Multi-Purpose Keccak for Modern FPGAs

Panasayya Yalla Ekawat Homsirikamol **Jens-Peter Kaps**

Cryptographic Engineering Research Group (CERG)
http://cryptography.gmu.edu
Department of ECE, Volgenau School of Engineering,
George Mason University, Fairfax, VA, USA

Cryptographic Architectures Embedded in Reconfigurable Devices – CryptArchi 2014

Outline

Cryptographic Services

Security protocols typically provide the following cryptographic services:

- Integrity
- Authenticity
- Confidentiality
- Non Repudiation
- Key Exchange/Agreement
- Pseudo Random Numbers

Services provided through secret key functions

With the exception of Non Repudiation and Key Exchange all other services are provided by secret key functions.

Providing Cryptographic Services

Secret key based cryptographic services can be provided by cryptographic functions.

- Integrity → Hash
- Authenticity, Integrity → Message Authentication Code (MAC)
- Confidentiality, Authenticity, Integrity → Authenticated Encryption with Associated Data (AEAD)
- Pseudo Random Numbers → Pseudo Random Number Generator (PRNG)

Providing cryptographic functions through a single algorithm

- Using modes of operation
- More area efficient than using dedicated algorithms

Cryptographic Algorithms

Advanced Encryption Standard

- Standard based on Rijndael
- Traditional block cipher
- 128-bit block size
- 128/192/256-bit key size

Cryptographic Algorithms

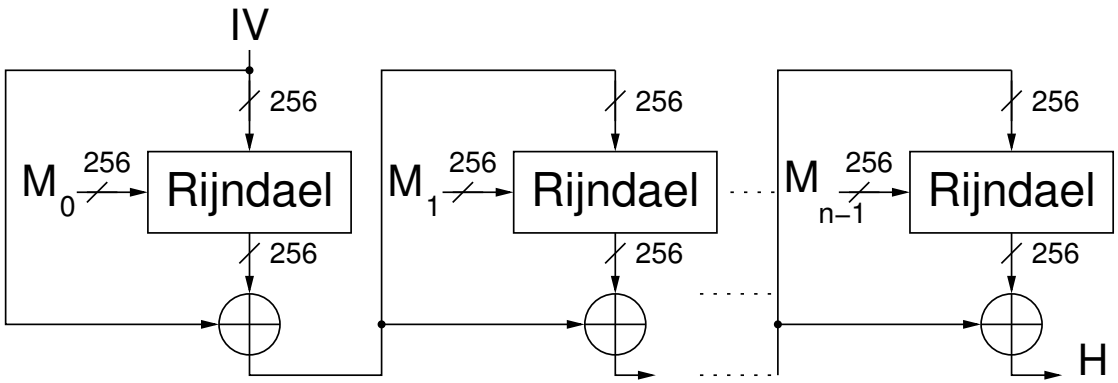
Advanced Encryption Standard

- Standard based on Rijndael
- Traditional block cipher
- 128-bit block size
- 128/192/256-bit key size

Keccak f-permutation

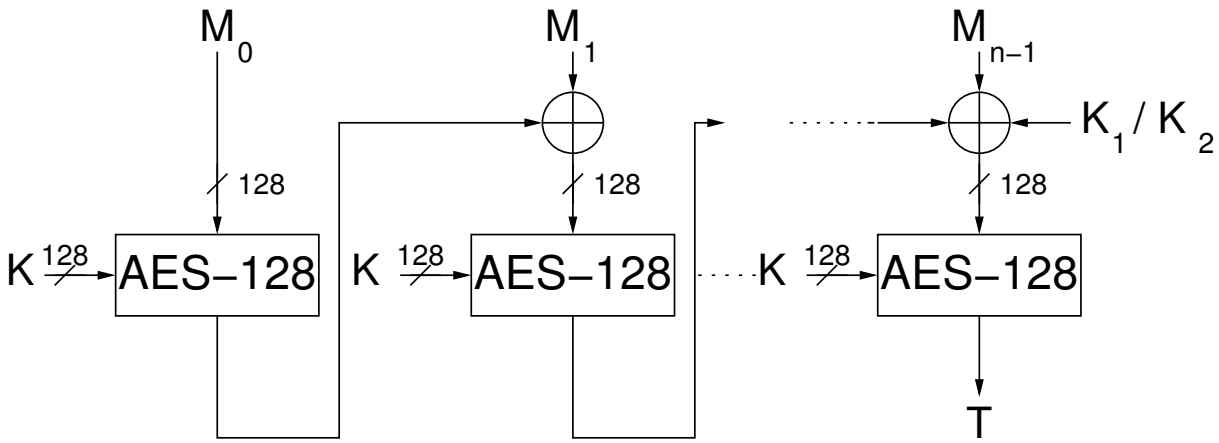
- It is the basis of Keccak, the Winner of competition for next Secure Hash Algorithm (SHA-3).
- 1600-bit state size
- Keccak is based on Sponge construction.

AES Hash: AES-Hash



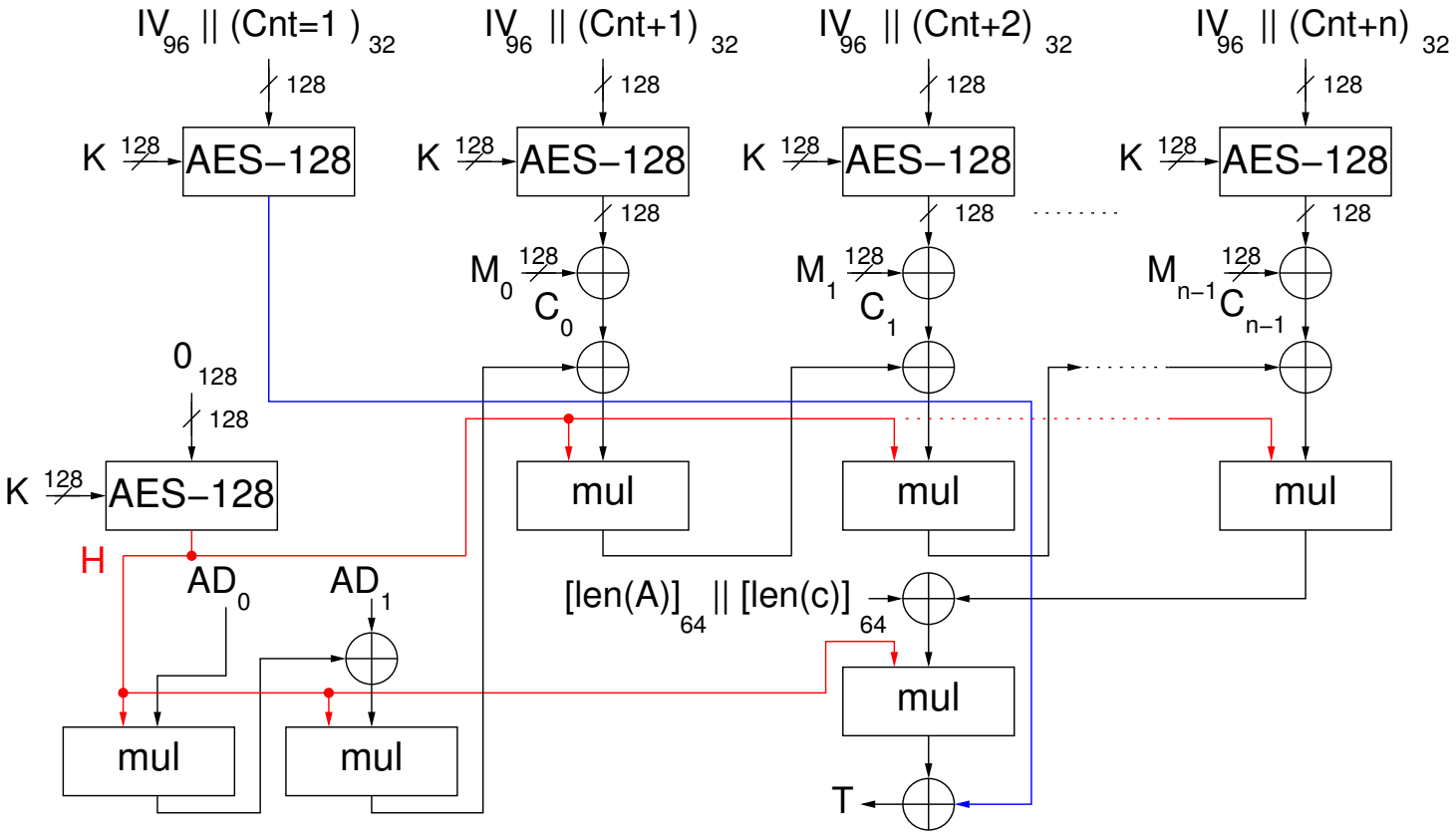
- Based on Davies-Meyer.
- The message enters on the input for the key.
- Uses a block size of 256-bit → Rijndael.
- Not a NIST standardized mode.

