A High-Speed Unified Hardware Architecture for AES and the SHA-3 Candidate Grøstl

Marcin Rogawski **Kris Gaj**

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

15th EUROMICRO Conference on Digital System Design – DSD'12

Outline

Motivation: SHA-3 Contribution

- SHA-3 Competition and evaluation criteria (security, software and **hardware performance, flexibility**)
- Final round candidates: Blake, **Grøstl**, JH, Keccak, Skein

NIST webpage:

"NIST also plans to (...) select the SHA-3 winner later in 2012."

Motivation: Application to IPSec

Protocol	**Security Service Provided**	**Supported Algorithms**
ESP	confidentiality, integrity, and data origin authentication	e.g.: (**AES-CTR** or AES-CBC) and (**HMAC-SHA** or AES-XCBC-MAC)
AH	integrity and data origin authentication	e.g.: **HMAC-SHA** or AES-XCBC-MAC
IKE	negotiates connection parameters	e.g.: DH and AES-PRNG

Motivation: SHA-3 Competition (round 3) - Comprehensive studies

Software benchmarking

- **General CPUs:** eBASH - *Bernstein and Lange*
- **Microcontrollers:** XBX - *Wenzel-Benner and Gräf*

Hardware benchmarking

- **ASICs:** *Guo et al. DSD'11, DATE'12*, *Gürkaynak et al. SHA-3'12*
- **FPGA high-speed:** *Homsirikamol et al. CHES'11*, *Mahboob et al. SHA-3'12*
- **FPGA high-speed:** (embedded-resources) *Sharif et al. ECRYPT II'11*, *Shahid et al. FPT'11*
- **FPGA low-area:** *Kerckhof et al. CARDIS'11*, *Kaps et al. Indocrypt'11*, *Jungk et al. ReConFig'11*

Motivation: SHA-3 candidates - Unique Features

Hash function mode of operation:

- Skein in tree hash mode: *Schorr et al. ReConFig'10*

Hash function and block cipher in a single core:

- Skein and Threefish: *At et al. NTMS'12*
- Fugue (round 2) and AES: *Järvinen SHA-3'10*
- Grøstl-0 (round 2) and AES: *Järvinen SHA-3'10*
- Grøstl (round 3) and AES: [This work]

Methodology 1/2

- Grøstl - Homsirikamol et al. (CHES'11), AES - (Cryptographic Engineering ch.10) - starting points
- `http://cryptography.gmu.edu/athena/index.php?id=source_codes`
- A Coprocessor for authenticated encryption based on HMAC-Grøstl and AES-CTR mode
- FIFO-based interface
- Long messages analysis - comparison to existing designs
- Short messages analysis - application for IPSec (up to 1536 bytes)

Methodology 2/2

- High-speed FPGA devices: Altera (Stratix III and Stratix IV) and Xilinx (Virtex-5 and Virtex-6)
- Low-cost 65nm Altera Cyclone III (previous work comparison)
- Altera Quartus 11.1 and Xilinx ISE 13.1

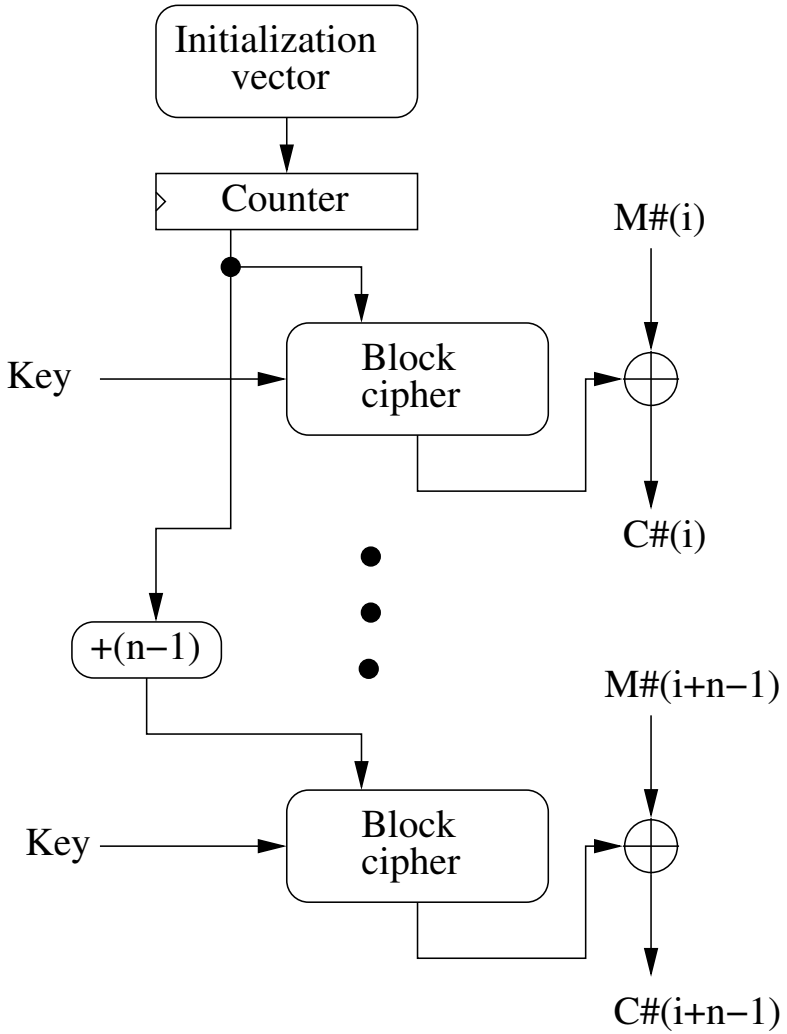
ATHENa – Automated Tool for Hardware EvaluatioN

http://cryptography.gmu.edu/athena

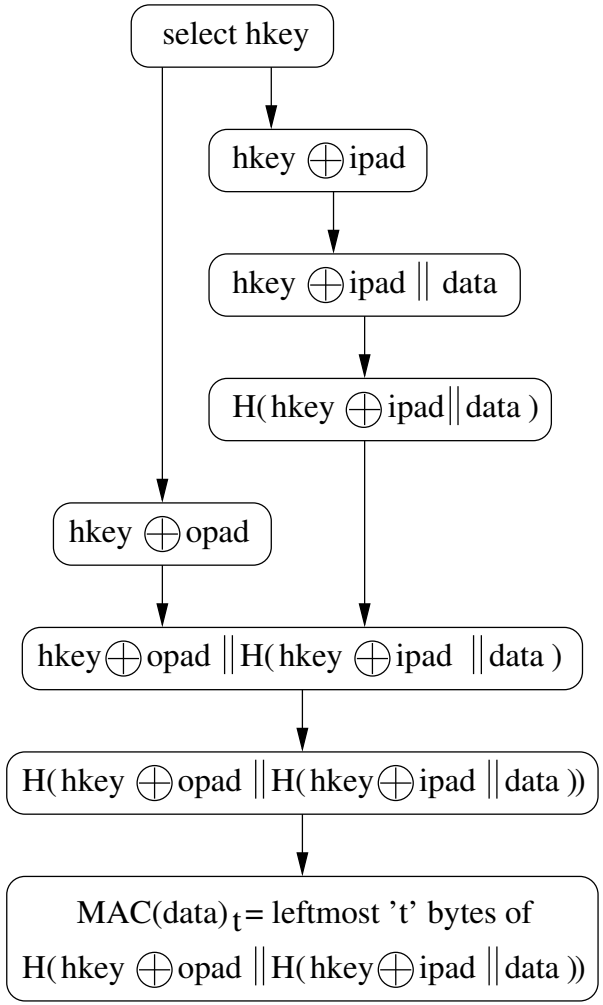
Benchmarking open-source tool, written in Perl, aimed at an AUTOMATED generation of OPTIMIZED results for MULTIPLE hardware platforms

Currently under development at George Mason University.

Block cipher in Counter mode

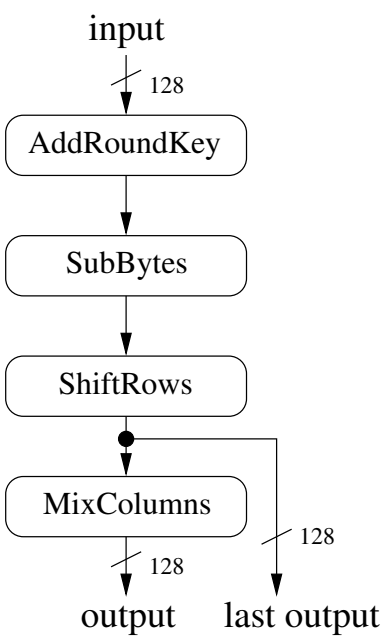


Hash-based message authentication code (HMAC)



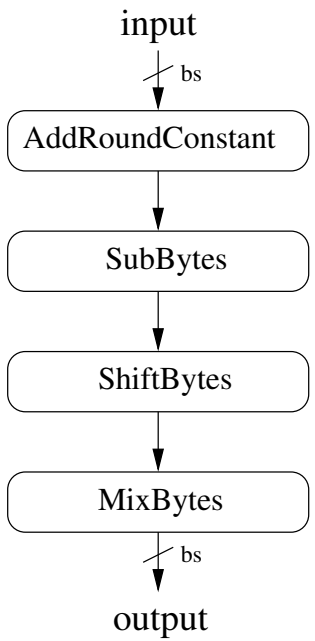
AES and Grøstl rounds

AES round

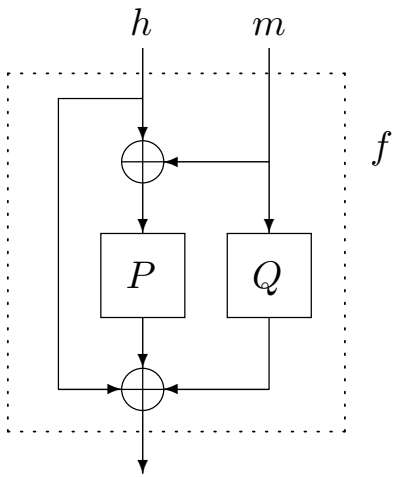


Groestl–256: bs=512

Groestl P/Q transformation



Groestl–512: bs=1024

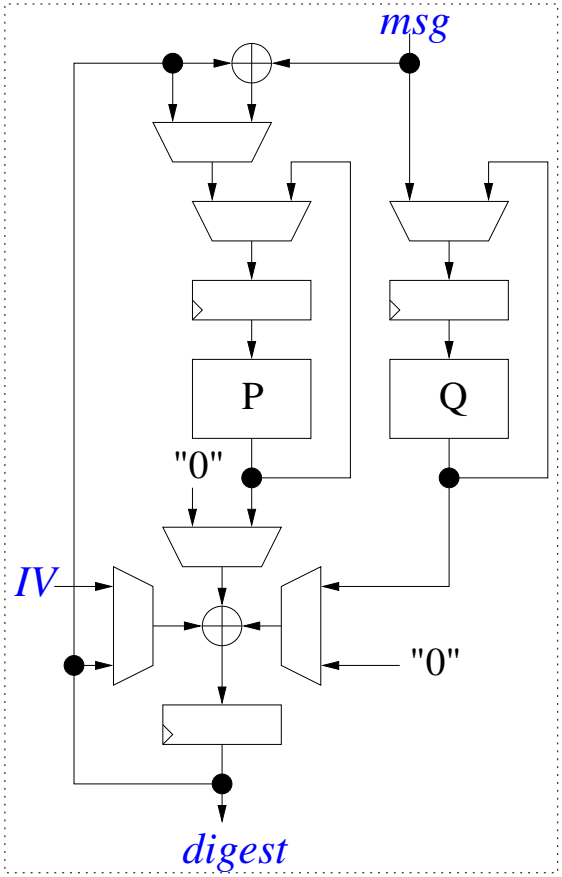


Tweaks on Grøstl (P and Q differences):

