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

Directions in Authenticated Ciphers – DIAC 2014
August 24th, 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

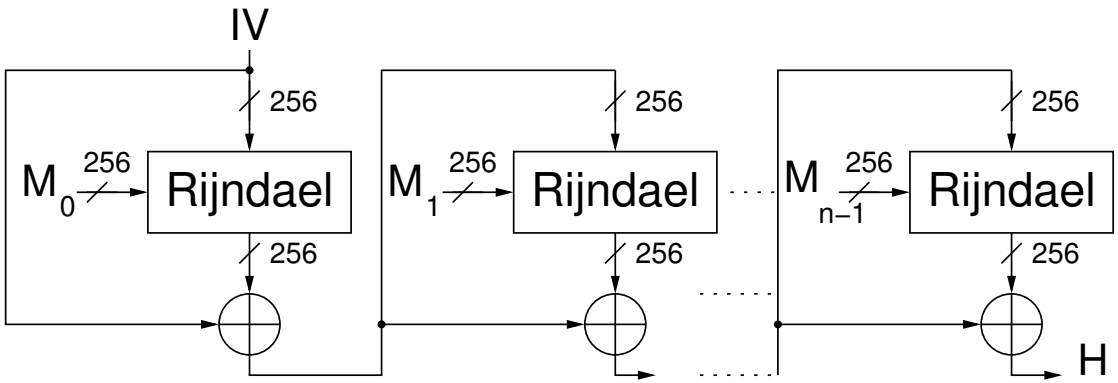
Advanced Encryption Standard

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

Keccak-p[1600,n_r] f-permutation

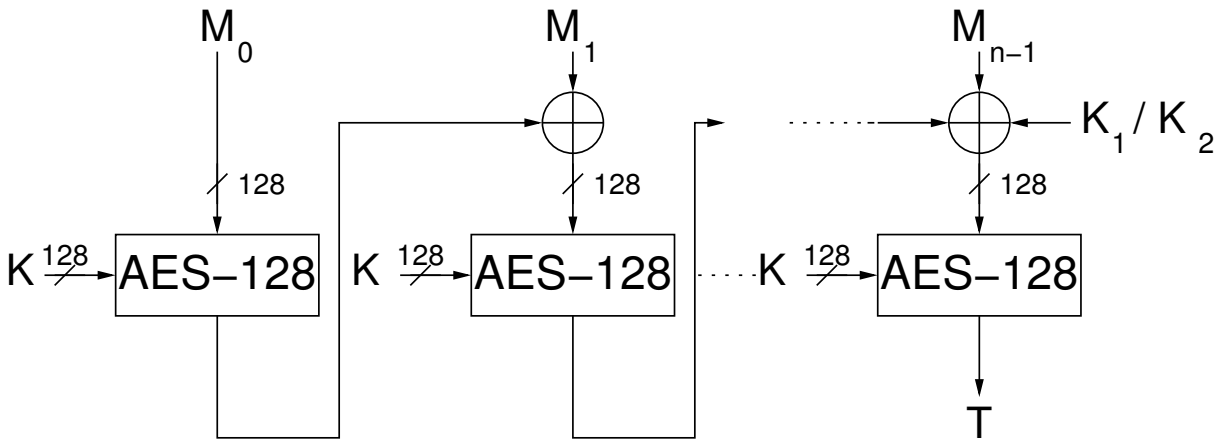
- It is the basis of Keccak, the Winner of competition for next Secure Hash Algorithm (SHA-3).
- 1600-bit state size
- Keccak is based on Sponge construction.

AES Hash: AES-Hash



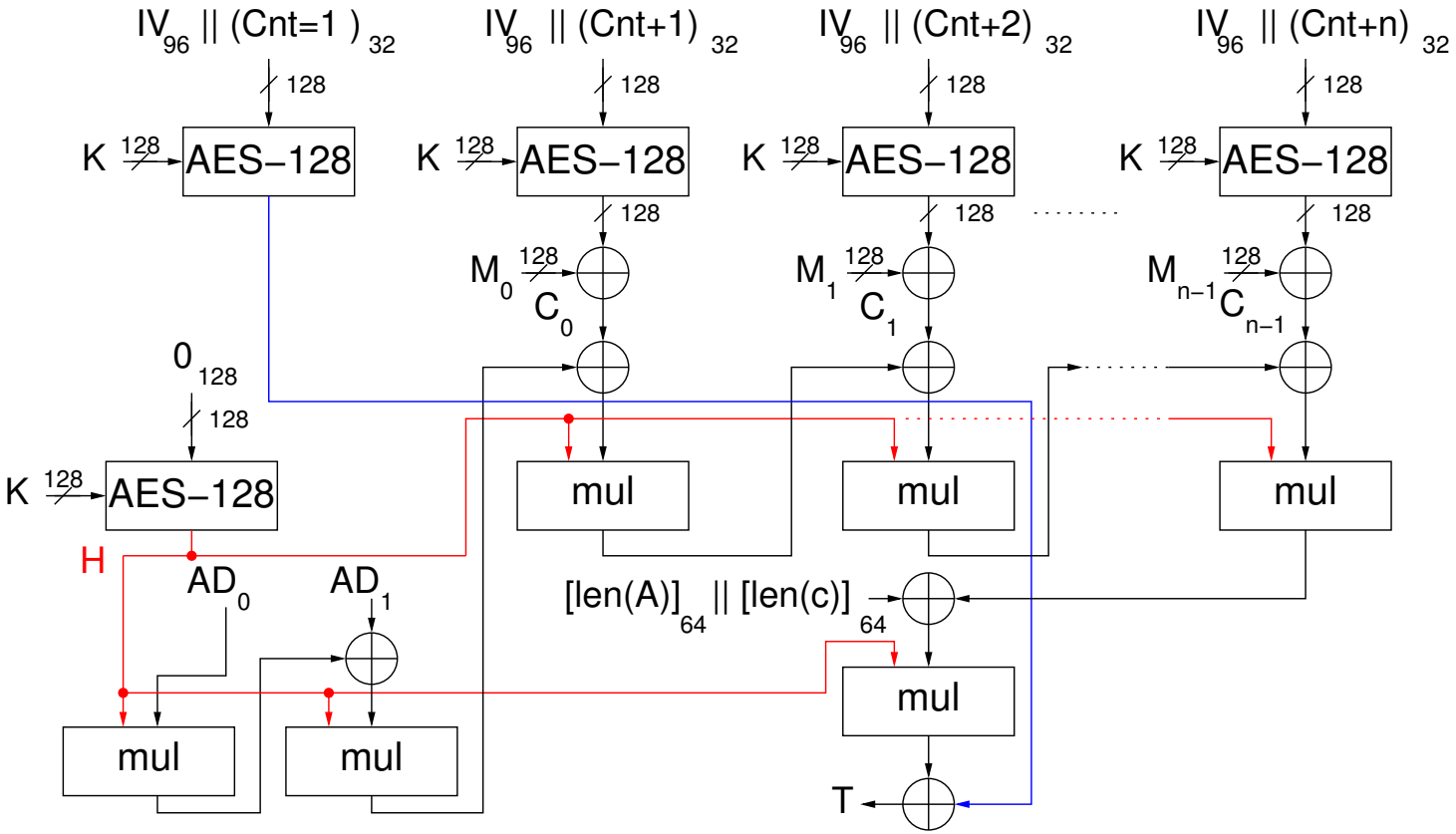
- Based on Davies-Meyer.
- The message enters on the input for the key.
- Uses a block size of 256-bit → Rijndael.
- Not a NIST standardized mode.