AES MAC: CMAC



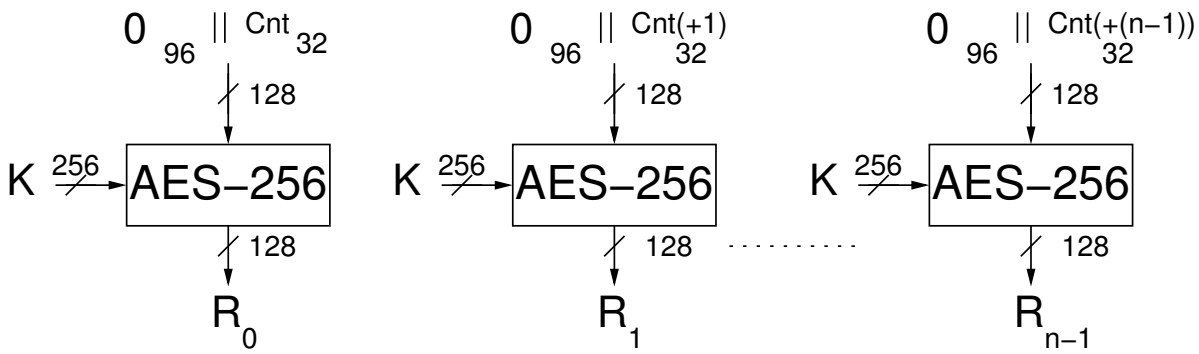
- Recommended mode of operation by NIST.
- Equivalent to One-Key CBC-MAC (OMAC1).
- K_1 and K_2 are derived from K through single bit shifts and XORed with constant.

AES AEAD: Galois Counter Mode



- Recommended mode of operation by NIST.

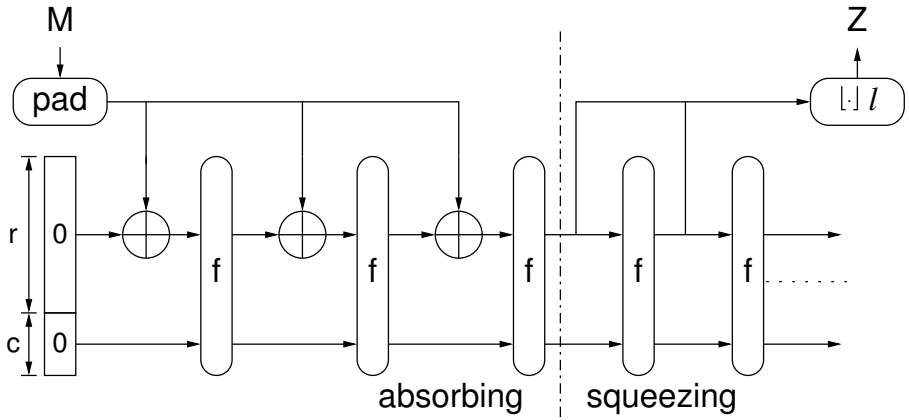
AES PRNG: Fortuna



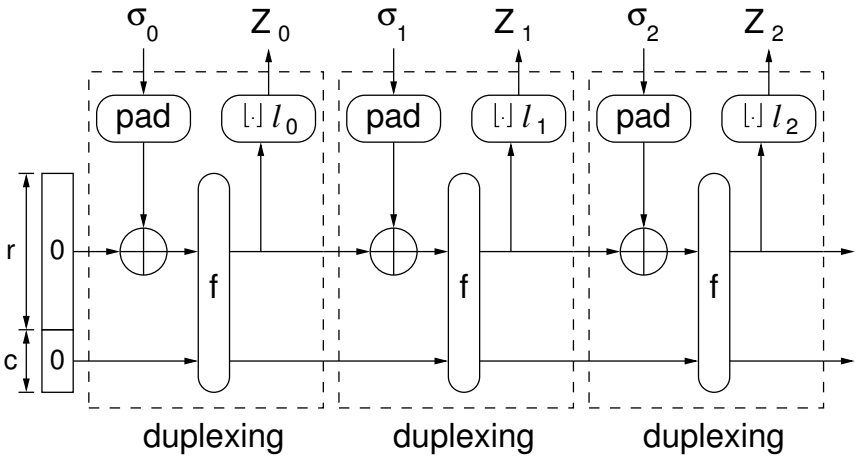
- Cryptographically secure PRNG
- Not a NIST standardized mode.
- Used in Windows 2000 and Windows XP
- The seed is processed as key.