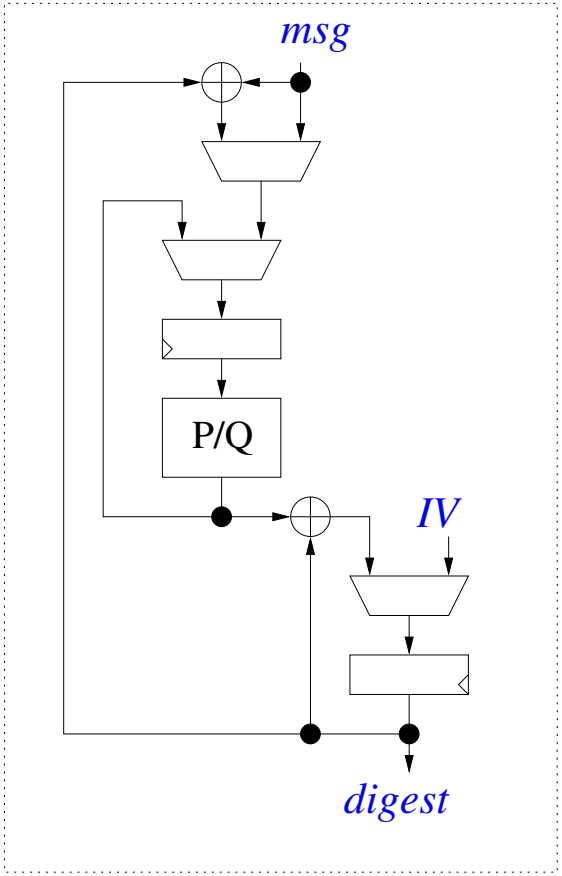
http://www.groestl.info/Round3Mods.pdf

Grøstl's hardware architectures

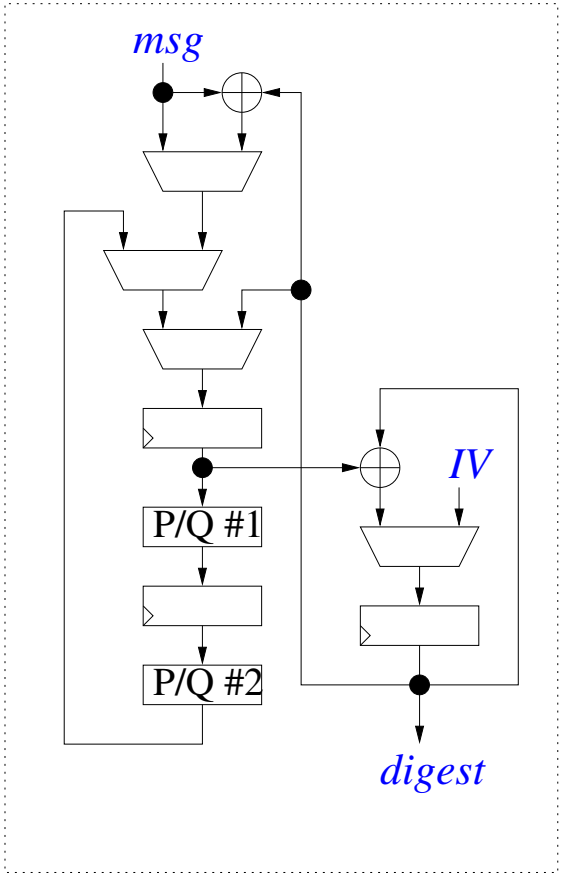
Parallel Architecture



Basic Iterative Architecture
Jarvinen 2010



Quasi-Pipelined Architecture



AES-128 and Grøstl-256

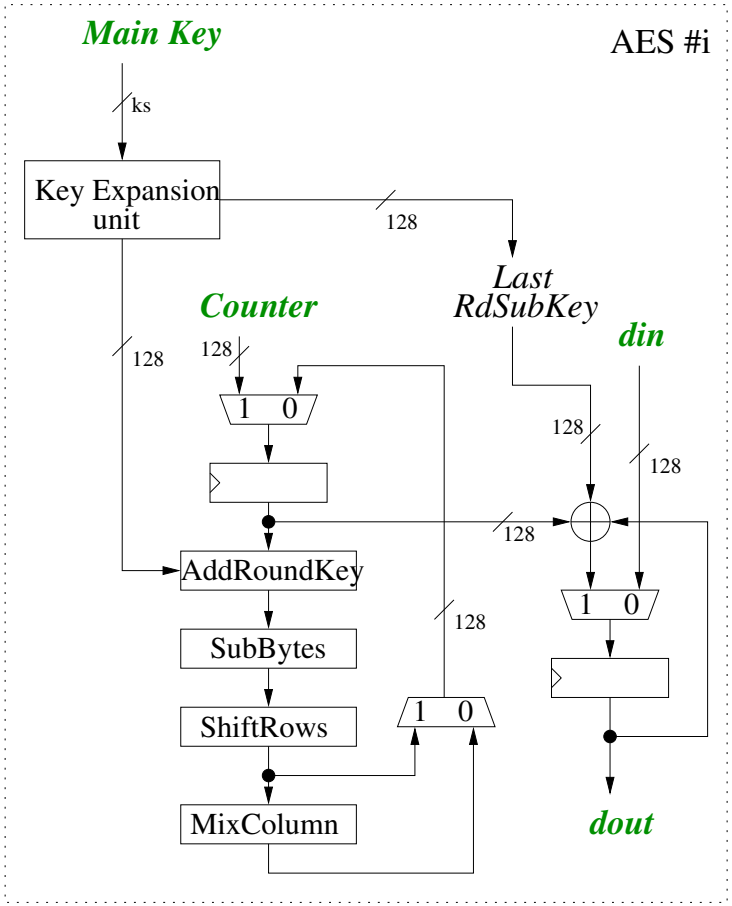
	Grøstl-256	AES-128
functionality	hash function	block cipher
rounds	10	10
block size	512	128[1]
finalization	yes	no[2]
data pipes	double (P and Q)	single [3]

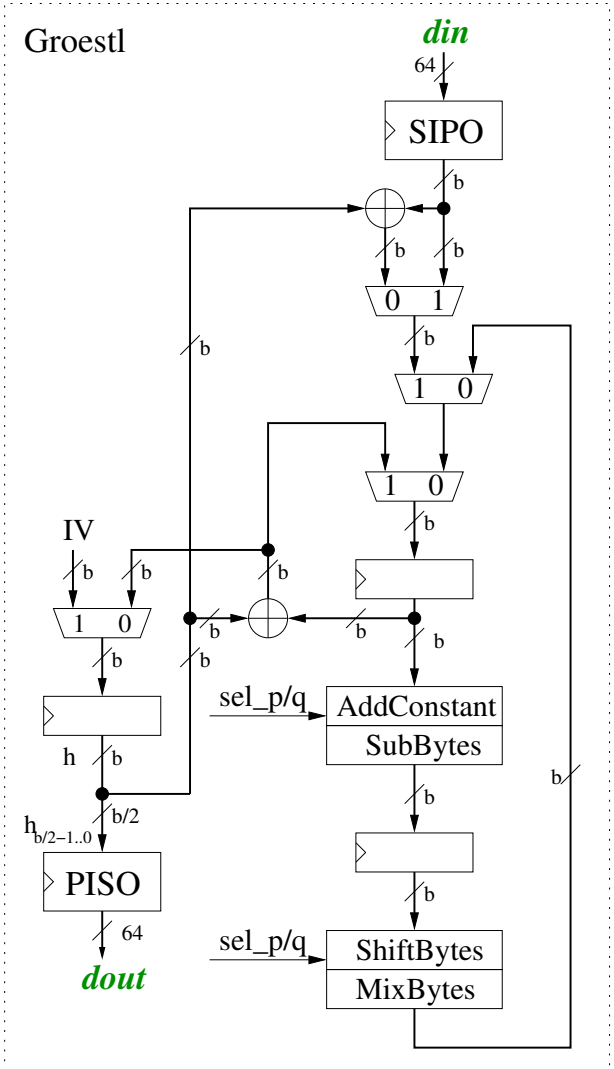
Comments:

[1] four instances of AES in parallel needed (non-feedback modes only), [2] Grøstl's output transformation (finalization) will affect short messages throughput, [3] Grøstl's quasi-pipelined architecture has to be used.

AES/Grøstl together

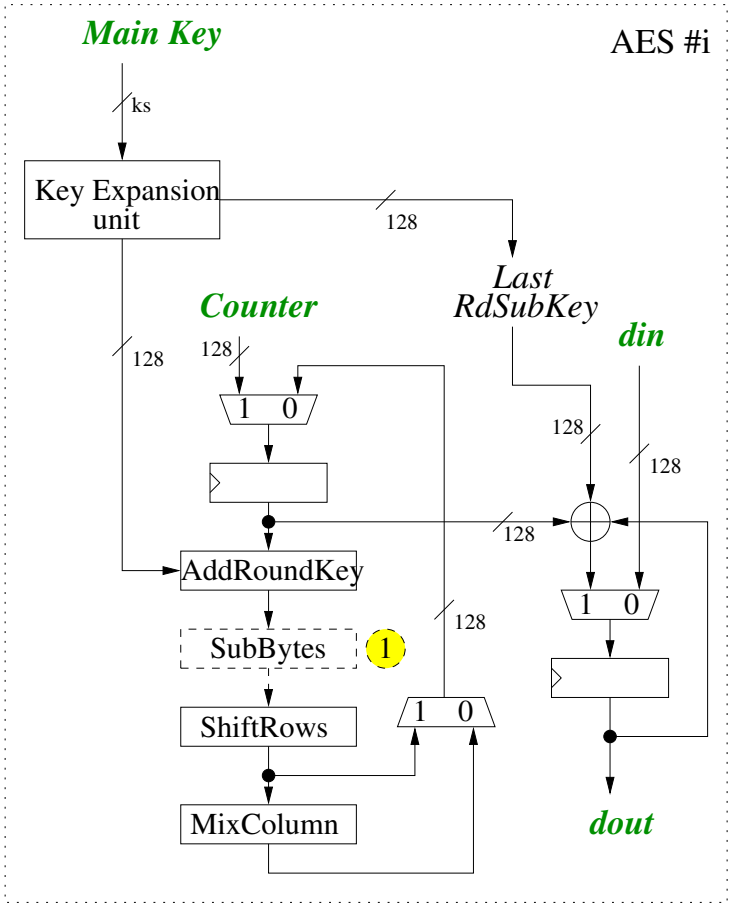
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