AES MAC: CMAC



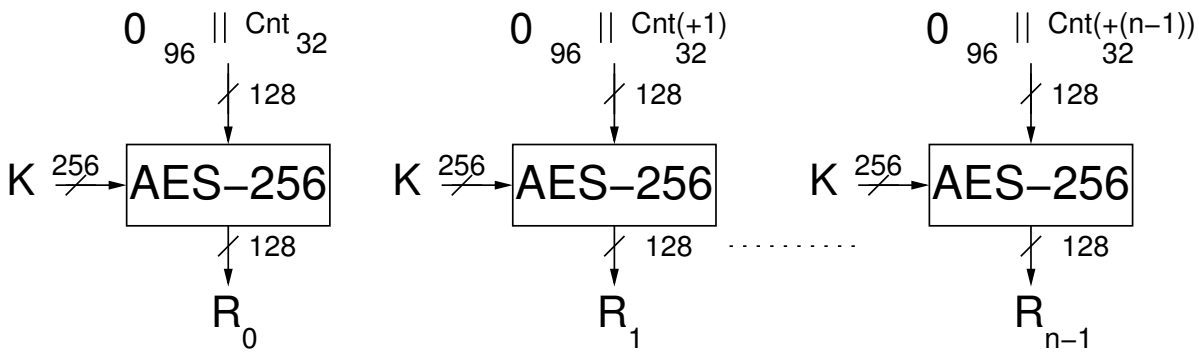
- Recommended mode of operation by NIST.
- Equivalent to One-Key CBC-MAC (OMAC1).
- K_1 and K_2 are derived from K through single bit shifts and XORed with constant.

AES AEAD: Galois Counter Mode



- Recommended mode of operation by NIST.

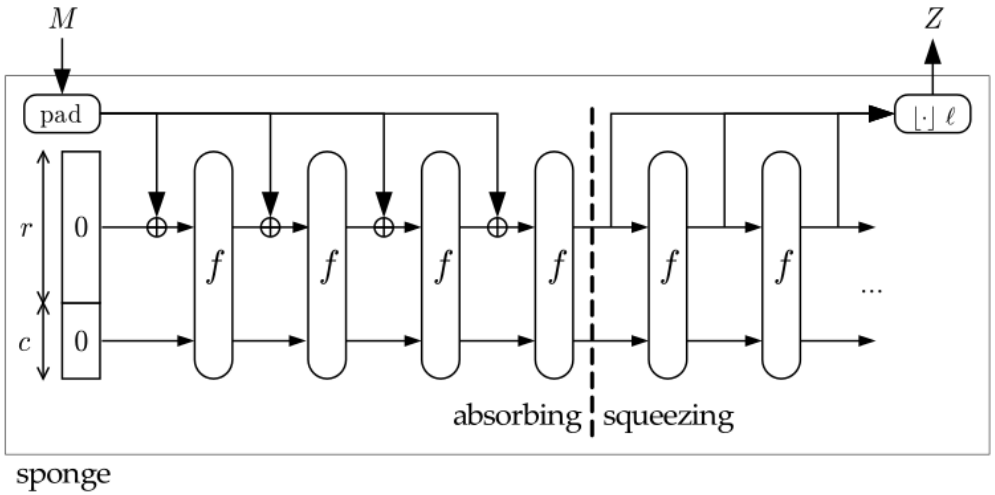
AES PRNG: Fortuna



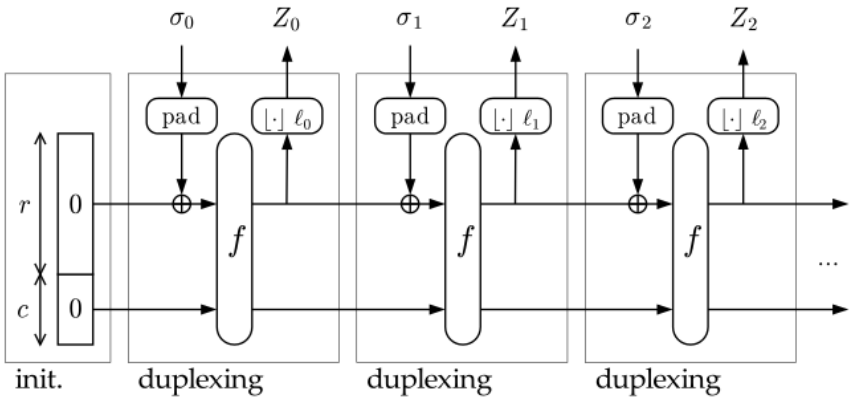
- Cryptographically secure PRNG
- Not a NIST standardized mode.
- Used in Windows 2000 and Windows XP
- The seed is processed as key.