Keccak Modes of Operation

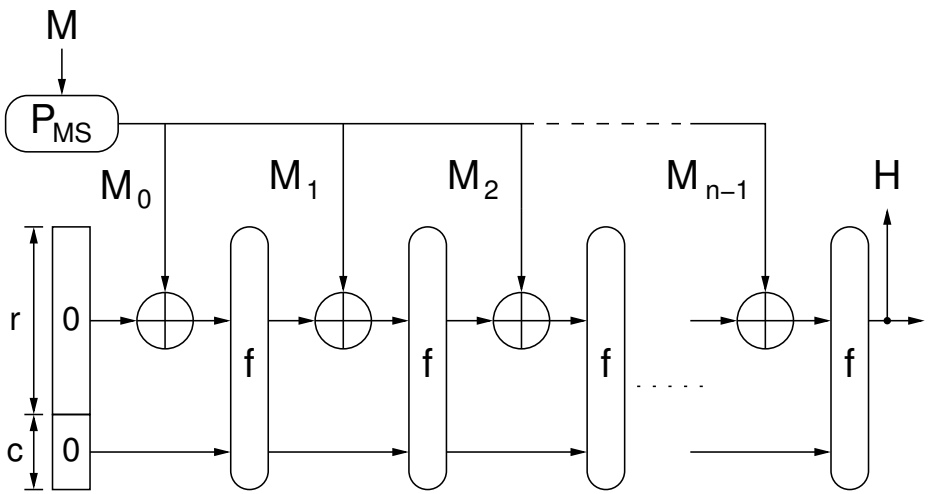
- Sponge Construction → Hash, MAC



- Duplex Construction → AEAD, PRNG

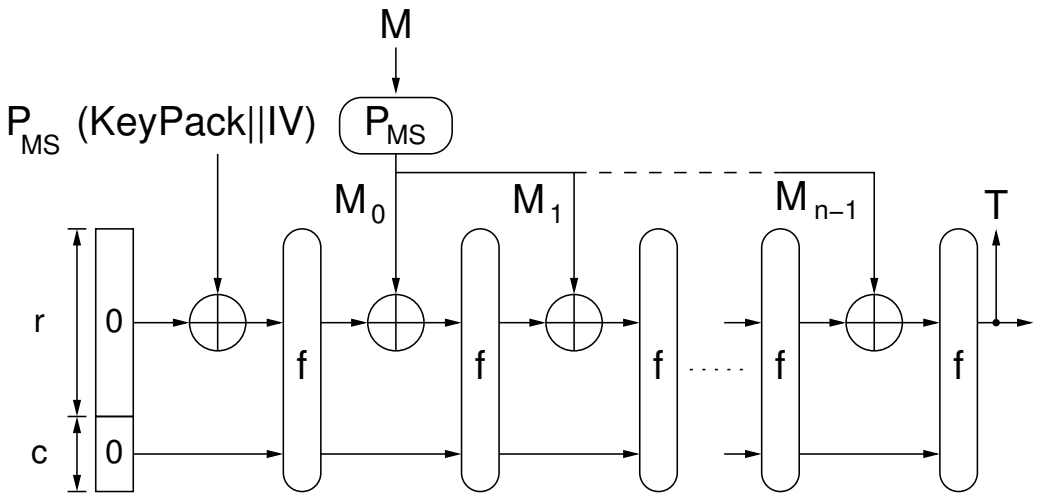


Keccak Hash: Keccak, i.e. the upcoming SHA-3



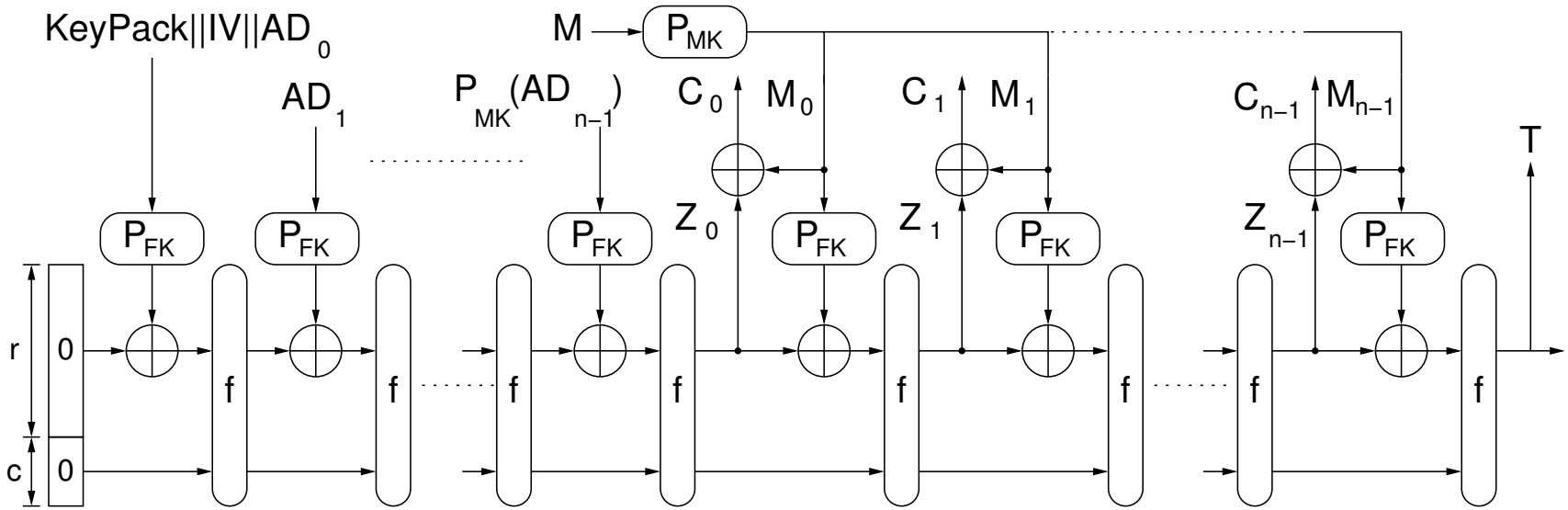
- Sponge Mode
- r=1088, c=512, 24 rounds
- P_{MS}: Padding for message in Sponge Mode
- $|P_{MS}(M)| = n \cdot 1088$

Keccak MAC: Sponge



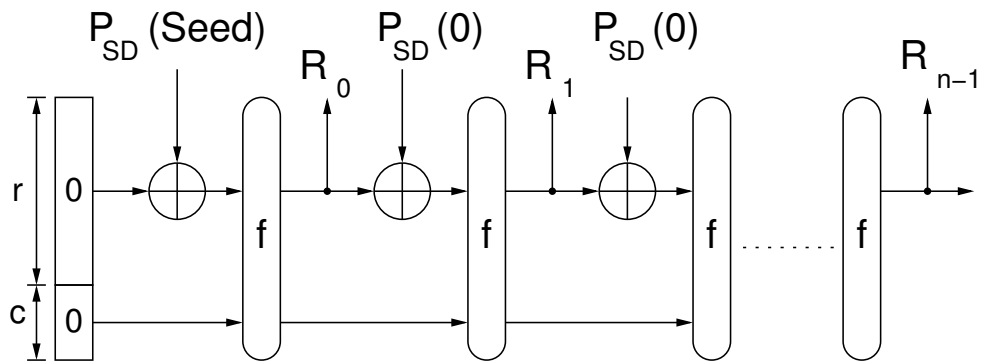
- KeyPack is used to encode the secret key in a uniform way.
- P_{MS}: Padding for message in Sponge Mode
- $|P_{MS}(M)| = n \cdot 1088$
- $|P_{MS}(KeyPack||IV)| = 1088$

Keccak AEAD: Keyak



- Lake Keyak, block size 1344, c=256, 12 rounds.
- Submission to Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR).
- P_{MK}: Message padding for Keyak, $|P_{MK}(M)| = n \cdot 1344$
- P_{FK}: Frame Padding for Keyak
- $|P_{FK}| = n \cdot 1348$: 4 padding frame bits are XORed with c. This is not shown in the figure.

Keccak PRNG: Duplex



- Block size 1344, c=256, 12 rounds
- P_{SD}: Padding for seed in PRNG Mode
- $P_{SD}(0)$: Padded empty seed for additional random bits.
- $|P_{SD}(\text{Seed})| = |P_{SD}(0)| = 1348$
- 4 padding frame bits are XORed with c. This is not shown in the figure.