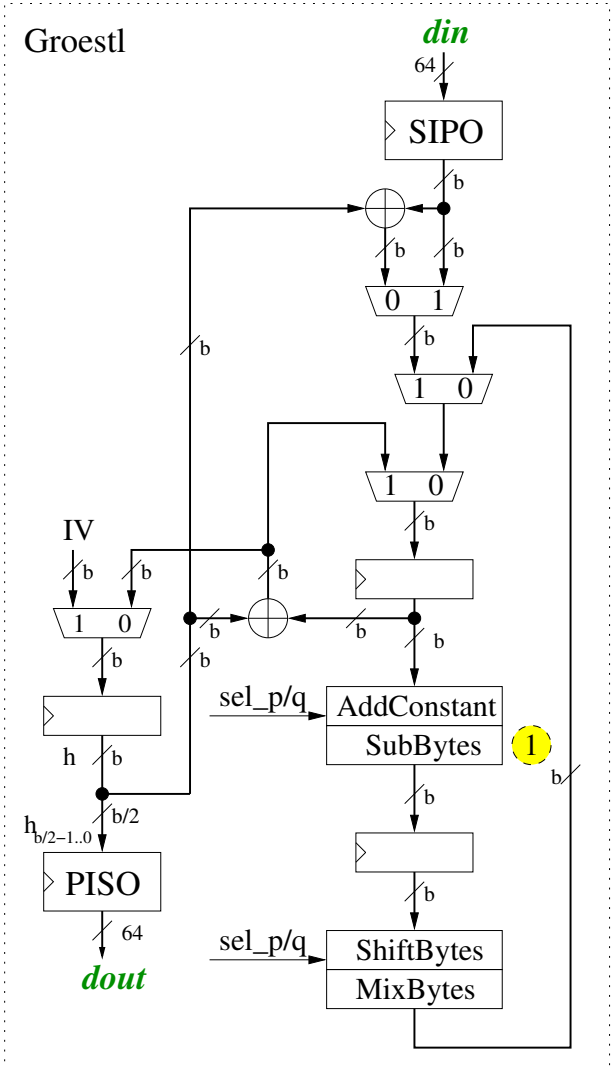




AES/Grøstl together - SubBytes

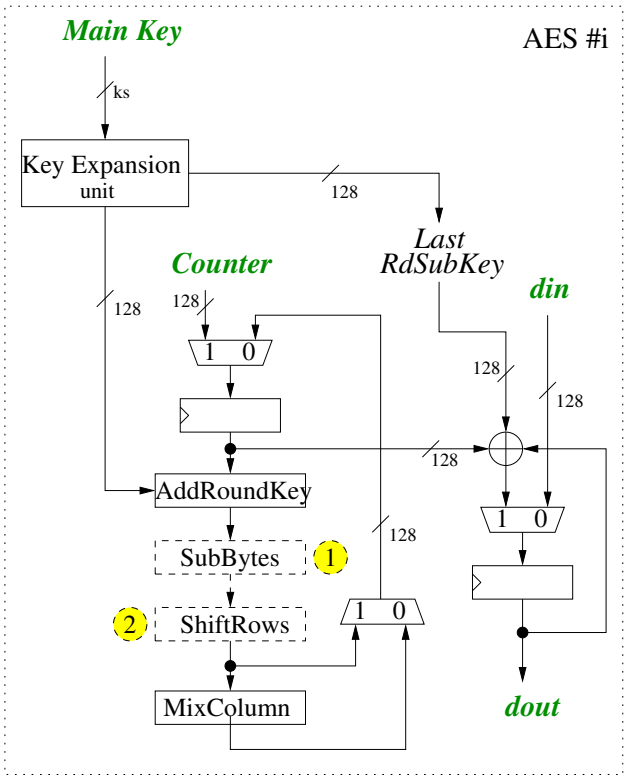
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

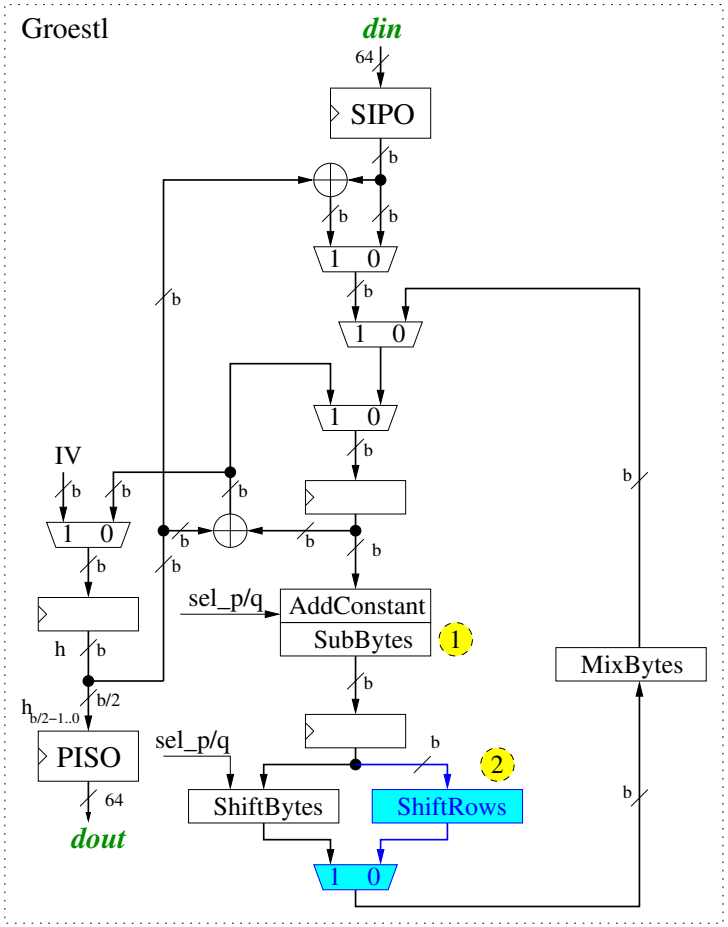




AES/Grøstl together - ShiftRows/ShiftBytes

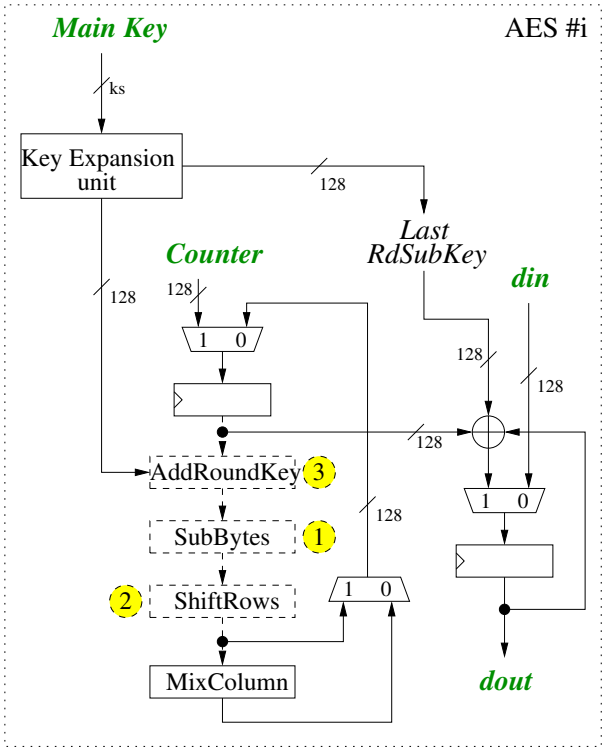
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

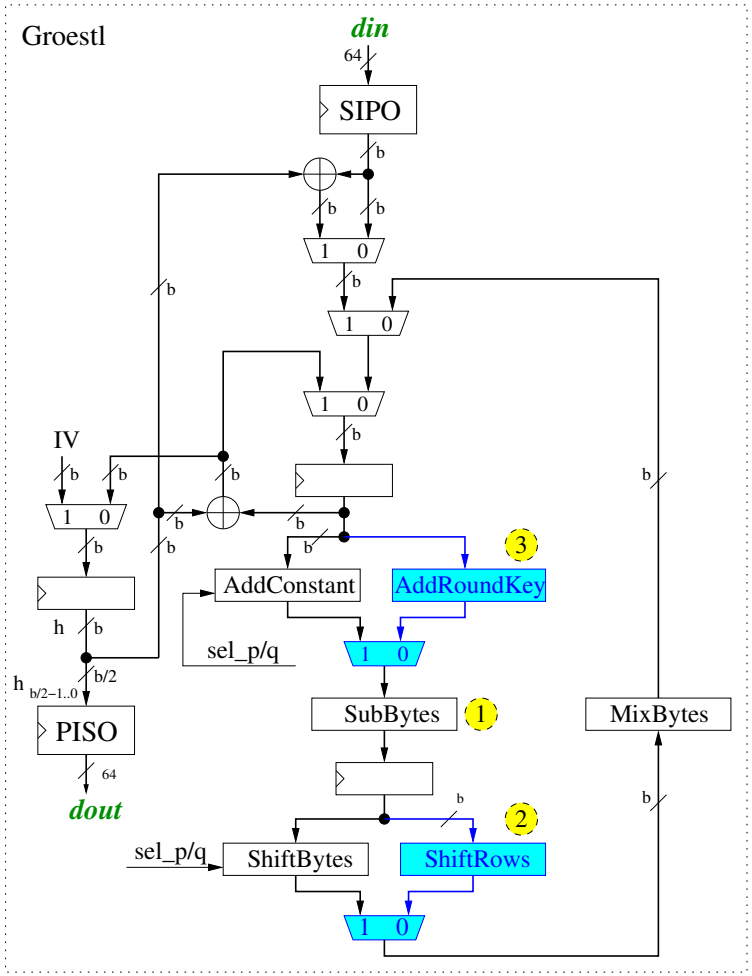




AES/Grøstl together - AddRoundKey/AddConstant

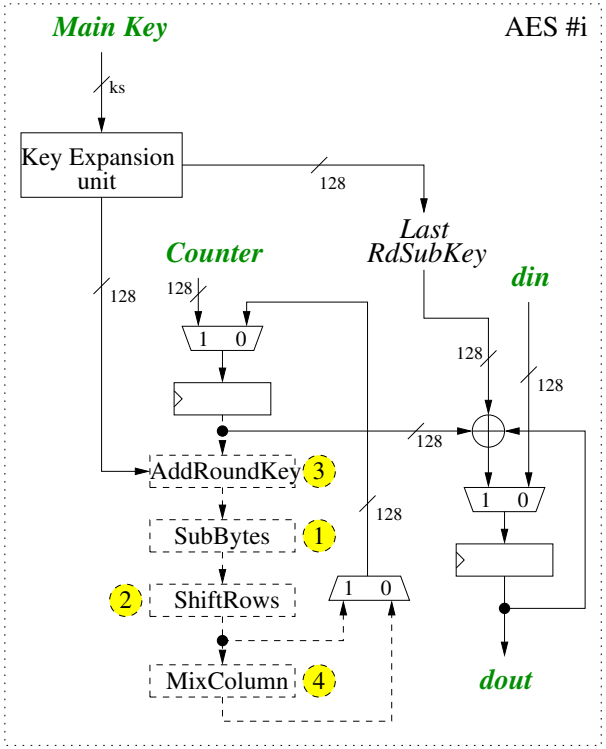
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