Keccak Modes of Operation

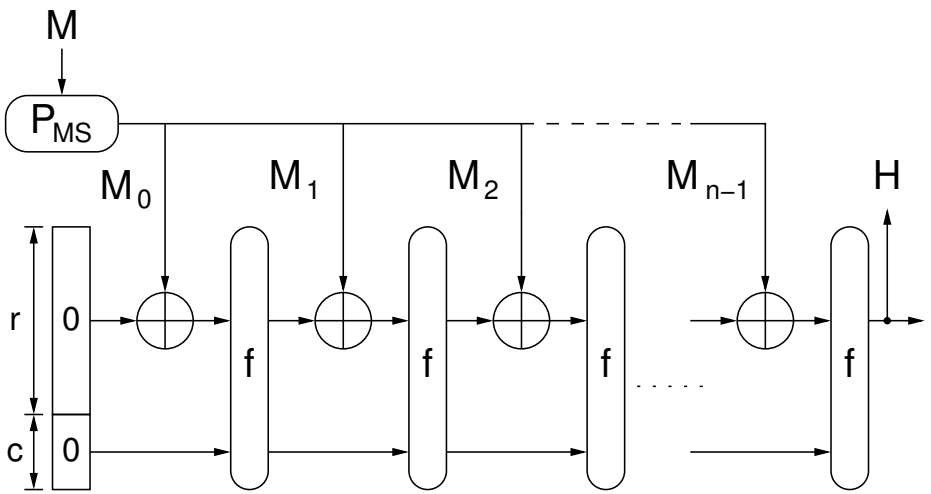
- Sponge Construction → Hash, MAC



- Duplex Construction → AEAD, PRNG

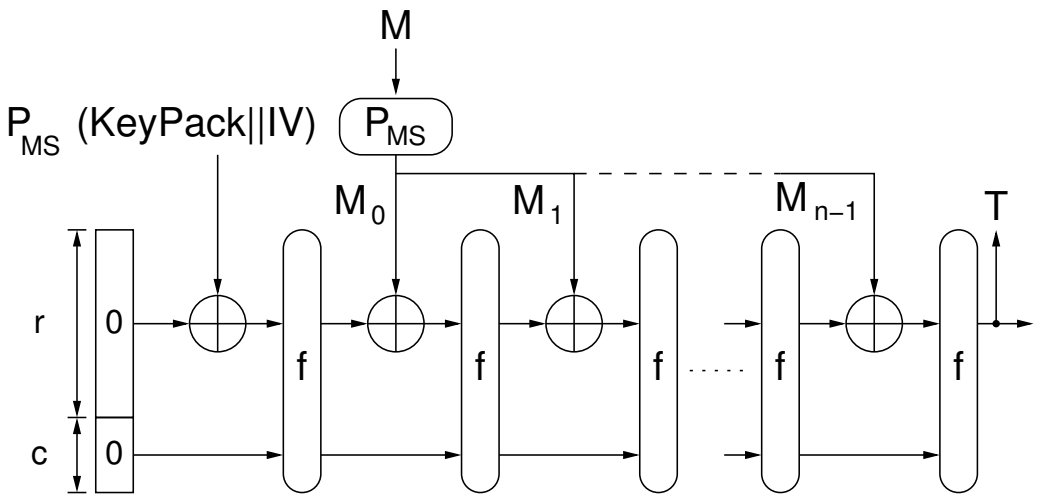


Keccak Hash: Keccak, i.e. the upcoming SHA-3



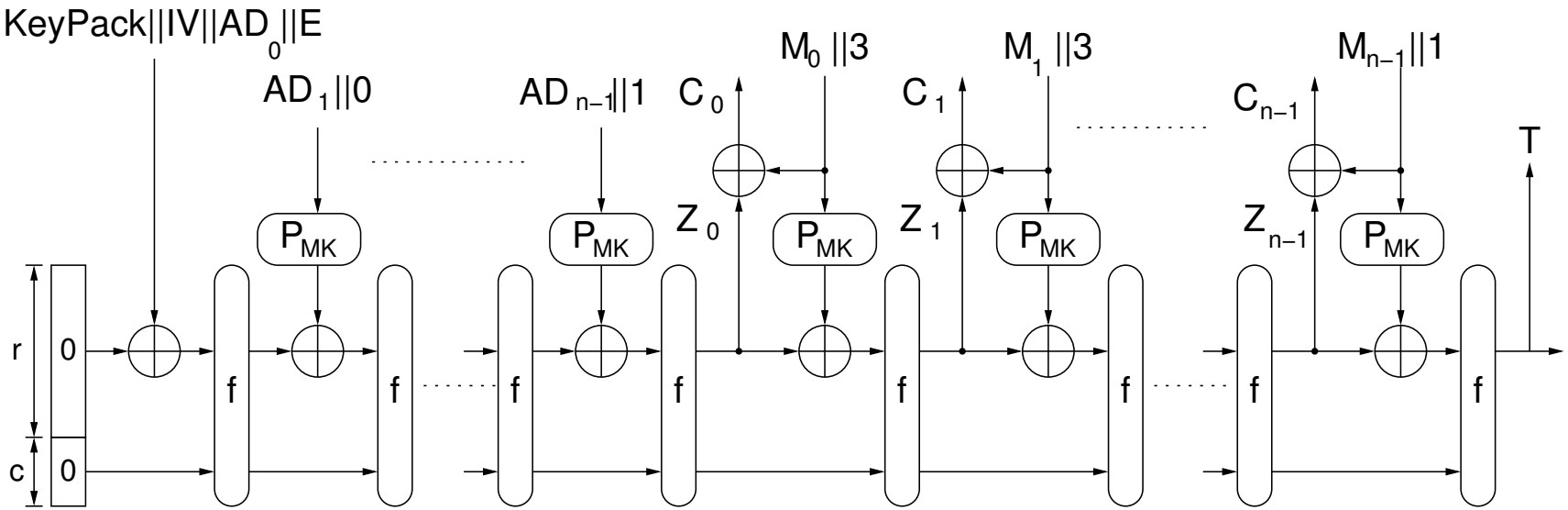
- Sponge Mode
- r=1088, c=512, 24 rounds
- P_{MS}: Padding for message in Sponge Mode
- $|P_{MS}(M)| = n \cdot 1088$

Keccak MAC: Sponge



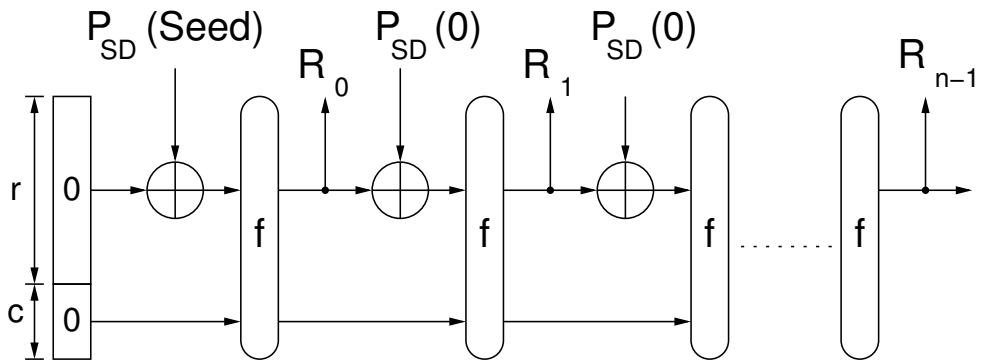
- KeyPack is used to encode the secret key in a uniform way.
- P_{MS}: Padding for message in Sponge Mode
- $|P_{MS}(M)| = n \cdot 1088$
- $|P_{MS}(KeyPack||IV)| = 1088$

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, $|P_{MK}(M_i\|3)| = 1348$, $\forall\, i \neq n-1$; $|P_{MK}(M_{n-1}\|1)| = 1348$

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.
- $|P_{SD}(\text{Seed})| = |P_{SD}(0)| = 1348$

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	14	S	R

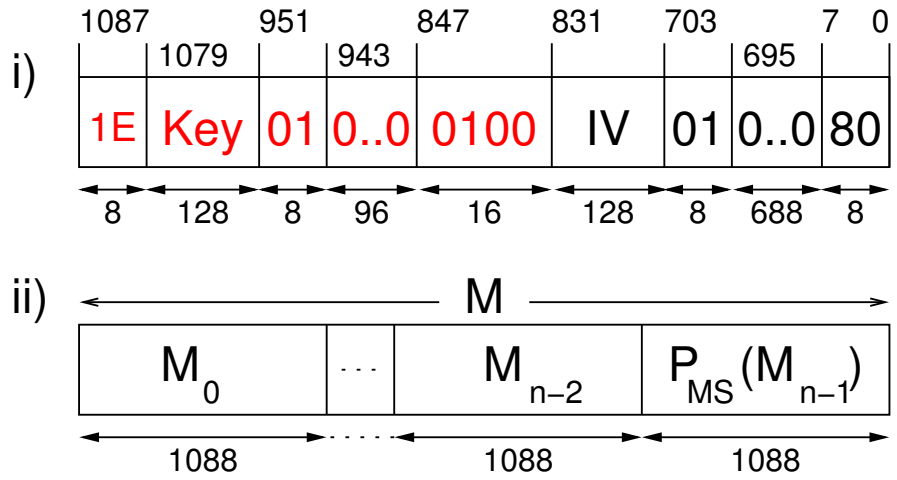
Keccak Modes

Operation	Mode	State	Key	Rd.	Block	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

