Ascon

(A Submission to CAESAR)

Ch. Dobraunig[1], M. Eichlseder[1], F. Mendel[1], M. Schläffer[2]

[1]IAIK, Graz University of Technology, Austria
[2]Infineon Technologies AG, Austria

22nd Crypto Day, Infineon, Munich

Overview

- CAESAR
- Design of ASCON
- Security analysis
- Implementations

CAESAR

- CAESAR: Competition for Authenticated Encryption – Security, Applicability, and Robustness (2014–2018)
  - http://competitions.cr.yp.to/caesar.html
  - Inspired by AES, eStream, SHA-3
- Authenticated Encryption
  - Confidentiality as provided by block cipher modes
  - Authenticity, Integrity as provided by MACs

"it is very easy to accidentally combine secure encryption schemes with secure MACs and still get insecure authenticated encryption schemes"

– Kohno, Whiting, and Viega

CAESAR

- CAESAR: Competition for Authenticated Encryption – Security, Applicability, and Robustness (2014–2018)
  - http://competitions.cr.yp.to/caesar.html
  - Inspired by AES, eStream, SHA-3
- Authenticated Encryption
  - Confidentiality as provided by block cipher modes
  - Authenticity, Integrity as provided by MACs

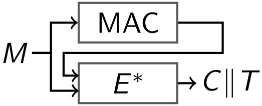
"it is very easy to accidentally combine secure encryption schemes with secure MACs and still get insecure authenticated encryption schemes"

– Kohno, Whiting, and Viega

Generic compositions

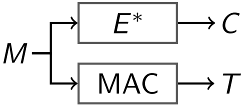
MAC-then-Encrypt (MtE)

- e.g. in SSL/TLS
- security depends on E and MAC



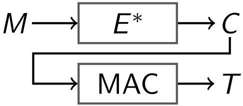
Encrypt-and-MAC (E&M)

- e.g. in SSH
- security depends on E and MAC



Encrypt-then-MAC (EtM)

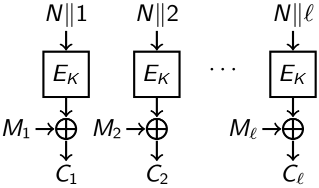
- IPSec, ISO/IEC 19772:2009
- provably secure



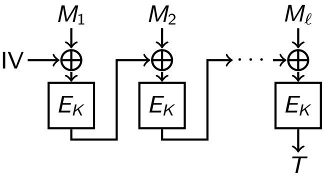
Pitfalls: Dependent Keys (Confidentiality)

Encrypt-and-MAC with CBC-MAC and CTR

CTR



CBC-MAC

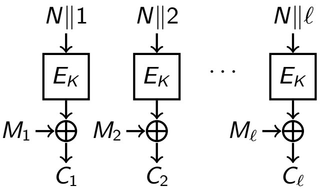


What can an attacker do?

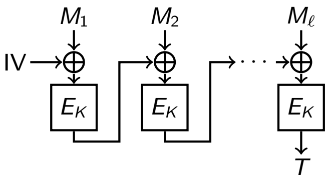
Pitfalls: Dependent Keys (Confidentiality)

Encrypt-and-MAC with CBC-MAC and CTR

CTR



CBC-MAC



What can an attacker do?

Tags for $M = IV \oplus (N\|1)$, $M = IV \oplus (N\|2)$, ...
are the key stream to read M_1, M_2, ...

(Keys for) E^* and MAC must be independent!

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

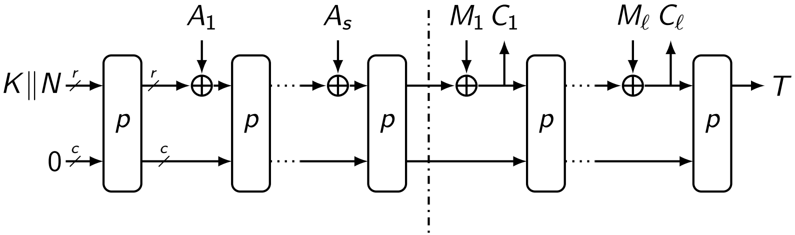
ACORN	~~++AE~~	AEGIS	~~AES-CMCC~~
~~AES-COBRA~~	AES-COPA	~~AES-CPFB~~	AES-JAMBU
AES-OTR	AEZ	~~Artemia~~	Ascon
~~AVALANCHE~~	~~Calico~~	~~CBA~~	~~CBEAM~~
CLOC	Deoxys	ELmD	~~Enchilada~~
~~FASER~~	~~HKC~~	HS1-SIV	ICEPOLE
~~iFeed[AES]~~	Joltik	~~Julius~~	Ketje
Keyak	~~KIASU~~	~~LAC~~	~~Marble~~
~~McMambo~~	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~~			