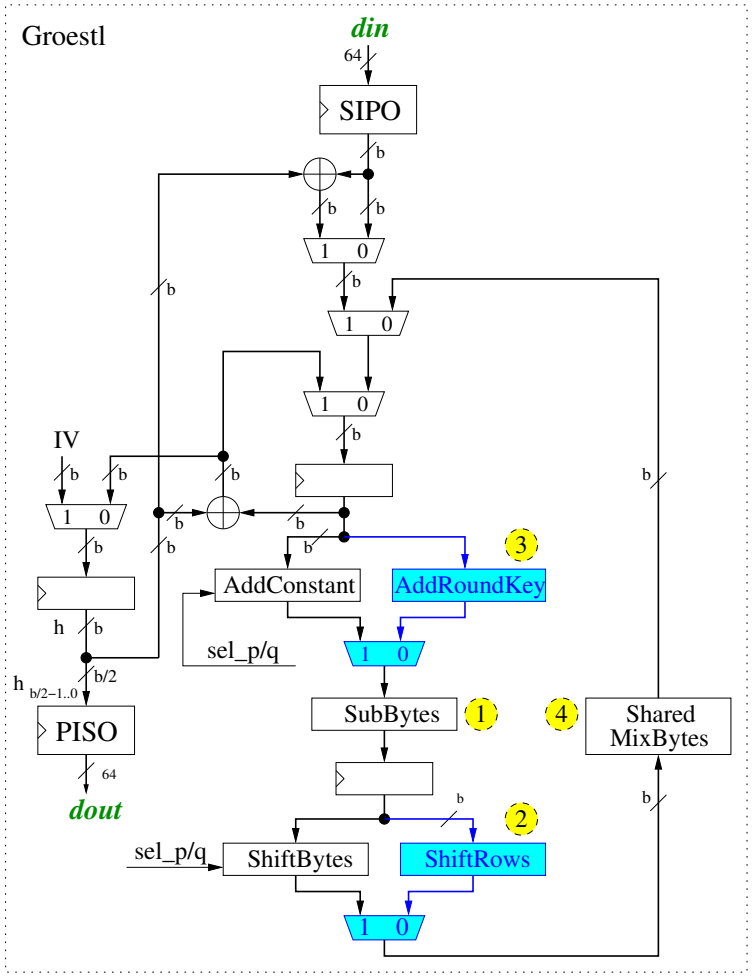




AES/Grøstl together - MixColumn/MixBytes

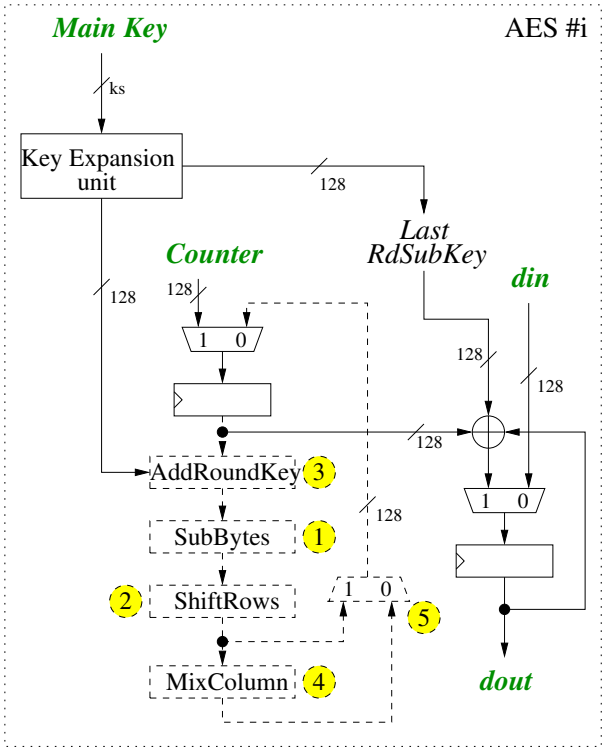
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

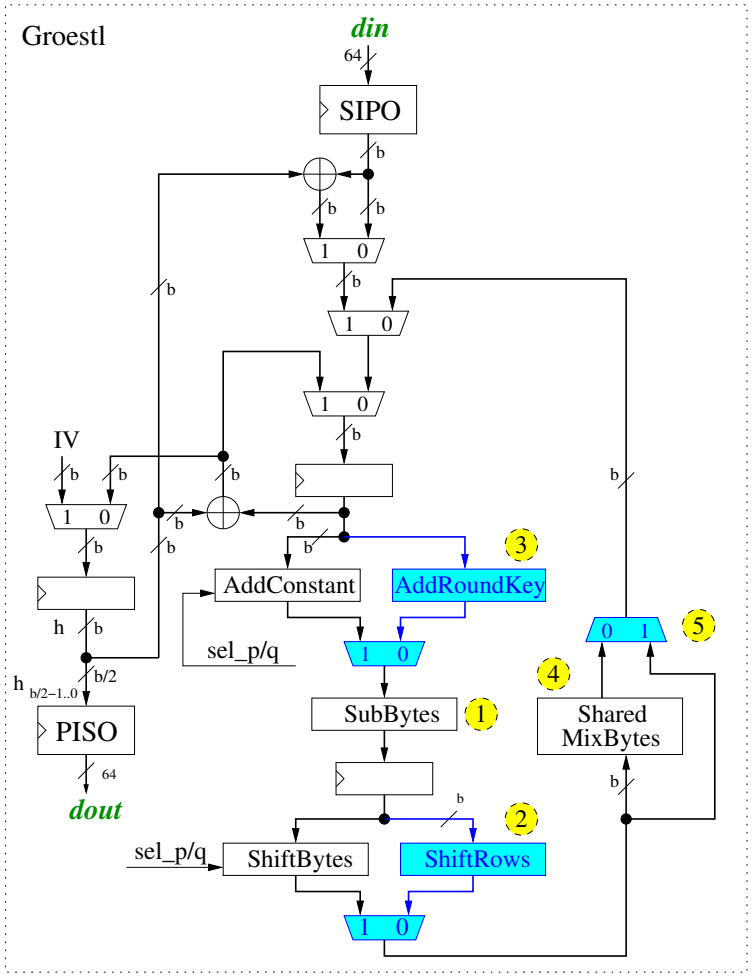




AES/Grøstl together - AES last round

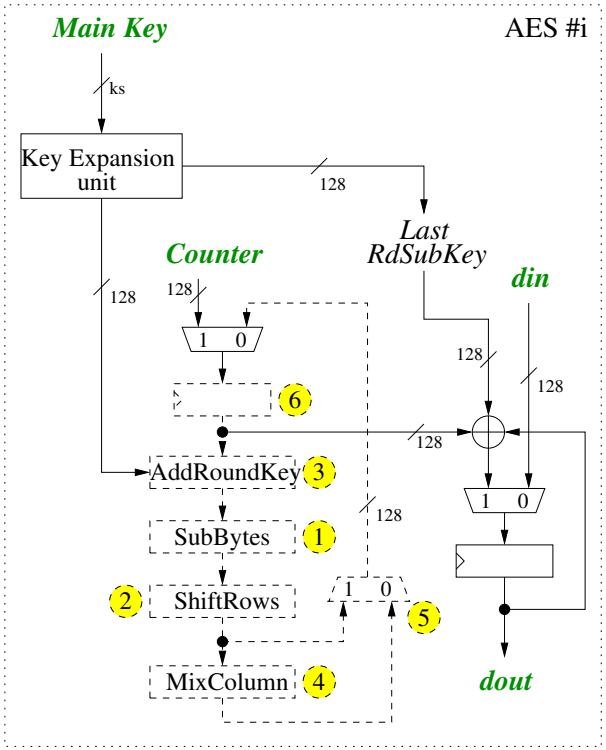
Groestl–256 :	b=512, AES–128, ks=128
Groestl–512 :	b=1024, AES–256, ks=256

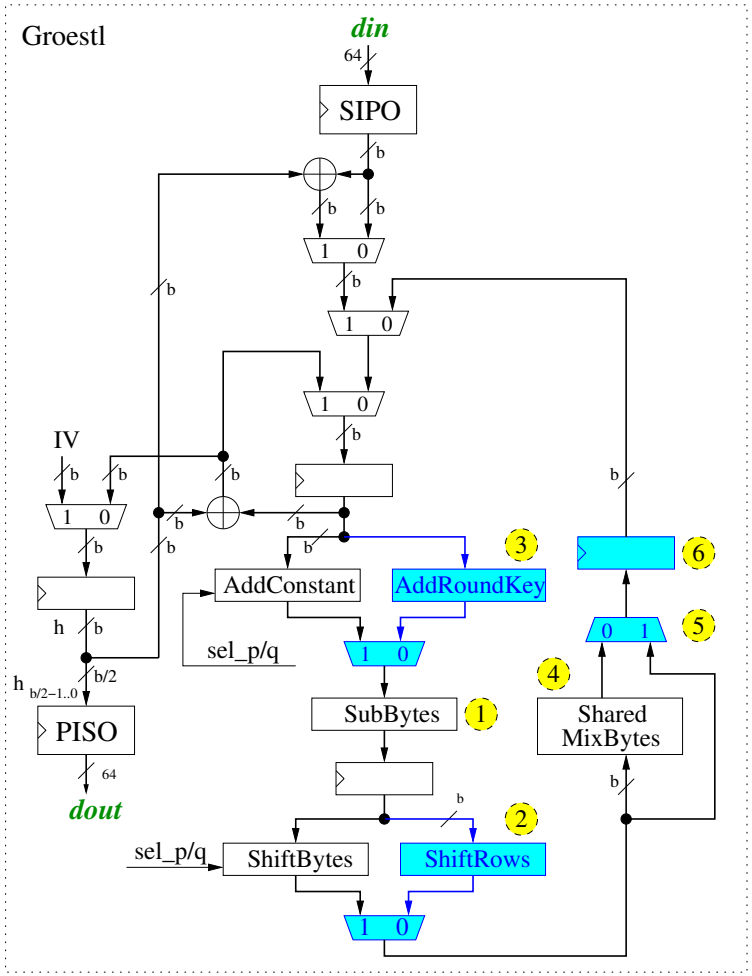




AES/Grøstl together - 3rd pipeline stage

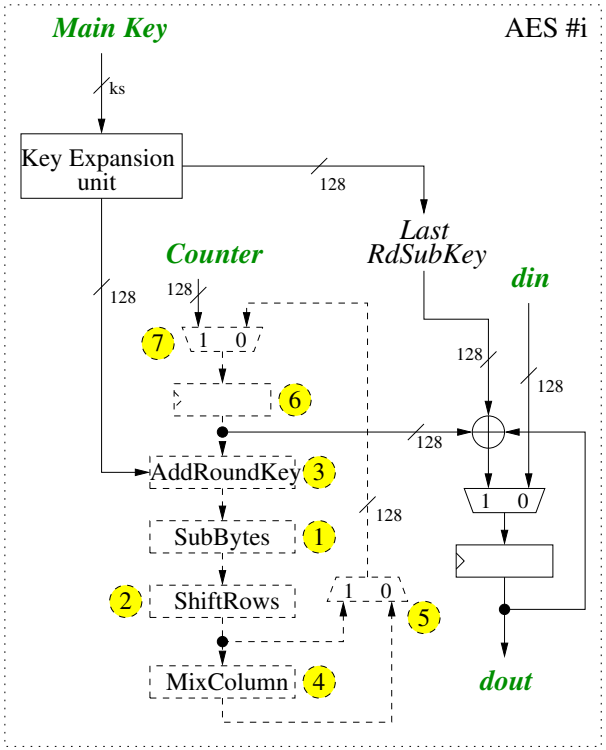
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