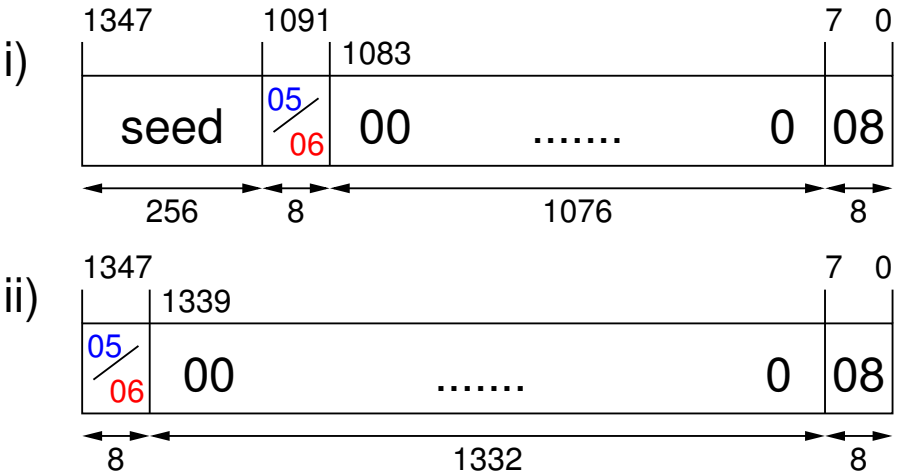
Sponge Mode for Hash and MAC



Padding for seed in Duplex Mode for PRNG

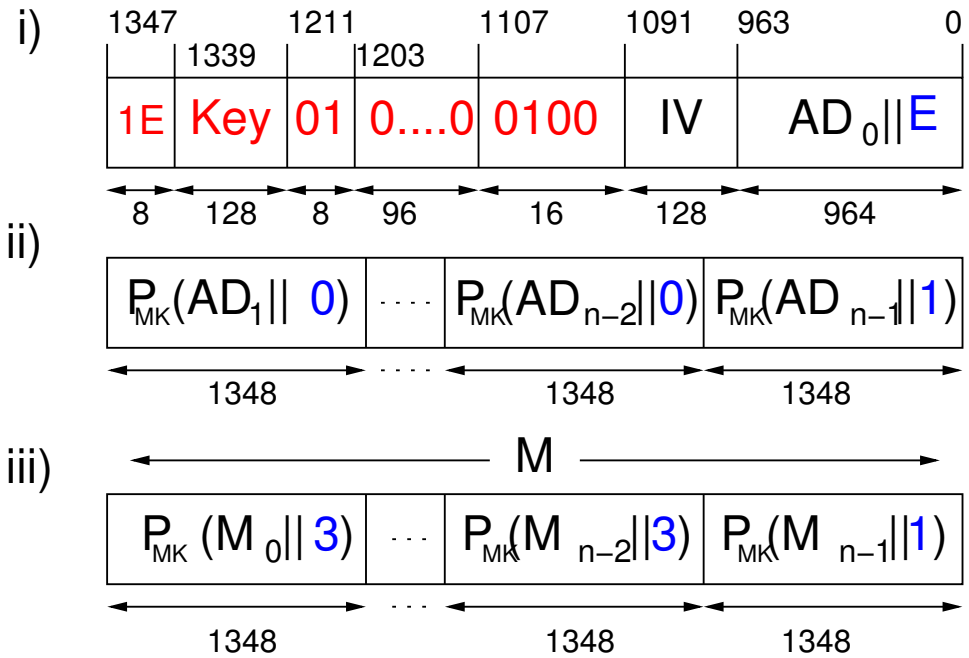
05: all blocks except last block

06: last block



Keccak Padding-*Cont...*

Padding for Keyak (Duplex Mode)

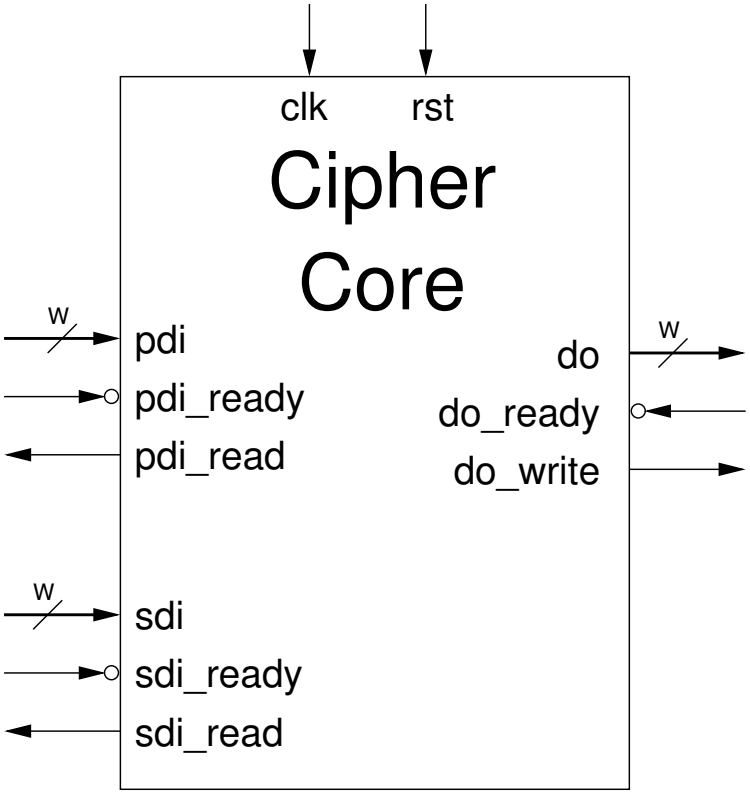


- The bits in blue are frame bits

Design Decisions

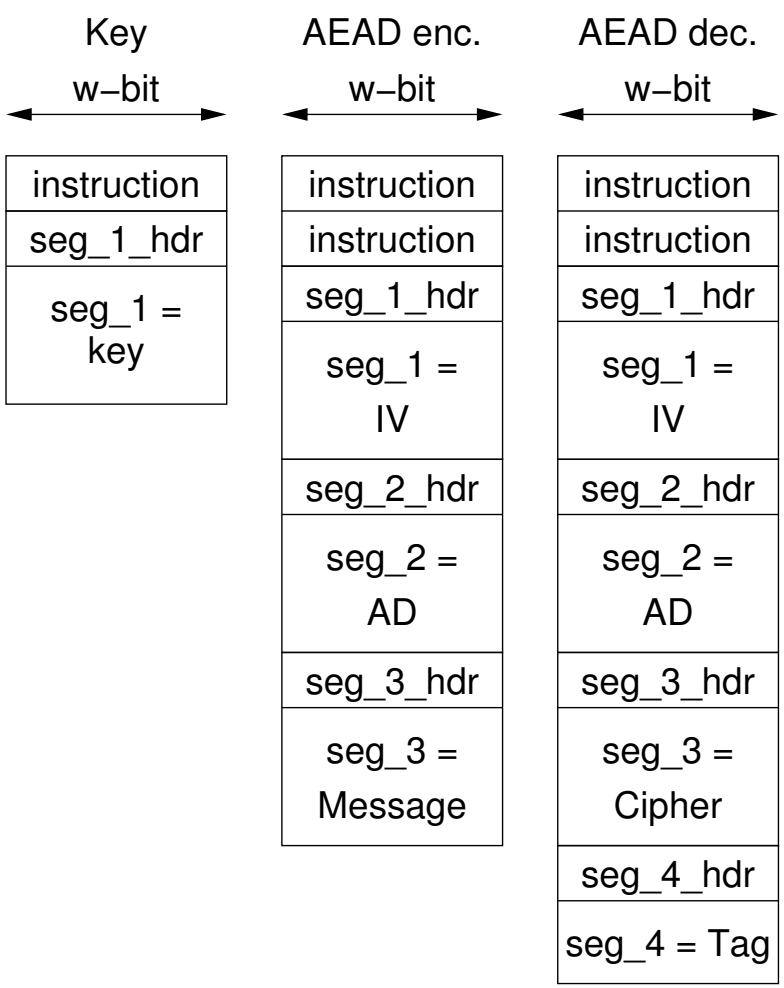
- One high speed (HS) and one low-area (LA) all-in-one design each.
- All-in-one supports Hash, MAC, AEAD, and PRNG.
- One HS and one LA dedicated AES-GCM and Keyak design each.
- HS design of Keccak uses full width datapath of 1600 bits.
- HS design of AES uses 2 cores of AES-128/256 that can be combined 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

