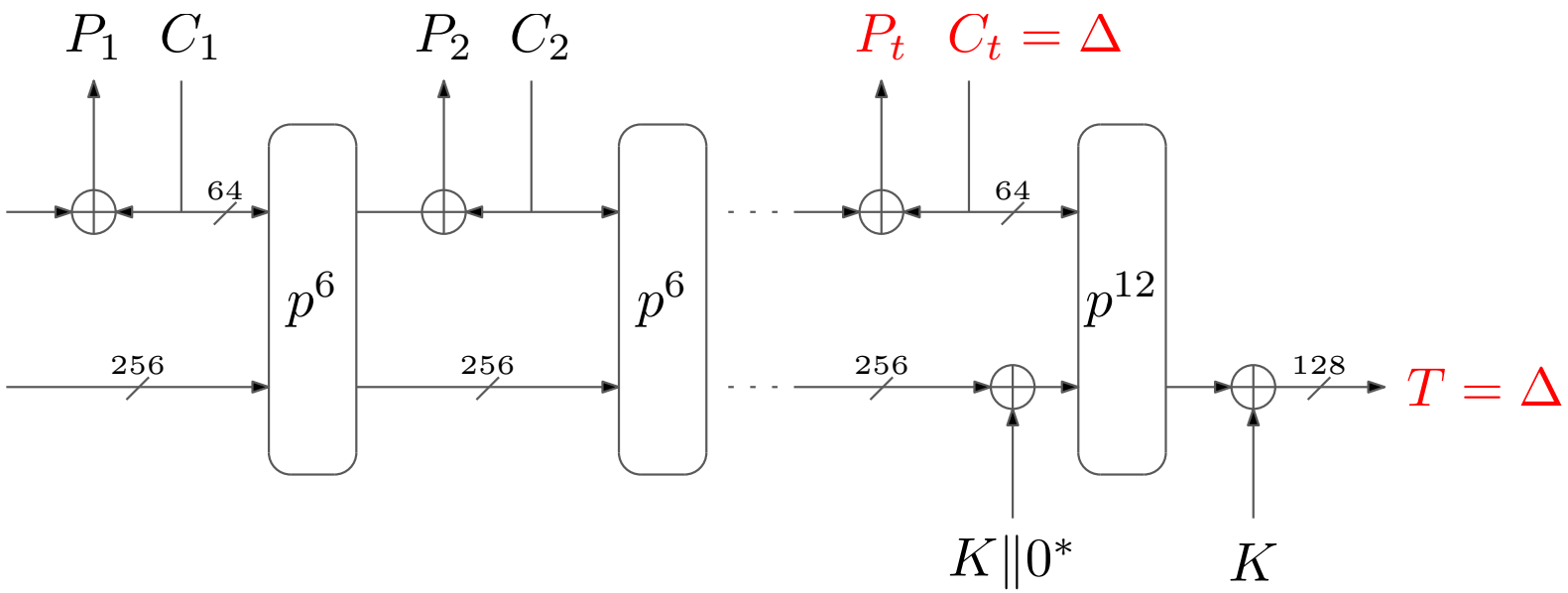
	rounds	time	method
ASCON-128	6 / 12	2^{66}	cube-like
	5 / 12	2^{35}	
	5 / 12	2^{36}	differential-linear
	4 / 12	2^{18}	

Key-recovery – Idea

- Target initialization
- Choose nonce
- Observe key-stream
- Deduce information about the secret key

	rounds	time	method
ASCON-128	6 / 12	2^{66}	cube-like
	5 / 12	2^{35}	
	5 / 12	2^{36}	differential-linear
	4 / 12	2^{18}	

Forgery – Idea



Forgery – ASCON-128

- 3/12 rounds finalization probability 2^{-33}

	input difference		after 1 round		after 2 rounds		after 3 rounds
x_0	8000000000000000		8000100800000000		8000000002000080		????????????????
x_1	0000000000000000		8000000001000004		9002904800000000		????????????????
x_2	0000000000000000	$\rightarrow$	0000000000000000	$\rightarrow$	d200000001840006	$\rightarrow$	????????????????
x_3	0000000000000000		0000000000000000		0102000001004084		4291316c5aa02140
x_4	0000000000000000		0000000000000000		0000000000000000		090280200302c084