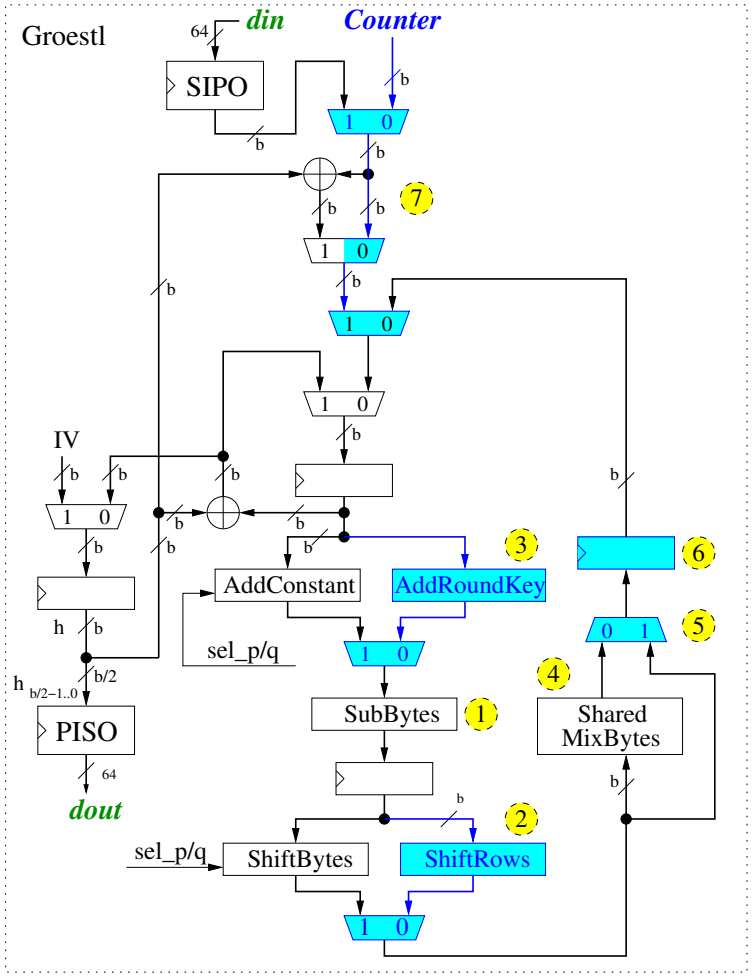




AES/Grøstl together - The Counter from AES-CTR

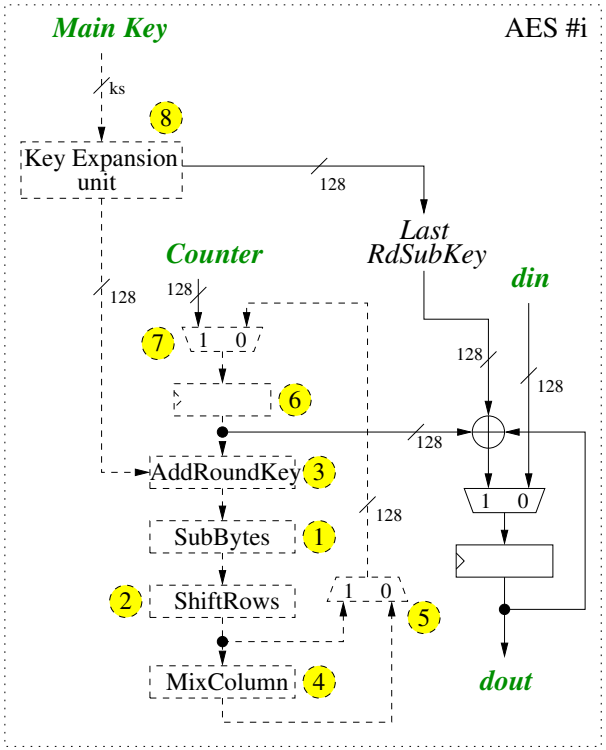
Groestl–256 : b=512, AES–128, ks=128
Groestl–512 : b=1024, AES–256, ks=256

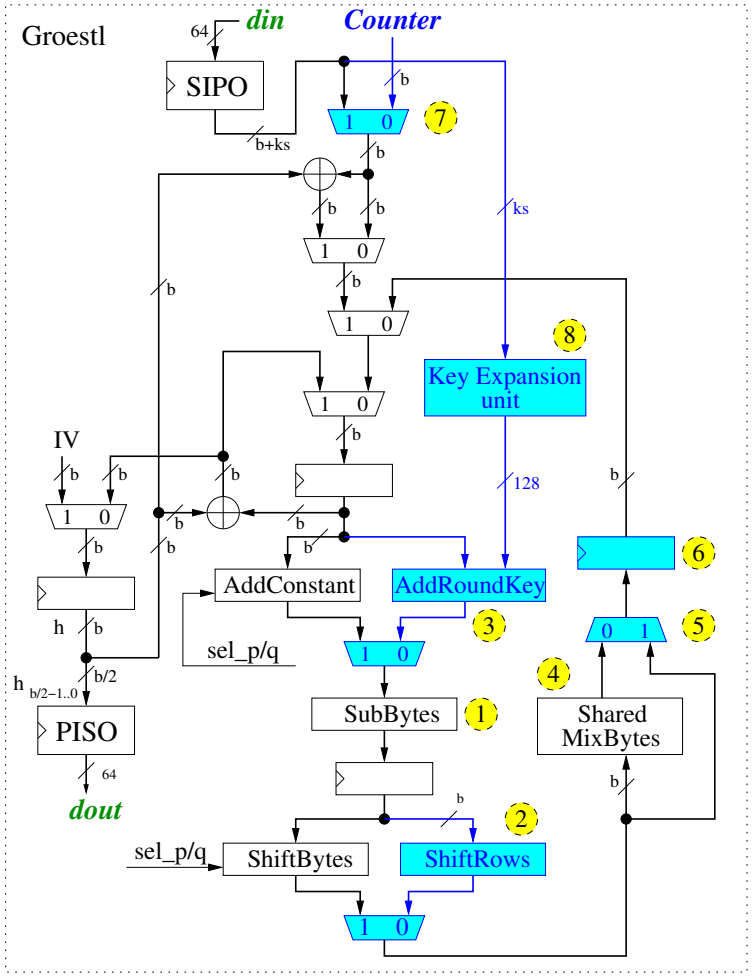




AES/Grøstl together - The AES Key Expansion Unit

Groestl–256 :	b=512, AES–128, ks=128
Groestl–512 :	b=1024, AES–256, ks=256

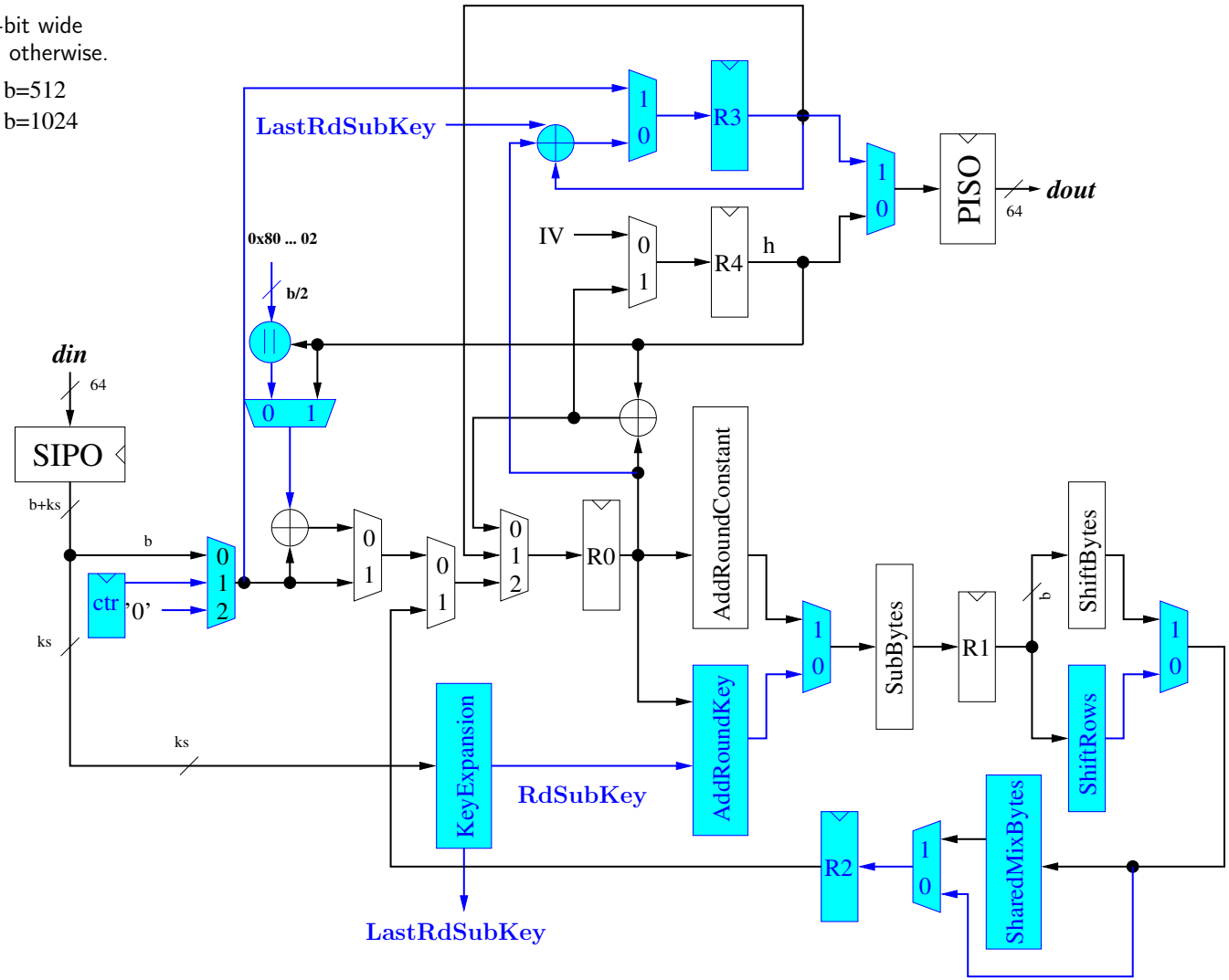




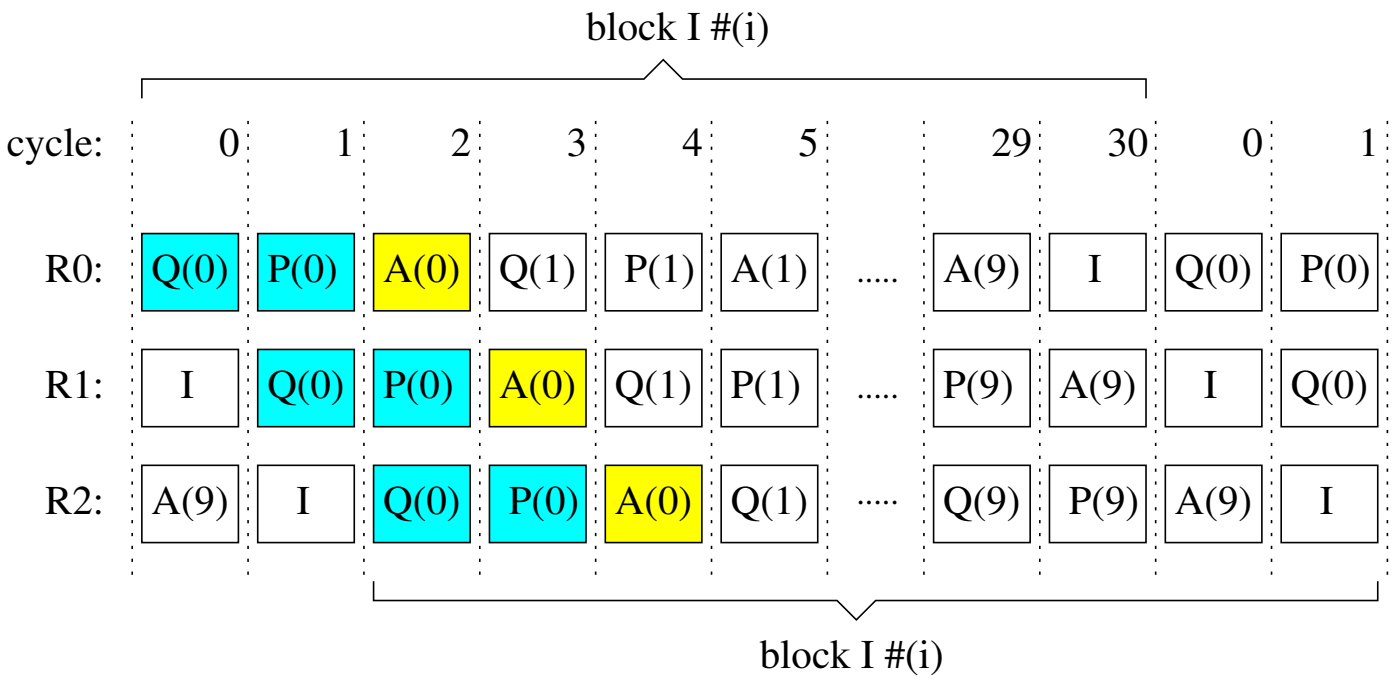
AES/Grøstl together - Proposed Design

All buses are b-bit wide unless specified otherwise.