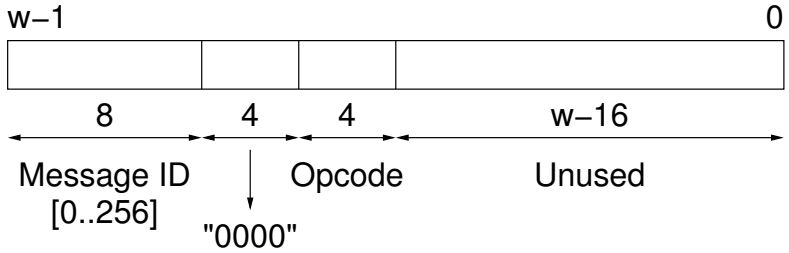


- HS design data width $w = 128$ bits
- LA design data width $w = 16$ bits
- Key for MAC and AEAD has to arrive at SDI beforehand.
- Activate Key command at PDI activates new key.

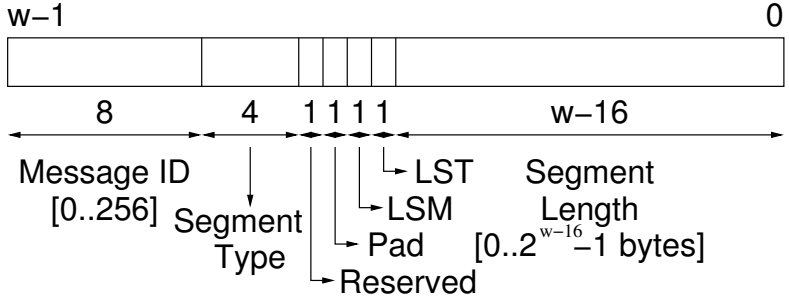
Protocol



Instruction

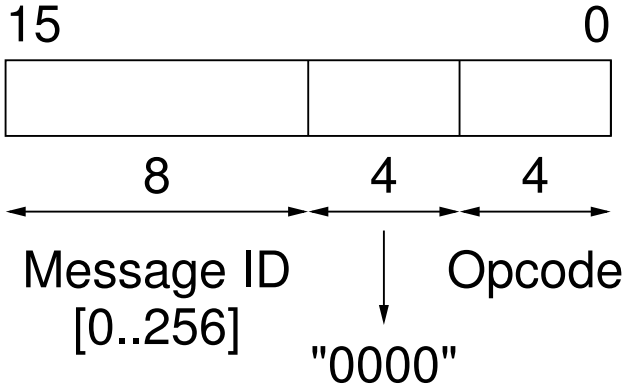


Segment Header and Length



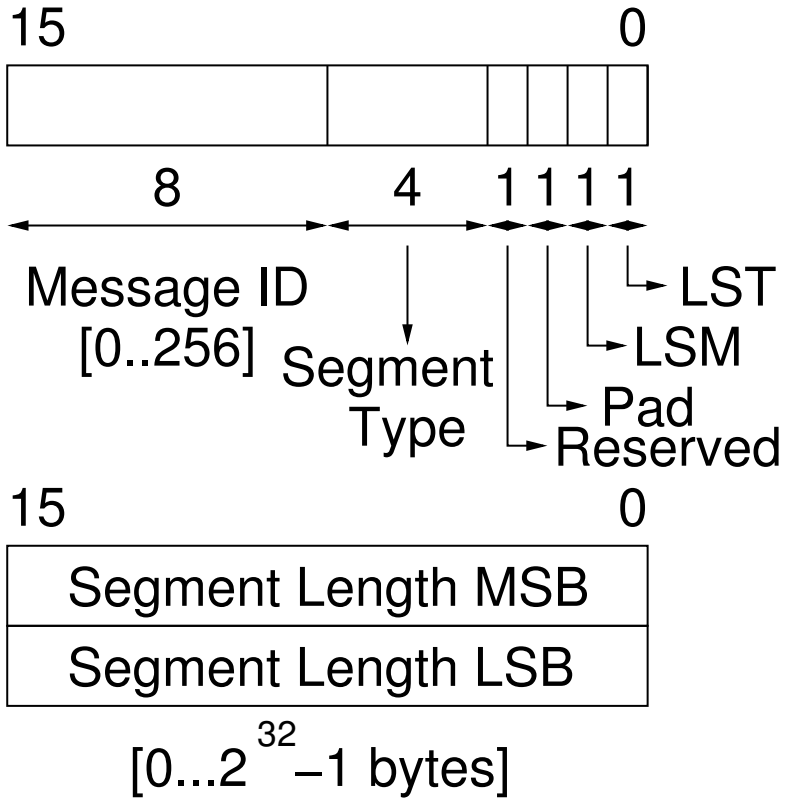
Protocol LA

Instruction

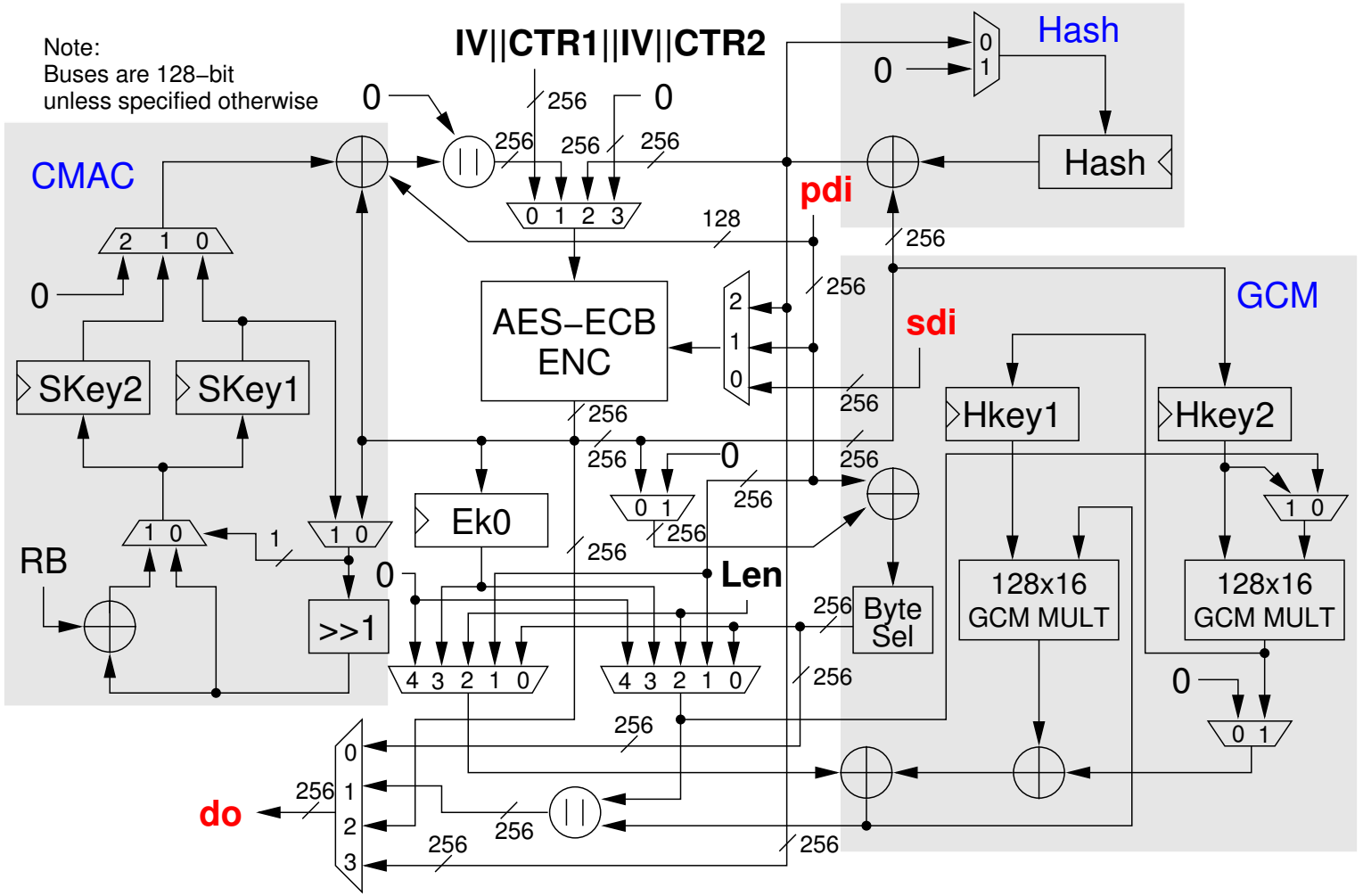


- Segment header is followed by two words for segment length.
- Maximum supported length of message is $(2^{32} - 1)$ bytes= 4GB