- 4/12 rounds finalization probability 2^{-101}

	input difference		after 4 rounds
x_0	8000000000000000		????????????????
x_1	0000000000000000		????????????????
x_2	0000000000000000	$\rightarrow$	????????????????
x_3	0000000000000000		280380ec6a0e9024
x_4	0000000000000000		eb2541b2a0e438b0

Analysis – Permutation

- Zero-sum distinguisher 12 rounds with complexity 2^{130}
- Search for differential and linear characteristics
- Proof on minimum number of active S-boxes

result	rounds	differential	linear
proof	1	1	1
	2	4	4
	3	15	13
heuristic	4	44	43
	≥ 5	> 64	> 64

Implementation – ASCON

- Software
  - 64-bit Intel platforms
  - ARM NEON
  - 8-bit ATmega128
- Hardware [GWDE15]
  - High-speed
  - Low-area
  - Threshold implementations

Software – 64-bit Intel

- One message per core (Core2Duo)

	64	512	1024	4096
ASCON-128 (c/B)	22.0	15.9	15.6	15.2
ASCON-96 (c/B)	17.7	11.0	10.5	10.3

Software – 64-bit Intel

- One message per core (Core2Duo)

	64	512	1024	4096
ASCON-128 (c/B)	22.0	15.9	15.6	15.2
ASCON-96 (c/B)	17.7	11.0	10.5	10.3

- Four messages per core [Sen15] (Haswell)

	64	512	1024	4096
ASCON-128 (c/B)	10.49	7.33	7.11	6.94
ASCON-96 (c/B)	8.55	5.26	5.02	4.85

Hardware – Results [GWDE15]

	Chip Area [kGE]	Throughput [Mbps]	Power [µW]	Energy [µJ/byte]
Unprotected Implementations				
Fast 1 round	7.08	5 524	43	33
Fast 6 rounds	24.93	13 218	184	23
Low-area	2.57	14	15	5 706

Hardware – Results [GWDE15]

	Chip Area [kGE]	Throughput [Mbps]	Power [µW]	Energy [µJ/byte]
Unprotected Implementations				
Fast 1 round	7.08	5 524	43	33
Fast 6 rounds	24.93	13 218	184	23
Low-area	2.57	14	15	5 706

Hardware – Results [GWDE15]

	Chip Area [kGE]	Throughput [Mbps]	Power [µW]	Energy [µJ/byte]
Unprotected Implementations				
Fast 1 round	7.08	5 524	43	33
Fast 6 rounds	24.93	13 218	184	23
Low-area	2.57	14	15	5 706
Threshold Implementations				
Fast 1 round	28.61	3 774	183	137
Fast 6 rounds	123.52	9 018	830	104
Low-area	7.97	15	45	17 234

ASCON-128 – Choice of Parameters

- Now: (c,r) = (256, 64)
  - Conservative choice
- Proposed: (c,r) = (192, 128) [BDPA11]
  - Significant speedup (factor 2)
  - Limit on data complexity 2^{64}
- Proposed: (c,r) = (128, 192) [JLM14]
  - Significant speedup (factor 3)
  - More analysis needed

More Information

http://ascon.iaik.tugraz.at

Acknowledgments

The work has been supported in part by the Austrian Science Fund (project P26494-N15) and by the Austrian Research Promotion Agency (FFG) and the Styrian Business Promotion Agency (SFG) under grant number 836628 (SeCoS).

Reference I

[BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Duplexing the sponge: Single-pass authenticated encryption and other applications.
In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography – SAC 2011*, volume 7118 of *LNCS*, pages 320–337. Springer, 2011.

[CAE14] CAESAR committee.
CAESAR: Competition for authenticated encryption: Security, applicability, and robustness.
`http://competitions.cr.yp.to/caesar.html`, 2014.

[DEMS14] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Ascon.
Submission to the CAESAR competition: `http://ascon.iaik.tugraz.at`, 2014.

[DEMS15] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Cryptanalysis of ascon.
In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015*, volume 9048 of *LNCS*, pages 371–387. Springer, 2015.