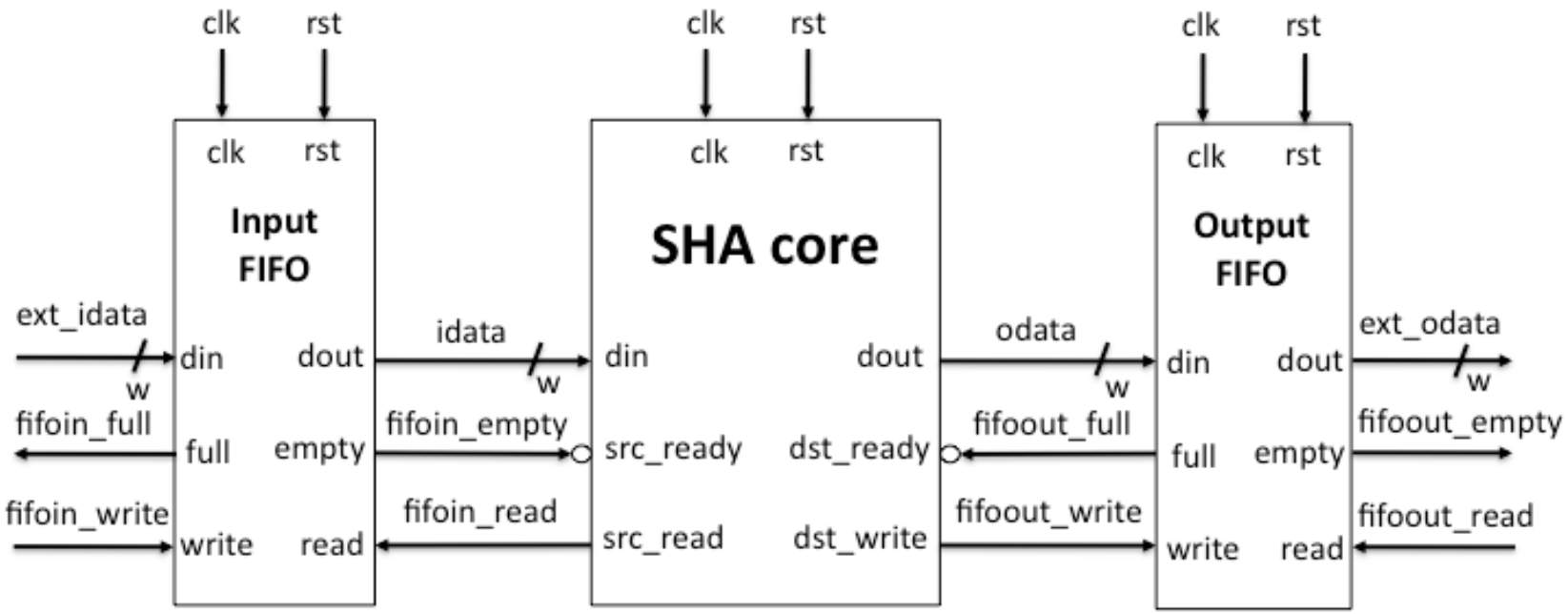
Groestl–256 : b=512
Groestl–512 : b=1024
AES: ks=b/4



Inner Pipelining (Receiver side)

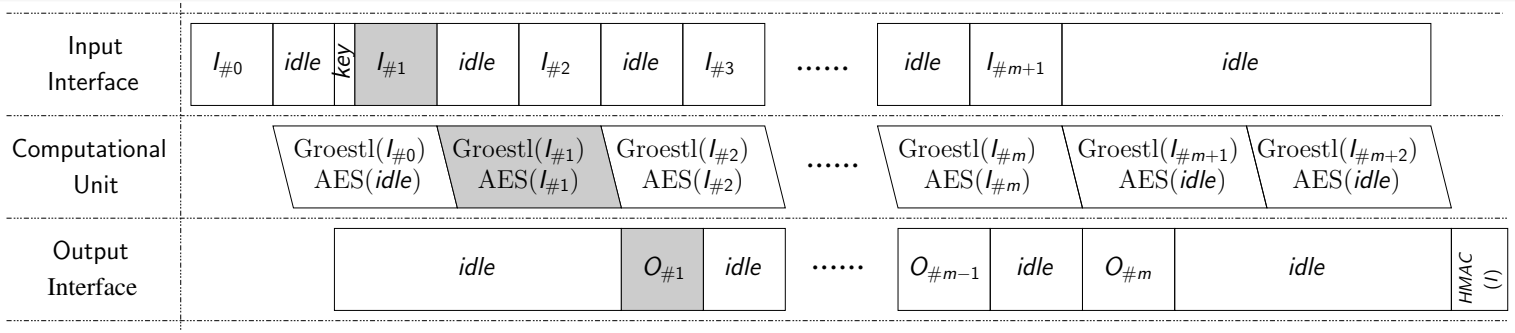


Core Interface



High-level scheduling

Receiver



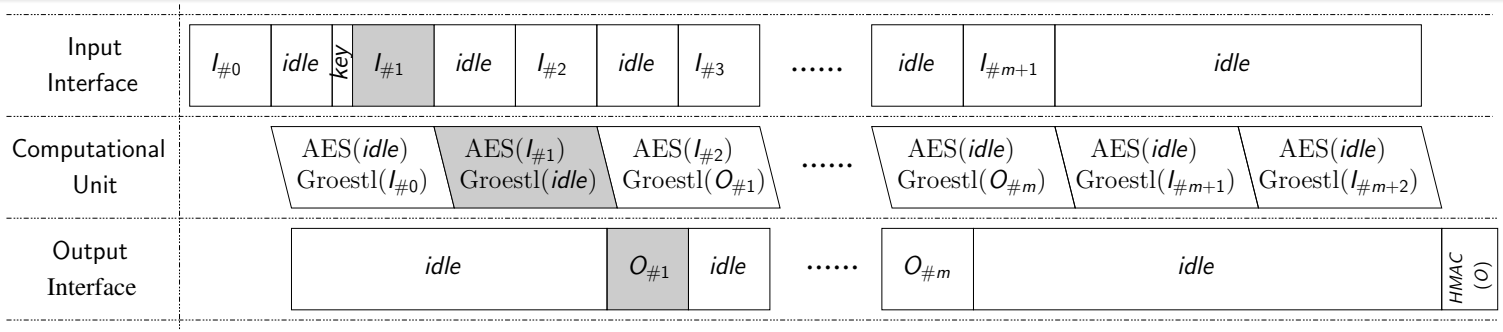
$I_{\#0} = \text{ipad} \oplus \text{hkey}$
$I_{\#m+1} = \text{opad} \oplus \text{hkey}$
$I_{\#m+2} = \text{H}(\text{ipad} \oplus \text{hkey} \,||\, \text{I})$

Ciphertext $= I_{\#1}, I_{\#2}, ..., I_{\#m}$
Plaintext $= O_{\#1}, O_{\#2}, ..., O_{\#m}$

HMAC(I) - HMAC value for a given ciphertext I

Groestl-256: 512-bit input block
Groestl-512: 1024-bit input block

Sender



$I_{\#0} = \text{ipad} \oplus \text{hkey}$
$I_{\#m+1} = \text{opad} \oplus \text{hkey}$
$I_{\#m+2} = \text{H}(\text{ipad} \oplus \text{hkey} \,||\, \text{O})$

Plaintext $= I_{\#1}, I_{\#2}, ..., I_{\#m}$
Ciphertext $= O_{\#1}, O_{\#2}, ..., O_{\#m}$

HMAC(O) - HMAC value for a given ciphertext O

Groestl-256: 512-bit input block
Groestl-512: 1024-bit input block

Throughput for long messages

$$throughput = \frac{blocksize}{T * (Time_{HE}(N+1) - Time_{HE}(N))} \quad (1)$$

$$throughput_{long} = \frac{blocksize}{cycles * T} \quad (2)$$

HMAC-Grøstl-256 and AES-128-CTR core parameters:

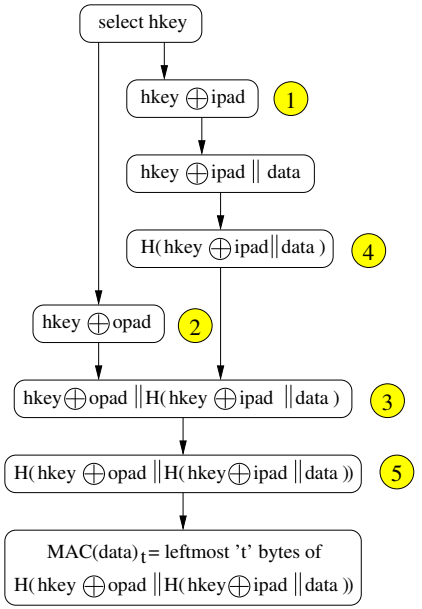
block size = 512, cycles = 31

$Time_{HE}(i)$ - time for Hash/Encryption process of i-th block of data

HMAC-Grøstl - Throughput for short messages

$$\frac{throughput_{HMAC/Grøstl}}{throughput_{Grøstl}} = \frac{\#blocks}{5 + \#blocks} \quad (3)$$