Keccak and AES Modes of Operation

AES Modes

Operation	Mode	Block	Key	Rd.	Inputs	Outputs
Hash	AES-Hash	256	N/A	14	$\|M\|$, M	H
MAC	CMAC	128	128	10	$\|M\|$, M, K, IV	T
AEAD	GCM	128	128	10	$\|M\|$, M, K, IV, $\|AD\|$, AD	T, C
PRNG	Fortuna	128	N/A	10	S	R

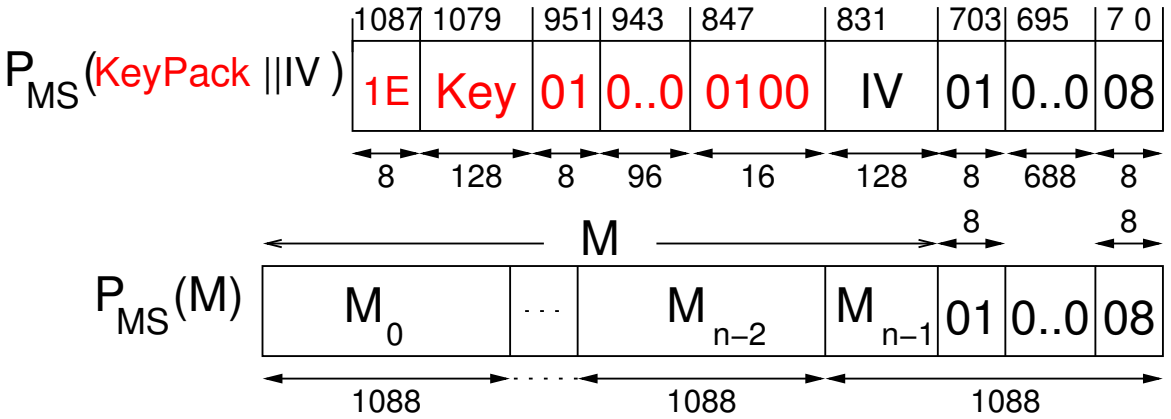
Keccak Modes

Operation	Mode	Block	Key	Rd.	ρ	Inputs	Outputs
Hash	Sponge	1600	N/A	24	1088	$\|M\|$, M	H
MAC	Sponge	1600	128	24	1088	$\|M\|$, M, K, IV	T
AEAD	Duplex	1600	128	12	1344	$\|M\|$, M, K, IV, $\|AD\|$, AD	T, C
PRNG	Duplex	1600	N/A	12	1344	S	R

M–Message, K–Key, AD–Associated Data, S–Seed, IV–Initialization Value
H–Hash, T–Tag, C–Cipher-text, R–Random Number, $|X|$–Length of X

Keccak Padding

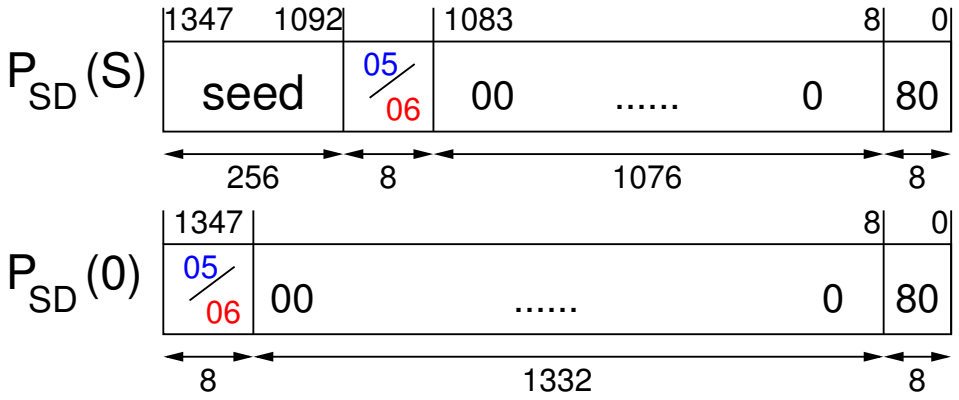
Sponge Mode for Hash and MAC



Padding for seed in Duplex Mode for PRNG

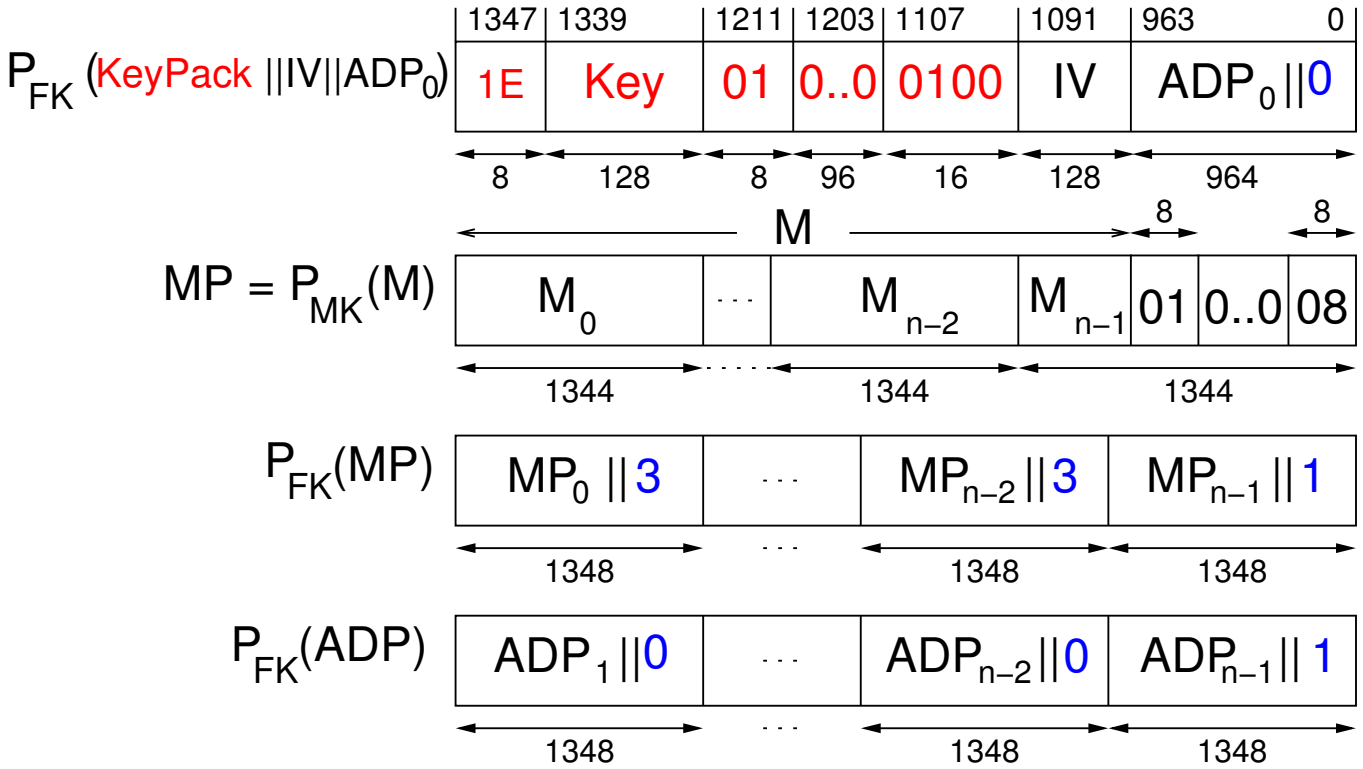
05: all blocks except last block

06: last block



Keccak Padding-*Cont...*

Padding for Keyak (Duplex Mode)