Reference II

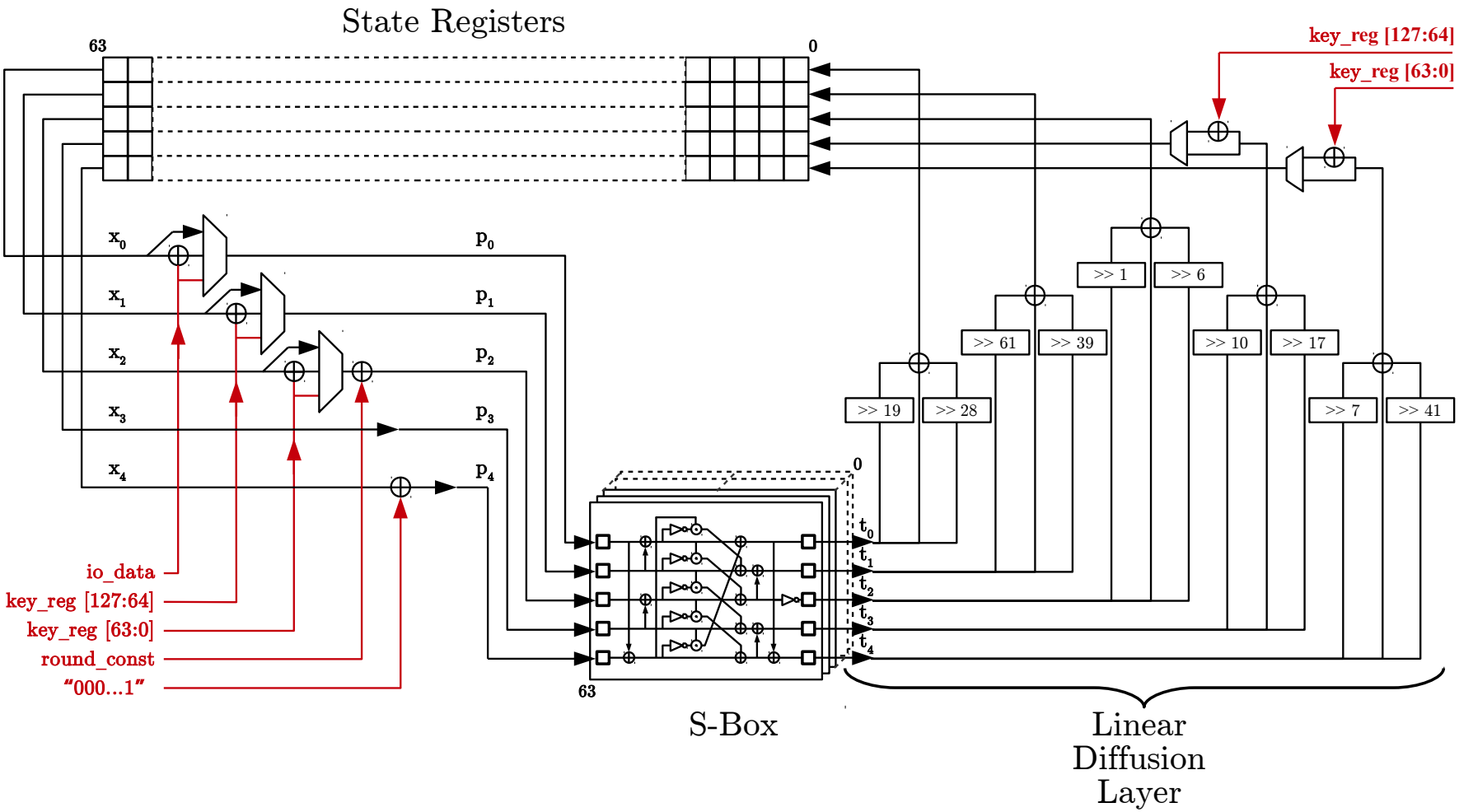
[DMP+15] Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michal Straus.
Cube attacks and cube-attack-like cryptanalysis on the round-reduced keccak sponge function.
In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 733–761. Springer, 2015.