ASCON – Design Goals

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

Duplex sponge constructions

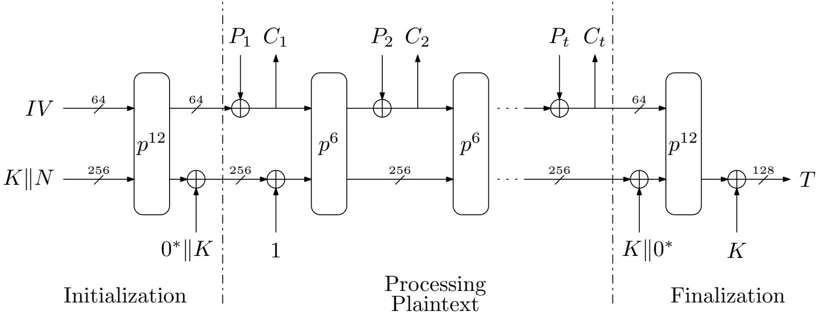
- Sponges became popular with SHA-3 winner Keccak
- Can be transformed to AE mode: duplex sponges
- Based on permutation p instead of block cipher E_K
- Security parameter: capacity c



ASCON – General Overview

- Nonce-based AEAD scheme
- Sponge inspired

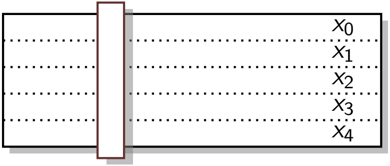
  ASCON-128: $(c, r) = (256, 64)$
  ASCON-96: $(c, r) = (192, 128)$



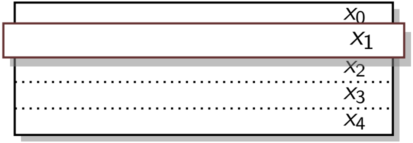
ASCON – Permutation

320-bit permutation, several rounds of:

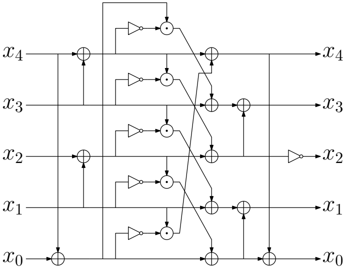
- Constant addition
- S-Box layer



- Linear transformation



Ascon – Round



S-box

$$x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41) \to x_4$$
$$x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) \to x_3$$
$$x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) \to x_2$$
$$x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39) \to x_1$$
$$x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) \to x_0$$

Linear transformation

Analysis – Permutation

- Branch number 3 for S-box and linear transformation
- Proof on minimum number of active S-boxes
- Search for differential and linear characteristics

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

Analysis – Ascon [DEMS15]

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

	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}	

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

- 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

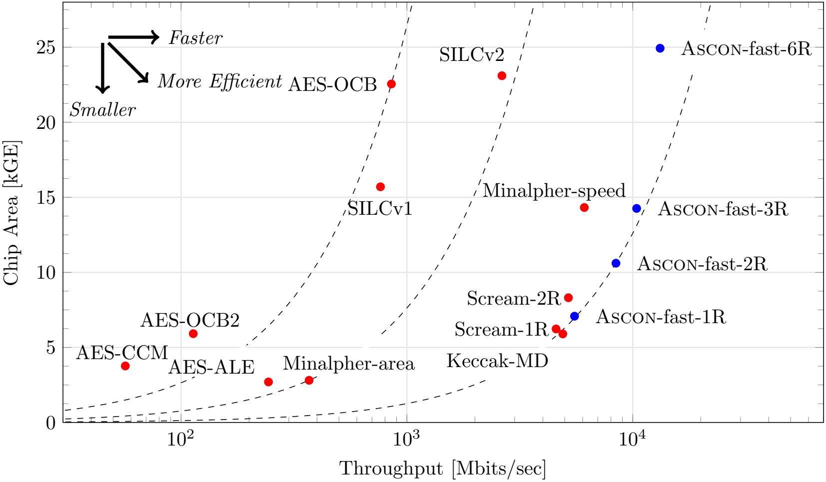
Hardware – Results [GWDE15]

	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
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

Hardware – Comparison [GWDE15]



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

Reference I

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.

CAESAR committee.

CAESAR: Competition for authenticated encryption: Security, applicability, and robustness.

`http://competitions.cr.yp.to/caesar.html`, 2014.

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.

Ascon.

Submission to the CAESAR competition: `http://ascon.iaik.tugraz.at`, 2014.

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.

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.

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.

Reference II

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.

Thomas Senfter.

Multi-message support for ascon.

Bachelors's Thesis, 2015.