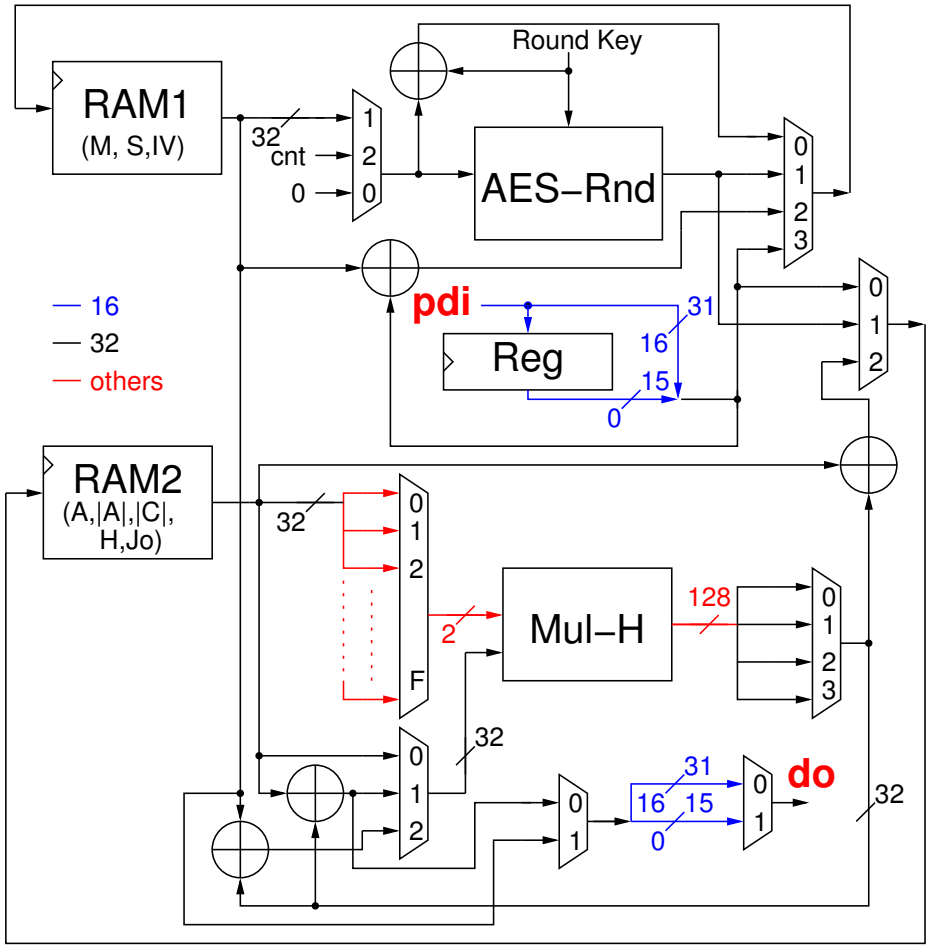
Segment Header and Length



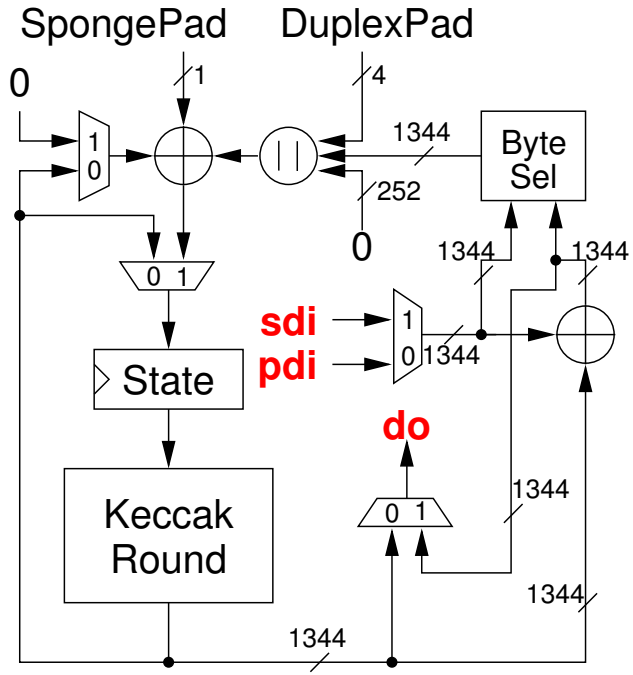
AES High Speed Architecture



AES Low Area

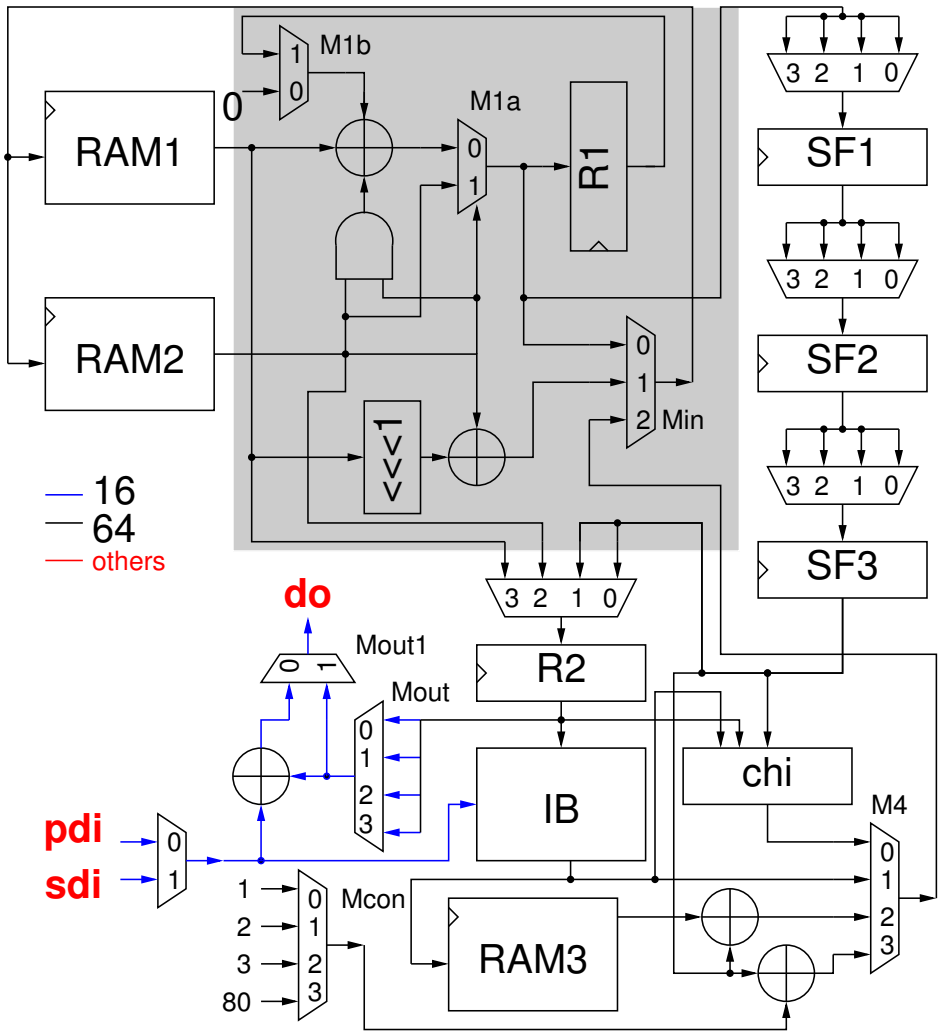

Round Key
RAM1
(M, S,IV)
32
cnt
0
AES–Rnd
16
32
others
pdi
Reg
31
16
15
0
RAM2
(A,|A|,|C|,
H,Jo)
Mul–H
128
2
F
do

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 14.7 and Quartus II 13.1.
- Optimized using ATHENa.
- All results are post place-and-route.

Xilinx		Altera	
Device	Technology	Device	Technology
Virtex-5	65 nm	Cyclone-IV	60 nm
Spartan6	45 nm		
Virtex6	40 nm	Stratix-IV	40 nm
Artix7	28 nm		
Virtex7	28 nm		

Implementations results for multi-purpose high-speed designs on Spartan-6

Mode	Algorithm	Block size	Clock cycles	TP [Gbps]	TP/area [Mbps/Slices]
Hash	AES-HASH	256	15	2.091	0.747
	Keccak-HASH	1088	24	5.825	2.239
MAC	AES-CMAC	128	11	1.426	0.509
	Keccak-MAC	1088	24	5.825	2.239
AEAD	AES-GCM	256	11	2.851	1.018
	Keyak	1344	12	14.390	5.533
PRNG	AES-PRNG	256	15	2.091	0.747
	Keccak-PRNG	1344	12	14.390	5.533

- AES: 2801 Slices at 122.52 MHz
- Keccak: 2601 Slices at 128.49 MHz

Implementations results for multi-purpose low-area designs on Spartan-6

Mode	Algorithm	Block size	Clock cycles	TP [Gbps]	TP/area [Mbps/Slices]
Hash	AES-HASH	256	128	0.184	0.410
	Keccak-HASH	1088	1323	0.136	0.504
MAC	AES-CMAC	128	56	0.210	0.468
	Keccak-MAC	1088	1391	0.129	0.479
AEAD	AES-GCM	128	144??	0.082	0.182
	Keyak	1344	747	0.298	1.103
PRNG	AES-PRNG	128	56??	0.210	0.468