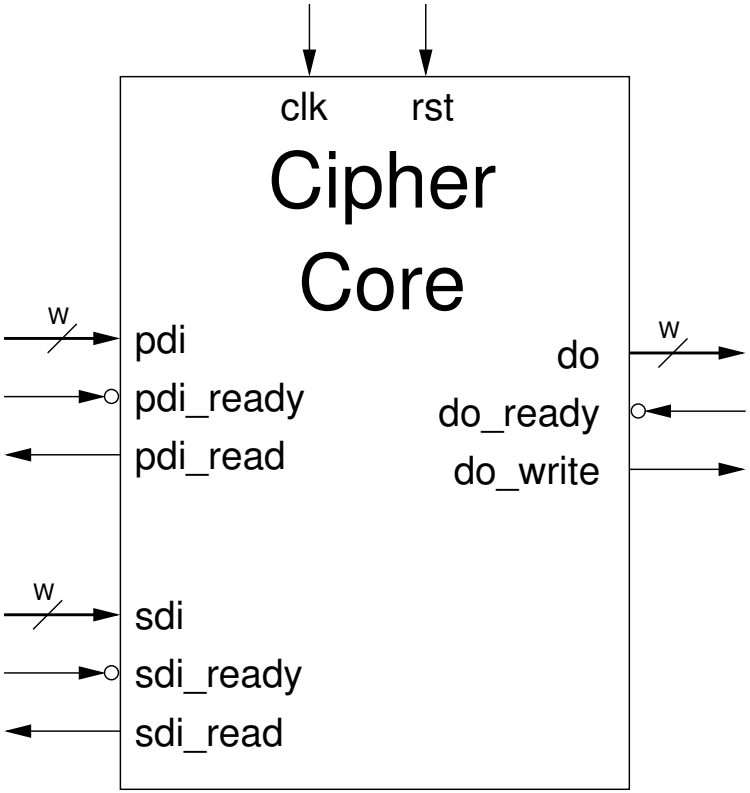


- The bits in blue are frame bits

Design Decisions

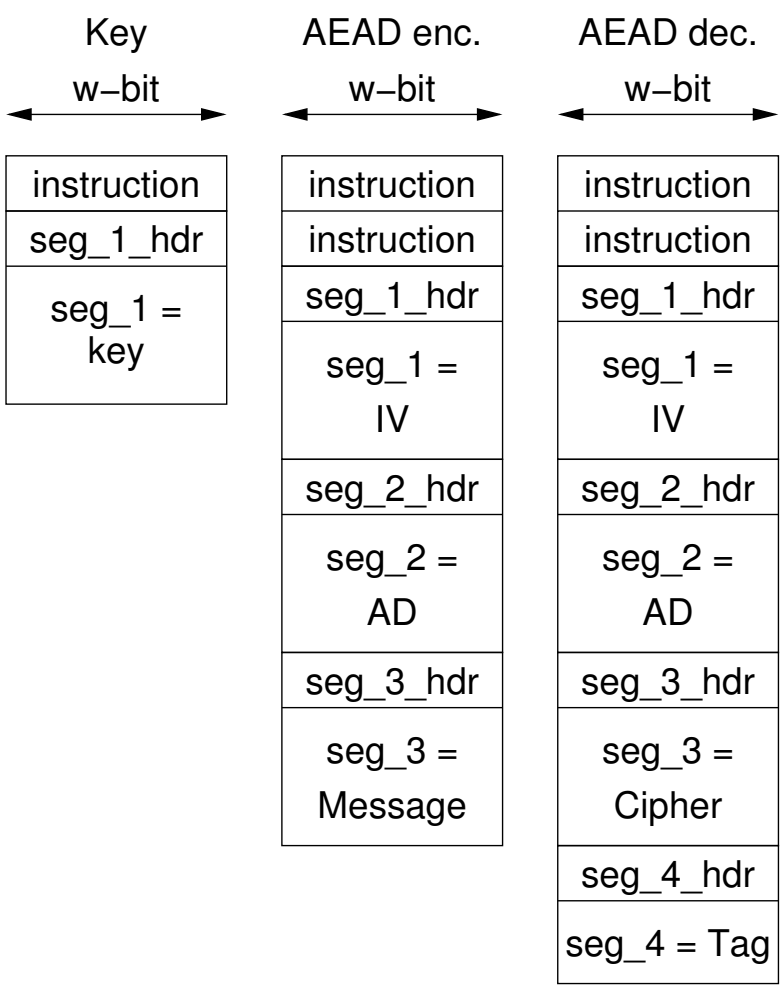
- One high speed (HS) and one low-area (LA) all-in-one design each.
- All-in-one supports Hash, MAC, AEAD, and PRNG.
- HS design of Keccak uses full width datapath of 1600 bits.
- HS design of AES uses 2 cores of AES-128/256 that can be combined to a single Rijndael with 256 block size.
- LA design AES 32-bit datapath (width of MixColumns).
- LA design Keccak 64-bit (width of a word in Keccak).
- All padding is performed in hardware.

Interface

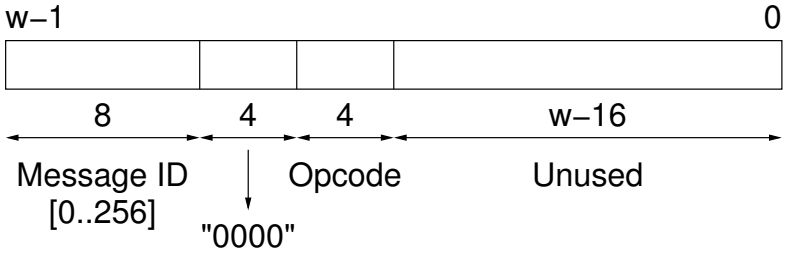


- HS design data width $w = 64$bits
- LA design data width $w = 16$bits
- Key for MAC and AEAD has to arrive at SDI beforehand.
- Activate Key command at PDI activates new key.