[GWDE15] Hannes Groß, Erich Wenger, Christoph Dobraunig, and Christoph Ehrenhöfer.
Suit up! made-to-measure hardware implementations of ascon.
IACR Cryptology ePrint Archive, 2015:34, 2015.
to appear on 18th Euromicro Conference on Digital Systems Design.

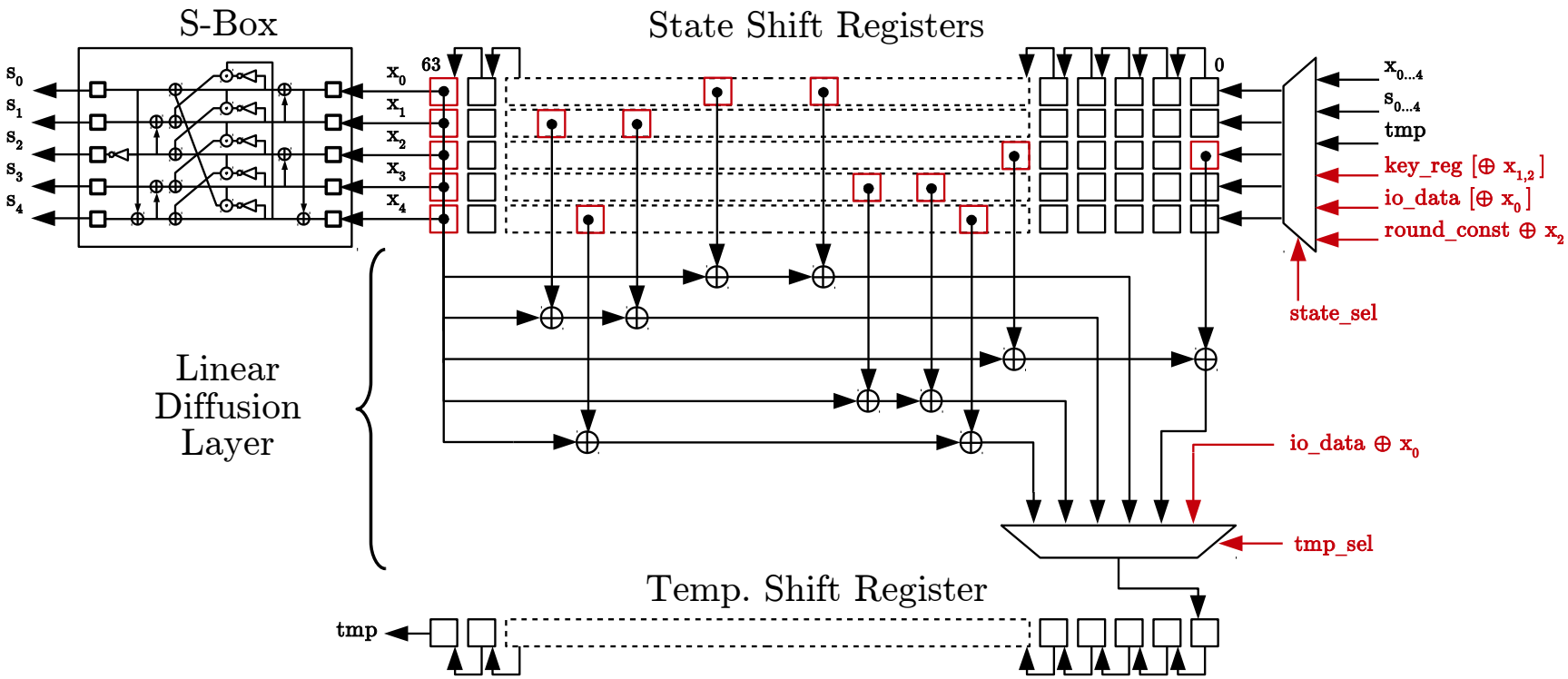
[JLM14] Philipp Jovanovic, Atul Luykx, and Bart Mennink.
Beyond $2^{c/2}$ security in sponge-based authenticated encryption modes.
In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 85–104. Springer, 2014.

[Sen15] Thomas Senfter.
Multi-message support for ascon.
Bachelors's Thesis, 2015.

Hardware – High-speed [GWDE15]



Hardware – Low-area [GWDE15]



Hardware – Comparison [GWDE15]