	Keccak-PRNG	1344	731	0.304	1.127

- AES: 449 Slices at 92.00 MHz
- Keccak: 270 Slices at 165.45 MHz

Implementations results for high-speed Keyak and AES-GCM designs on Xilinx devices

Algorithm	Dev	Area Slices		Freq [MHz]		TP [Gbps]		TP/Area [Gbps/Slices]	
		M	D	M	D	M	D	M	D
AES-GCM	V-5	2871	1089	203	284	4.73	3.30	1.65	3.03
Keyak		2805	2357	164	244	18.36	27.32	6.55	11.59
AES-GCM	S-6	2801	1246	123	177	2.85	2.06	1.02	1.65
Keyak		2601	2279	129	157	14.39	17.60	5.53	7.72
AES-GCM	V-6	2419	1005	230	320	5.35	3.72	2.21	3.70
Keyak		2201	1958	172	203	19.29	22.74	8.76	11.61
AES-GCM	A-7	2852	1425	108	173	2.50	2.01	0.88	1.41
Keyak		2299	2173	116	133	12.98	14.94	5.65	6.88
AES-GCM	V-7	3061	1455	188	353	4.38	4.11	1.43	2.82
Keyak		2495	2444	207	258	23.15	28.94	9.28	11.84

M→Multi-purpose, D→Dedicated, A→Artix, S→Spartan, V→Virtex

Implementations results for low-area Keyak and AES-GCM designs on Xilinx devices

Algorithm	Dev	Area Slices		Freq [MHz]		TP [Gbps]		TP/Area [Gbps/Slices]	
		M	D	M	D	M	D	M	D
AES-GCM	V-5	478	351	131	131	0.12	0.12	0.24	0.33
Keyak		318	259	257	281	0.46	0.51	1.45	1.95
AES-GCM	S-6	449	389	92	88	0.08	0.08	0.18	0.20
Keyak		270	221	166	219	0.30	0.39	1.10	1.78
AES-GCM	V-6	464	350	151	143	0.13	0.13	0.29	0.36
Keyak		261	218	291	382	0.52	0.69	2.01	3.15
AES-GCM	A-7	629	548	83	71	0.07	0.06	0.12	0.12
Keyak		264	260	152	178	0.27	0.32	1.04	1.23
AES-GCM	V-7	532	521	169	154	0.15	0.14	0.28	0.26
Keyak		272	267	307	414	0.55	0.75	2.03	2.79