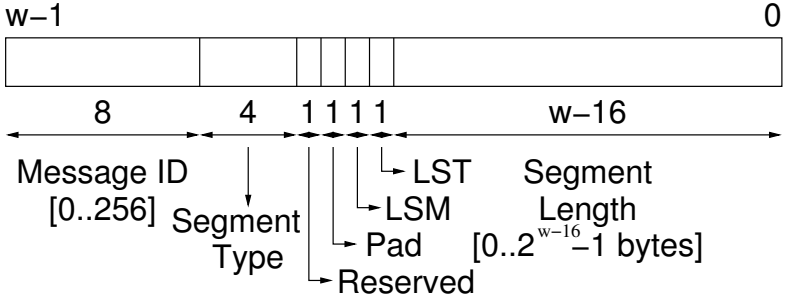
Protocol



Instruction

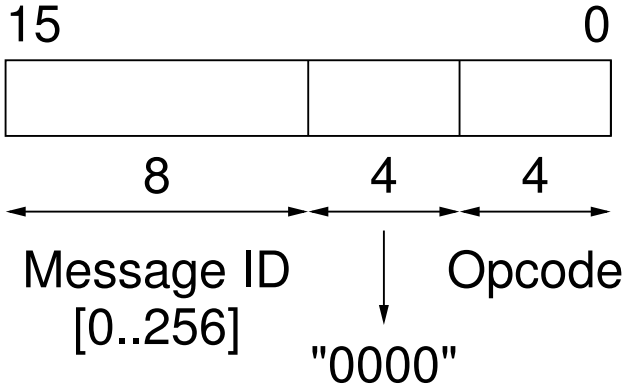


Segment Header and Length



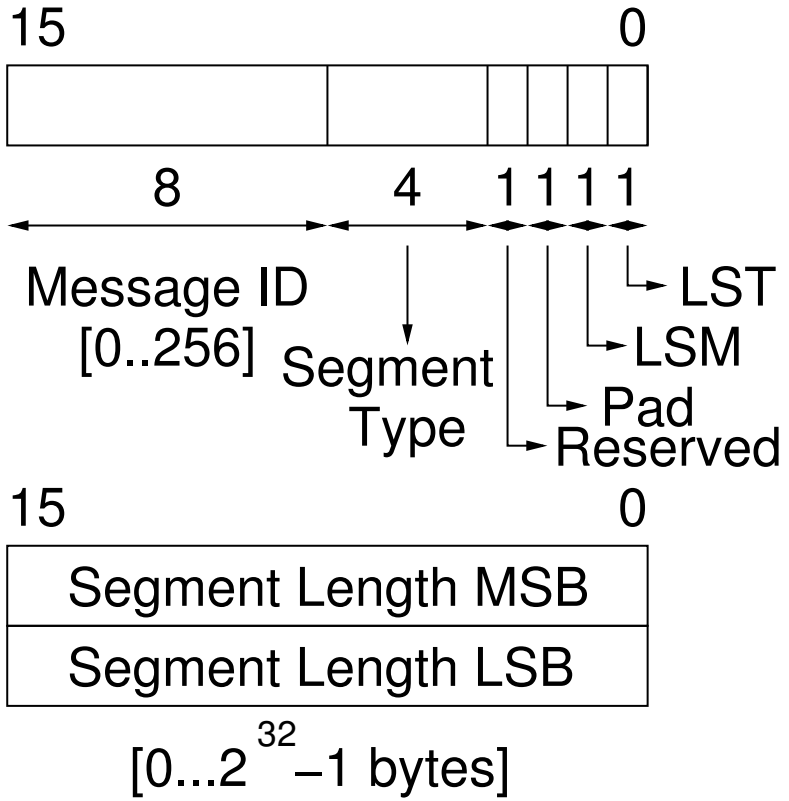
Protocol LA

Instruction

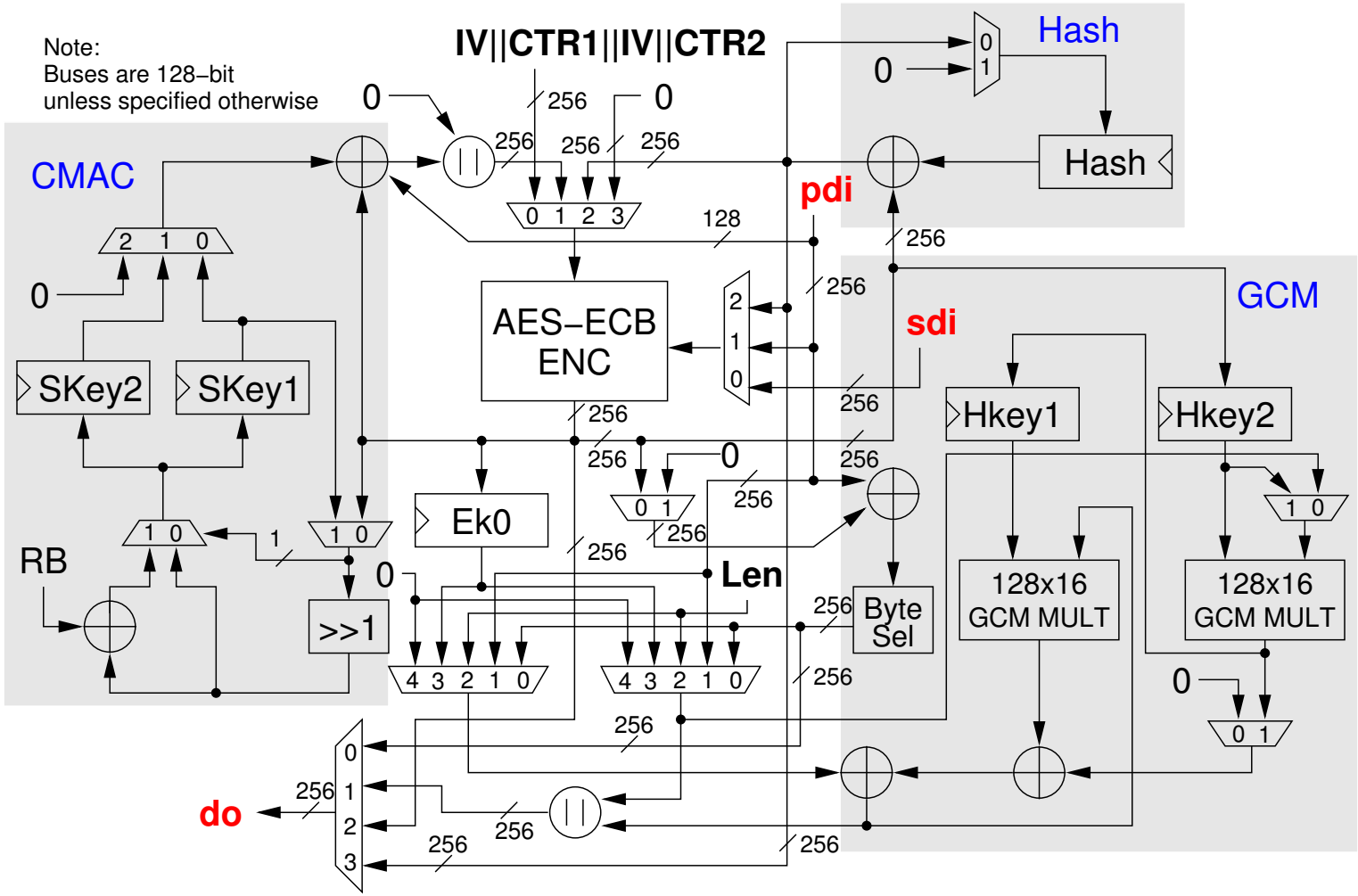


- Segment header is followed by two words for segment length.
- Maximum supported length of message is $(2^{32} - 1)$ bytes= 4GB