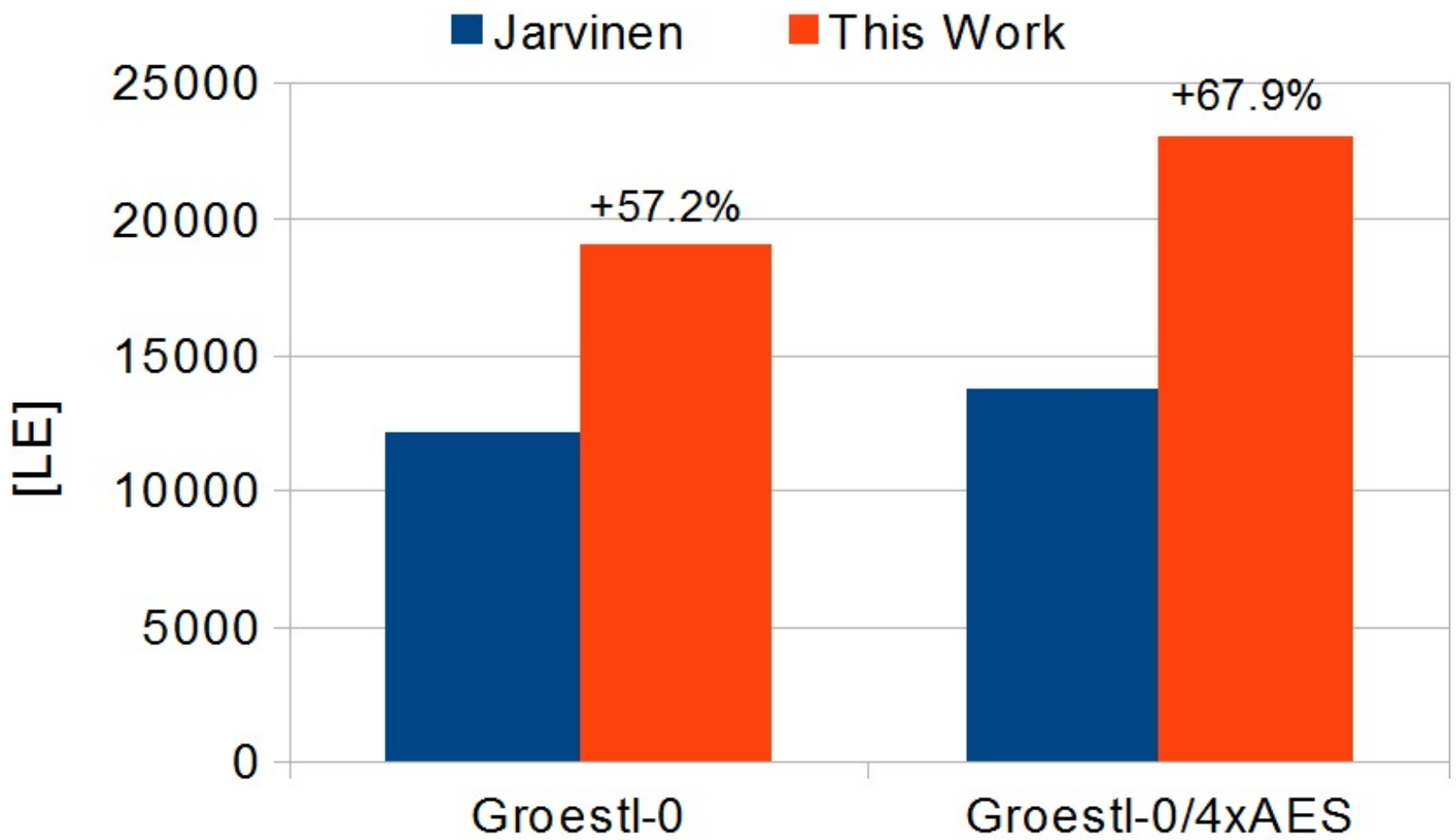
$$throughput = \frac{blocksize * \#blocks}{(5 + \#blocks) * (cycles * T)} \quad (4)$$



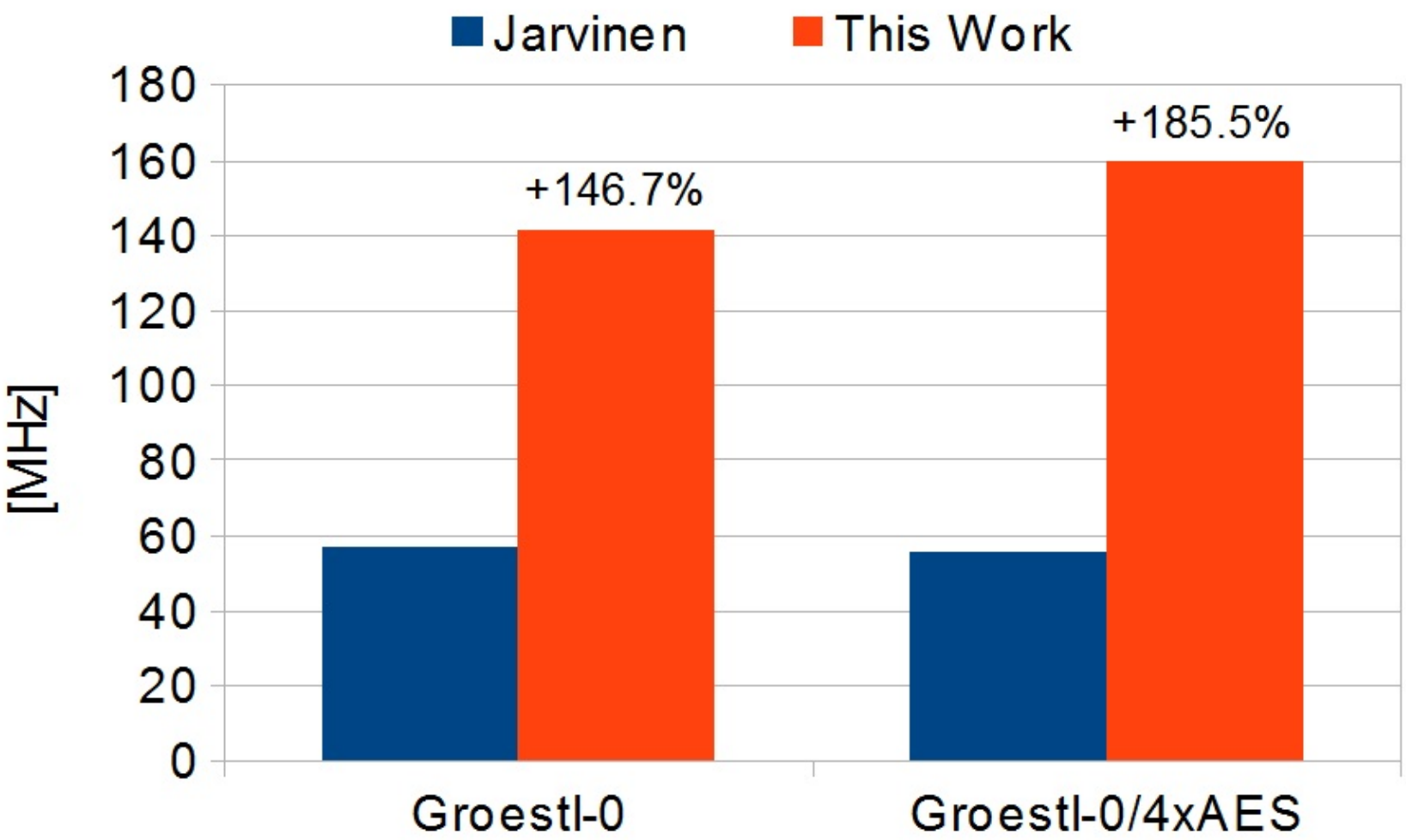
Five additional blocks come from:

Two HMAC-Key injections [1-2], first hashing result [3], Grøstl finalization operation [4-5].

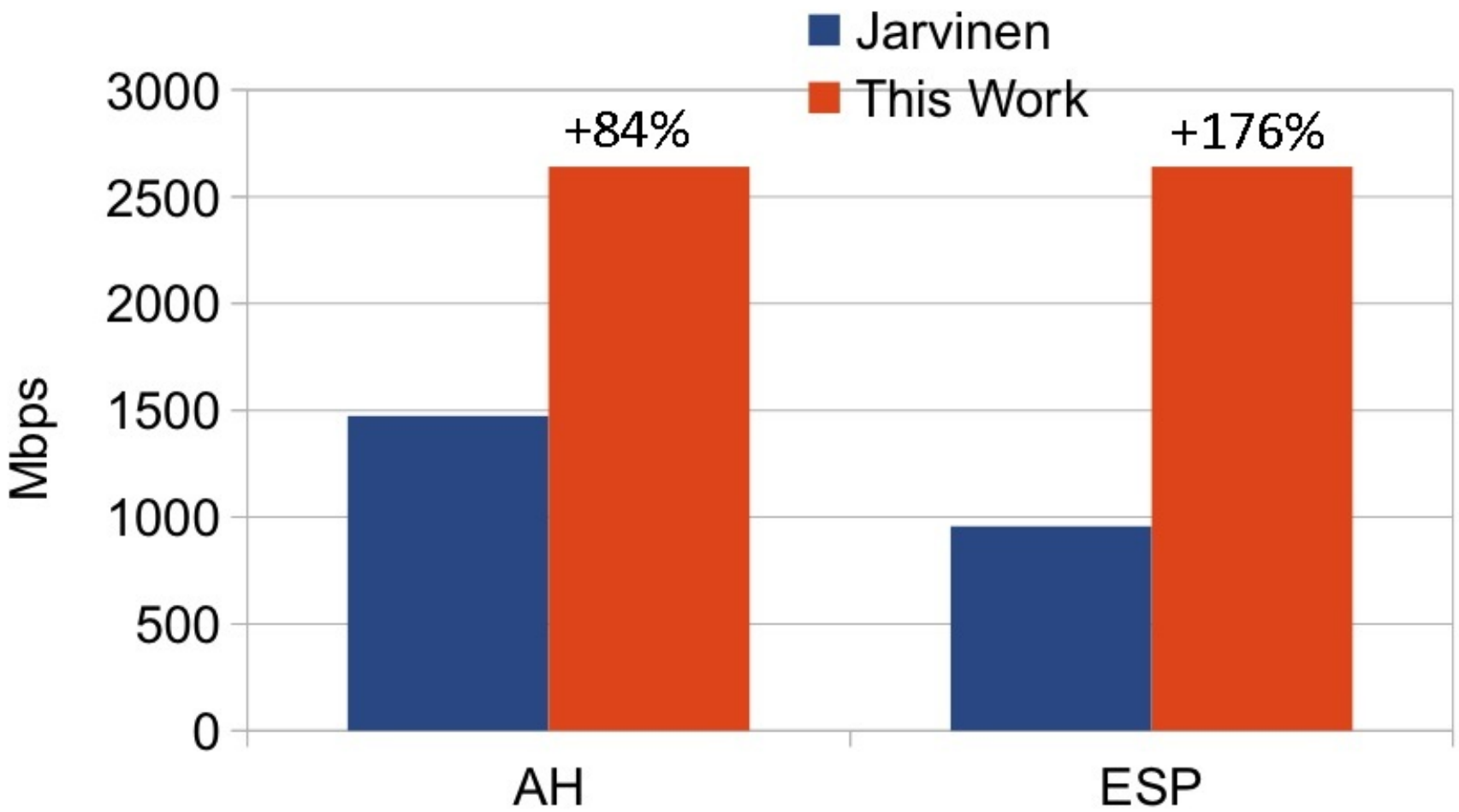
Comparison to Järvinen on Cyclone III - Area