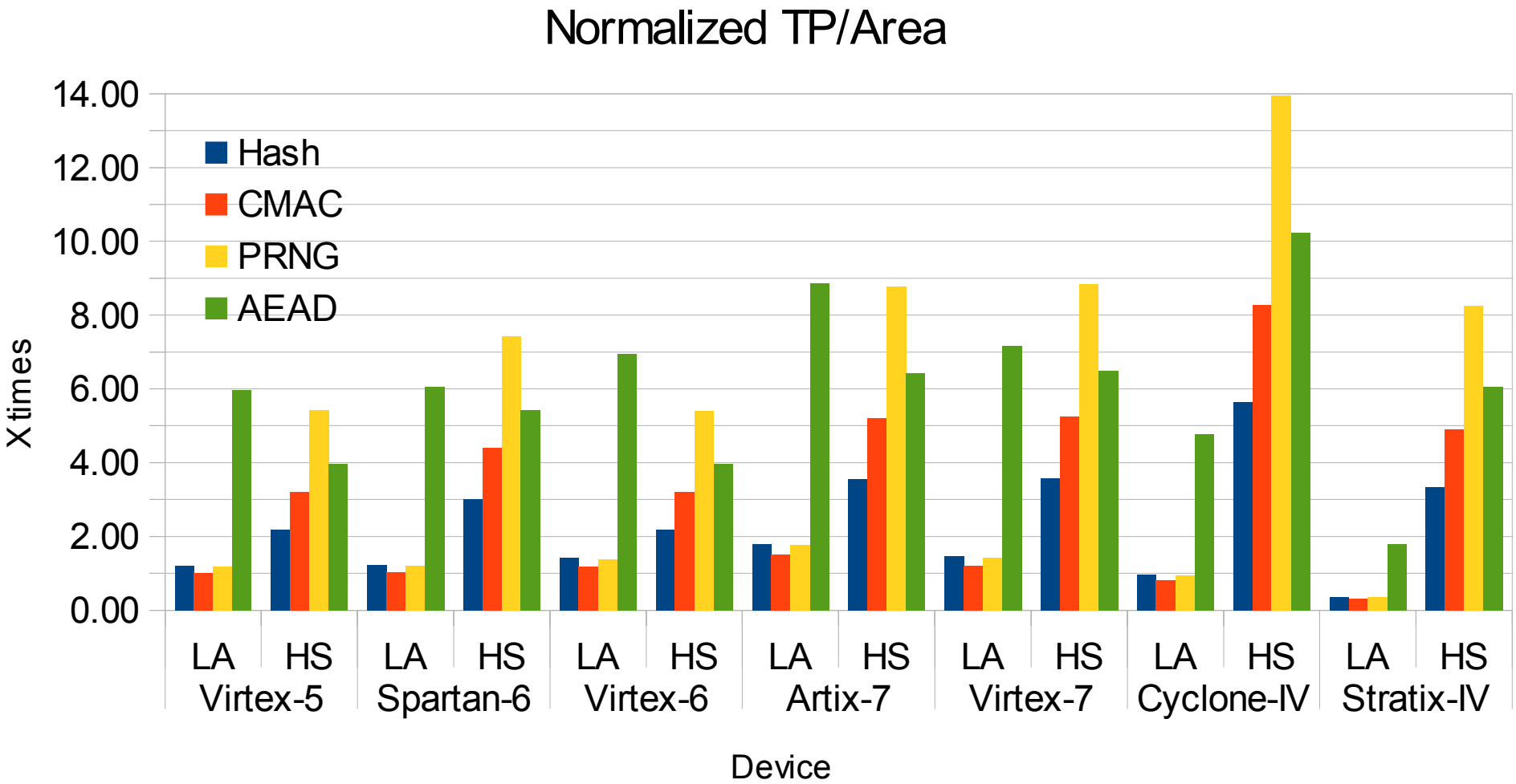
M→Multi-purpose, D→Dedicated, A→Artix, S→Spartan, V→Virtex

Implementations results for Keyak and AES-GCM designs on Altera devices

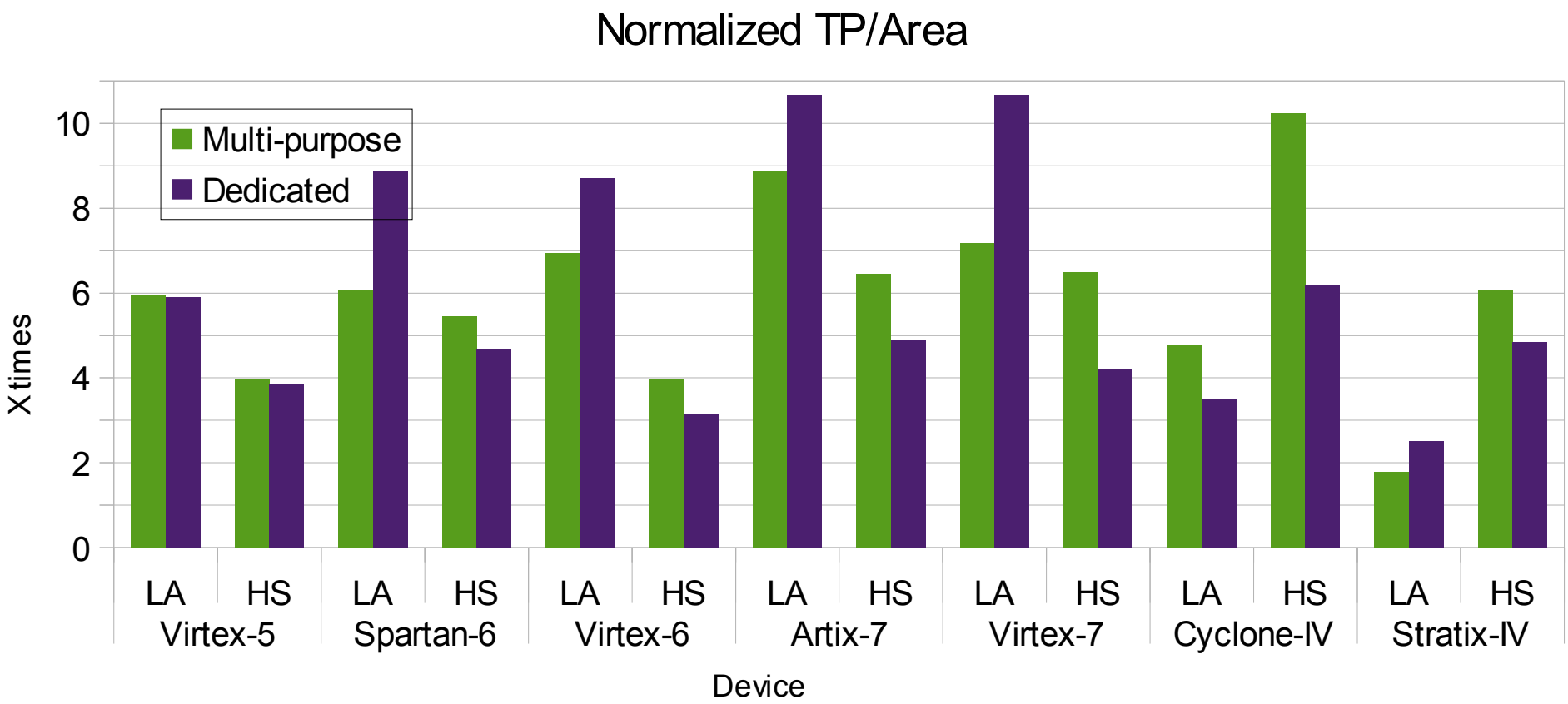
Algorithm	Dev	Area LEs		Freq [MHz]		TP [Gbps]		TP/Area [Gbps/LEs]	
		M	D	M	D	M	D	M	D
High-Speed									
AES-GCM	C-IV	20763	9074	102	159	2.37	1.85	0.11	0.20
Keyak	C-IV	12453	12333	130	139	14.53	15.59	1.17	1.26
AES-GCM	S-IV	9760	4012	240	301	5.59	3.51	0.57	0.87
Keyak	S-IV	8294	6765	257	255	28.73	28.56	3.46	4.22
Low-Area									
AES-GCM	C-IV	7796	6842	66	63	0.06	0.06	0.01	0.01
Keyak	C-IV	12271	11121	163	111	0.29	0.20	0.02	0.02
AES-GCM	S-IV	2661	2435	130	132	0.12	0.12	0.04	0.05
Keyak	S-IV	4075	3521	176	236	0.32	0.42	0.08	0.12

M→Multi-purpose, D→Dedicated, C→Cyclone, S→Stratix

Plot for multi-purpose cores



Plot for multi-purpose and dedicated cores



Conclusions

- Our multi-purpose Keccak outperforms our multi-purpose AES in terms of throughput over area by an average of 4.0.
- In Keyak mode our multi-purpose Keccak reaches 28.732 Gbps on Altera Stratix-IV, AES-GCM 5.586 Gbps.
- 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.