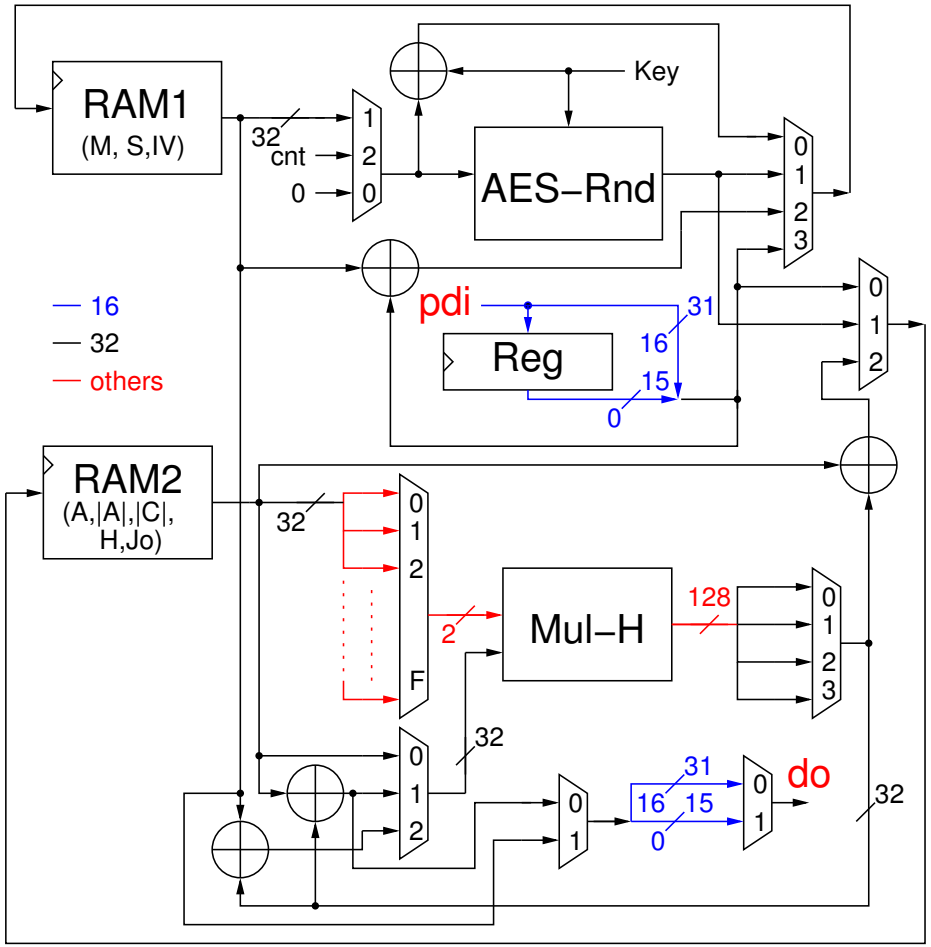
Segment Header and Length



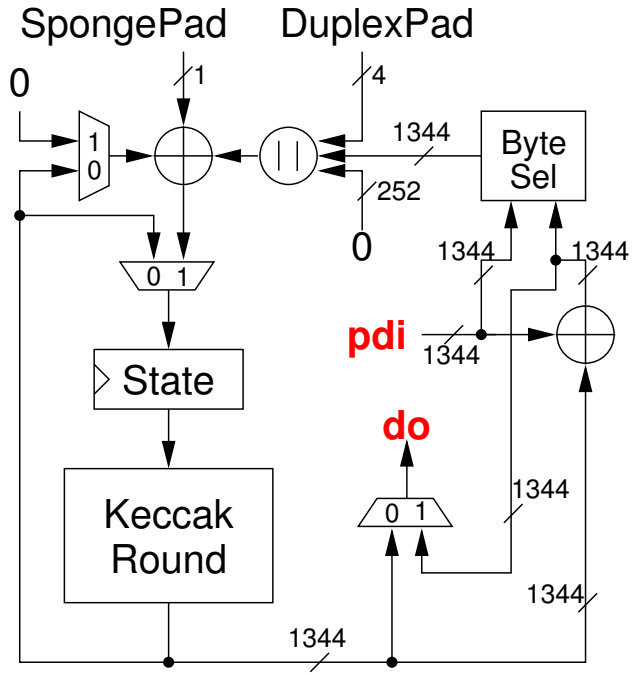
AES High Speed Architecture



AES Low Area

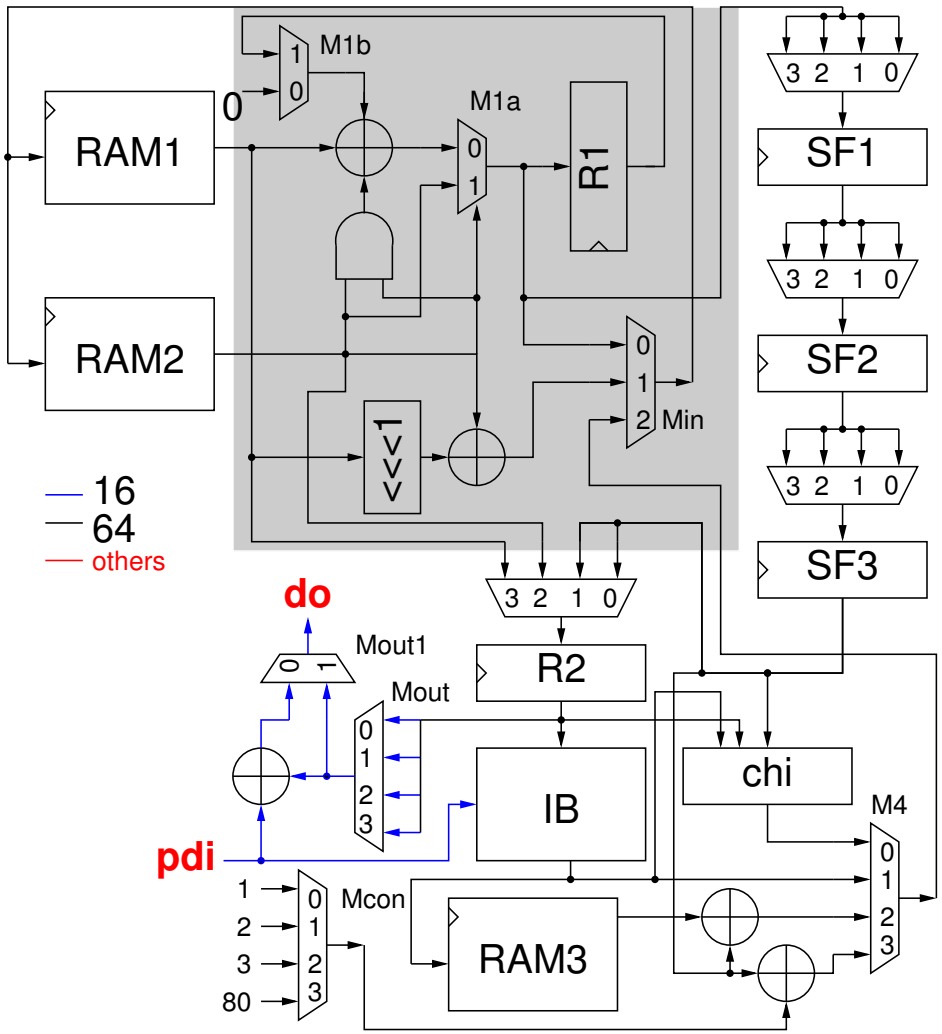

RAM1
(M, S,IV)
32
cnt
0
1
2
0
Key
AES–Rnd
0
1
2
3
16
32
others
pdi
Reg
31
16
15
0
0
1
2
RAM2
(A,|A|,|C|,
H,Jo)
32
0
1
2
F
2
Mul–H
128
0
1
2
3
32
0
1
2
0
1
31
16
15
0
0
1
do
32

Keccak High Speed Architecture



- Buses are 1600-bit unless specified otherwise

Keccak Low Area



Test Setup

- All implementations are coded VHDL and do not use embedded resources.
- Implemented using Xilinx ISE 14.6.
- Optimized using ATHENa.
- All results are post place-and-route.

Device	Technology
Spartan6	45nm
Virtex6	40nm
Artix7	28nm
Virtex7	28nm

Implementations results for High-Speed on Spartan-6

Mode	Algorithm	TP [Gbps]	TP/area [Mbps/Slices]
AEAD	AES-GCM	2.942	0.953
	Keyak	14.390	11.322
MAC	AES-CMAC	1.471	0.476
	Keccak-MAC	5.825	4.583
PRNG	AES-PRNG	2.157	0.699
	Keccak-PRNG	14.390	11.322
Hash	AES-HASH	2.157	0.699
	Keccak-HASH	5.825	4.583

- AES: 3087 Slices at 126.41 MHz
- Keccak: 1271 Slices at 128.49 MHz

Implementations results for Low-Area on Spartan-6

Mode	Algorithm	TP [Gbps]	TP/area [Mbps/Slices]
AEAD	AES-GCM	0.160	0.221
	Keyak	0.279	1.120
MAC	AES-CMAC	0.274	0.379
	Keccak-MAC	0.121	0.487
PRNG	AES-PRNG	0.547	0.759
	Keccak-PRNG	0.285	1.145
Hash	AES-HASH	0.239	0.332
	Keccak-HASH	0.128	0.512

- AES: 721 Slices at 119.67 MHz
- Keccak: 249 Slices at 155.06 MHz

Implementations results for High-Speed on Virtex-6

Mode	Algorithm	TP [Gbps]	TP/area [Mbps/Slices]
AEAD	AES-GCM	5.744	2.753
	Keyak	34.707	27.589
MAC	AES-CMAC	2.872	1.377
	Keccak-MAC	14.048	11.167
PRNG	AES-PRNG	4.212	2.019
	Keccak-PRNG	34.707	27.589
Hash	AES-HASH	4.212	2.019
	Keccak-HASH	14.048	11.167

- AES: 2086 Slices at 246.79 MHz
- Keccak: 1258 Slices at 309.89 MHz

Implementations results for Low-Area on Virtex-6

Mode	Algorithm	TP [Gbps]	TP/area [Mbps/Slices]
AEAD	AES-GCM	0.308	0.410
	Keyak	0.524	2.007
MAC	AES-CMAC	0.528	0.703
	Keccak-MAC	0.228	0.873
PRNG	AES-PRNG	1.056	1.405
	Keccak-PRNG	0.535	2.051
Hash	AES-HASH	0.462	0.615
	Keccak-HASH	0.239	0.918

- AES: 751 Slices at 230.89 MHz
- Keccak: 261 Slices at 291.21 MHz

Implementations results for High-Speed on Virtex-7

Mode	Algorithm	TP [Gbps]	TP/area [Mbps/Slices]
AEAD	AES-GCM	6.968	2.662
	Keyak	23.150	8.511
MAC	AES-CMAC	3.484	1.331
	Keccak-MAC	9.370	3.445
PRNG	AES-PRNG	5.110	1.952
	Keccak-PRNG	23.150	8.511
Hash	AES-HASH	5.110	1.952
	Keccak-HASH	9.370	3.445

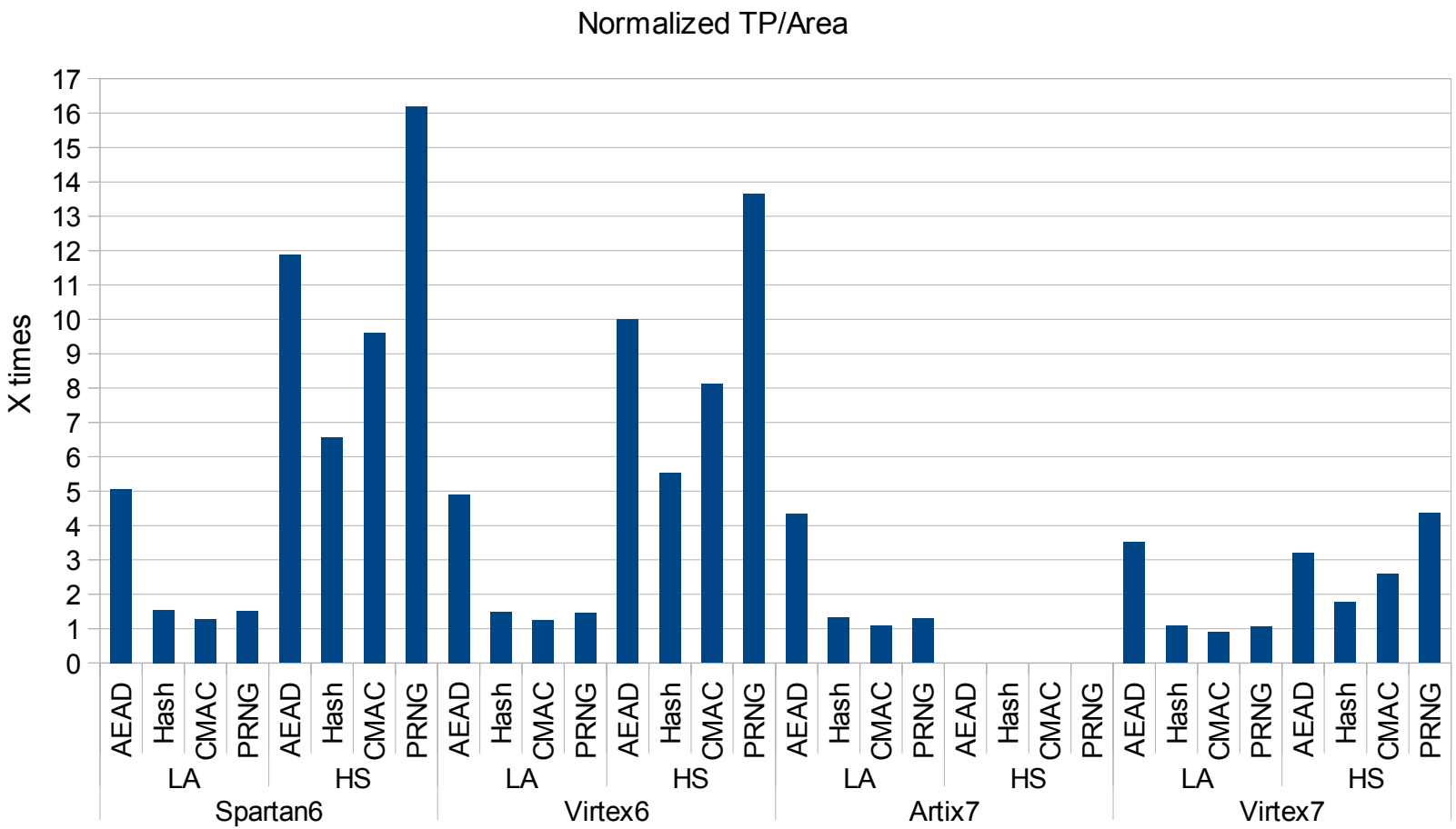
- AES: 2618 Slices at 299.40 MHz
- Keccak: 2720 Slices at 206.70 MHz

Implementations results for Low-Area on Virtex-7

Mode	Algorithm	TP [Gbps]	TP/area [Mbps/Slices]
AEAD	AES-GCM	0.297	0.358
	Keyak	0.437	1.263
MAC	AES-CMAC	0.510	0.614
	Keccak-MAC	0.190	0.549
PRNG	AES-PRNG	1.020	1.229
	Keccak-PRNG	0.447	1.291
Hash	AES-HASH	0.446	0.538
	Keccak-HASH	0.200	0.577

- AES: 830 Slices at 223.06 MHz
- Keccak: 346 Slices at 242.90 MHz

Plot


Normalized TP/Area
X times
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
AEAD
Hash
CMAC
PRNG
LA
HS
Spartan6
Virtex6
Artix7
Virtex7

Conclusions

- Our multi-purpose Keccak outperforms our multi-purpose AES in terms of throughput over area by an average of 7.8.
- In Keyak mode our multi-purpose Keccak reaches 34.7 Gbps on Xilinx Virtex 6, AES-GCM 27.6 Gbps.
- In terms of Area, our dual-core AES is up to 2.9 times as large as Keccak.
- Typically a *plain* AES is much smaller than a *plain* Keccak.
- Addition of modes is more costly for AES than Keccak
  $\Rightarrow$ Keccak is more flexible than AES.

Thanks for your attention.