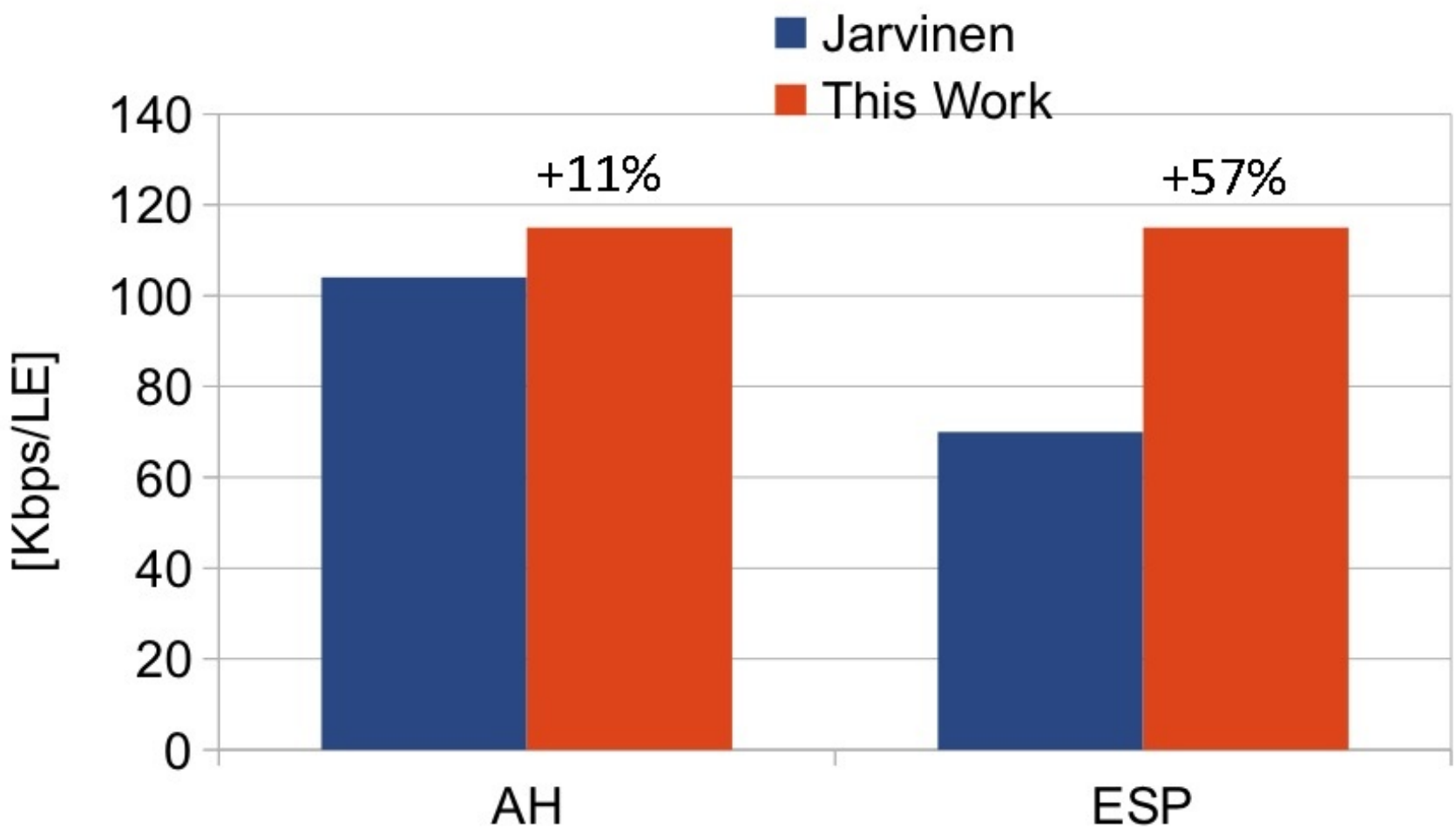
Comparison to Järvinen on Cyclone III - Frequency



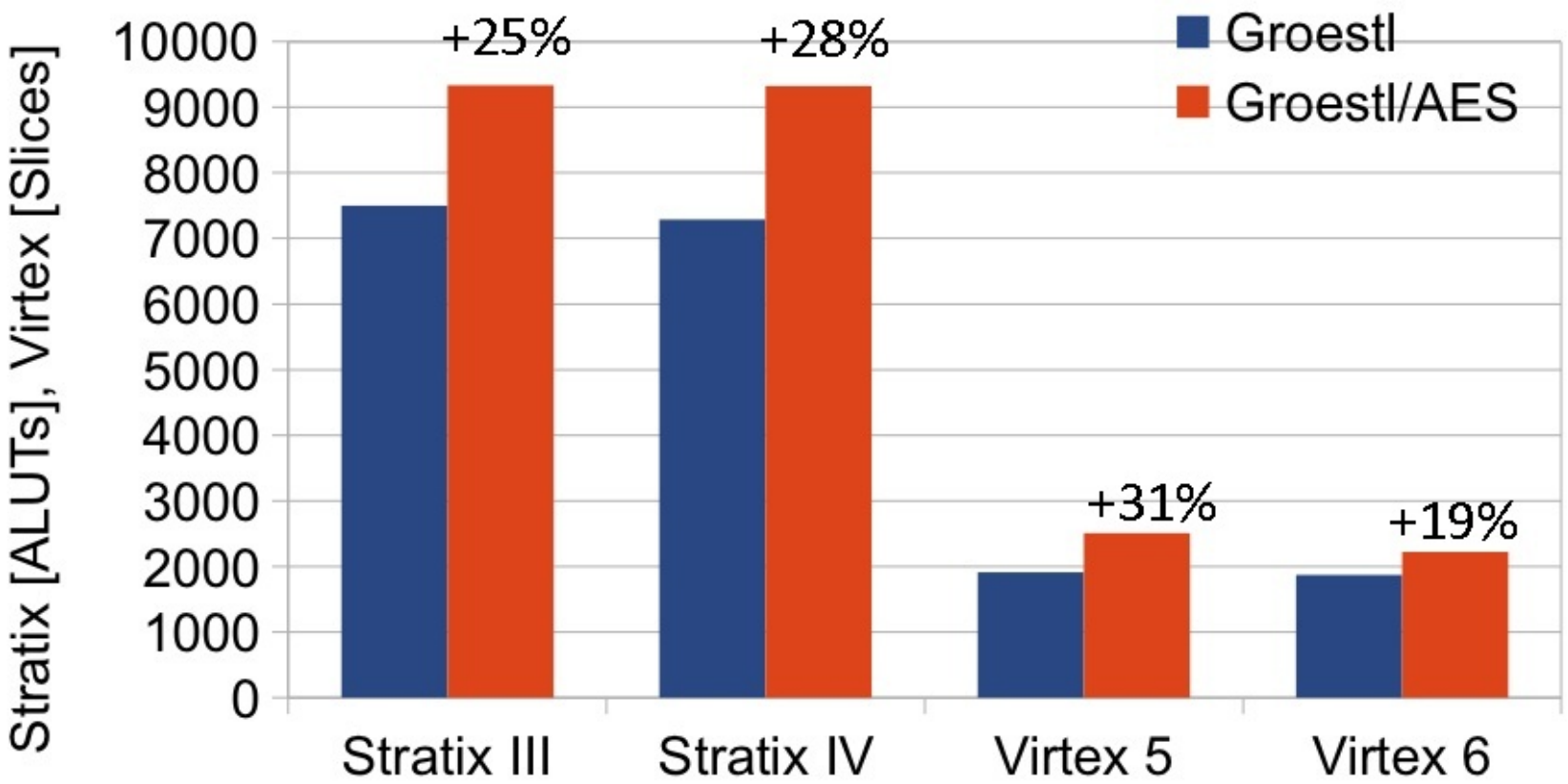
Comparison to Järvinen on Cyclone III - Throughput



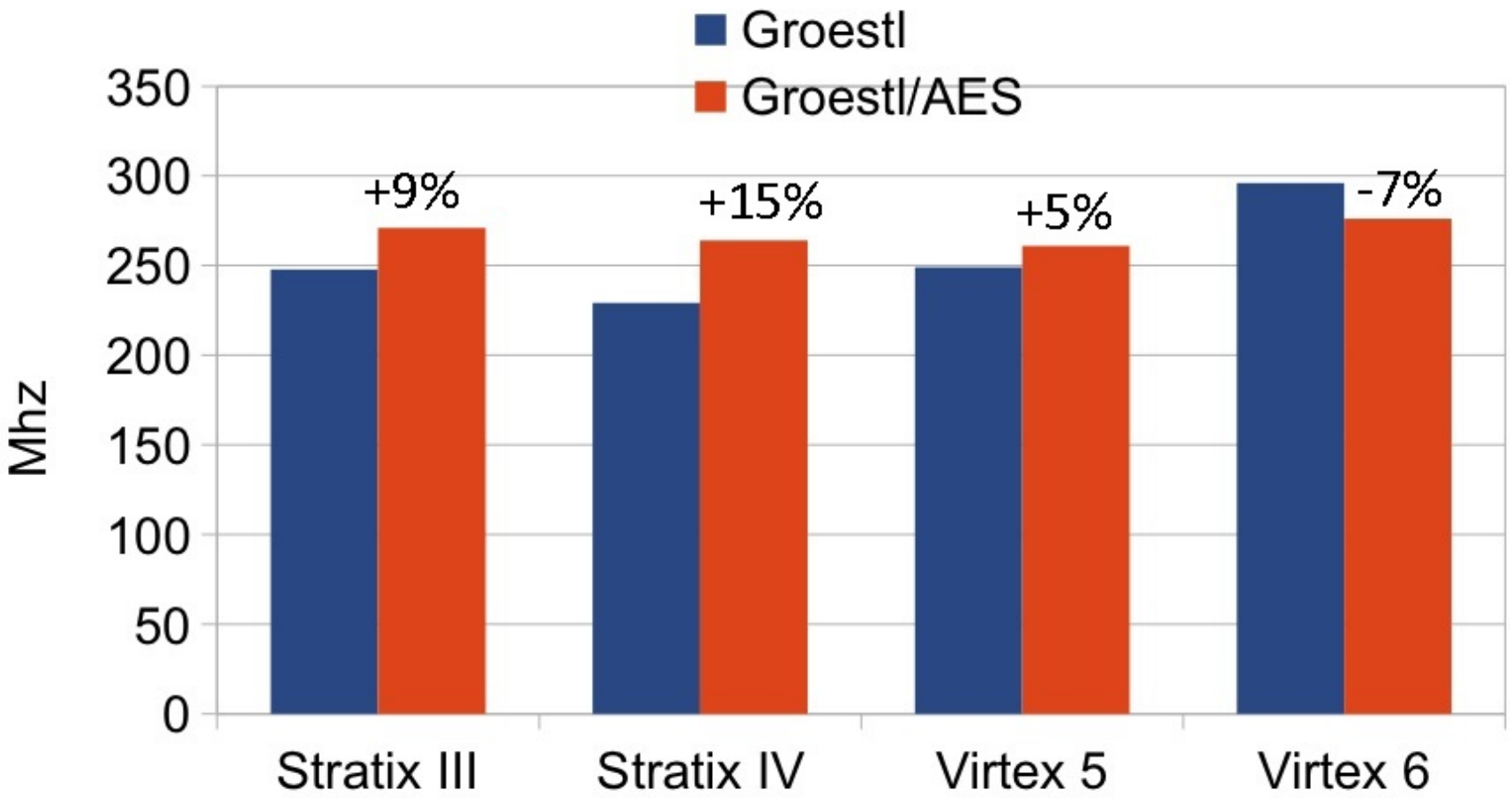
Comparison to Järvinen on Cyclone III - Throughput/Area



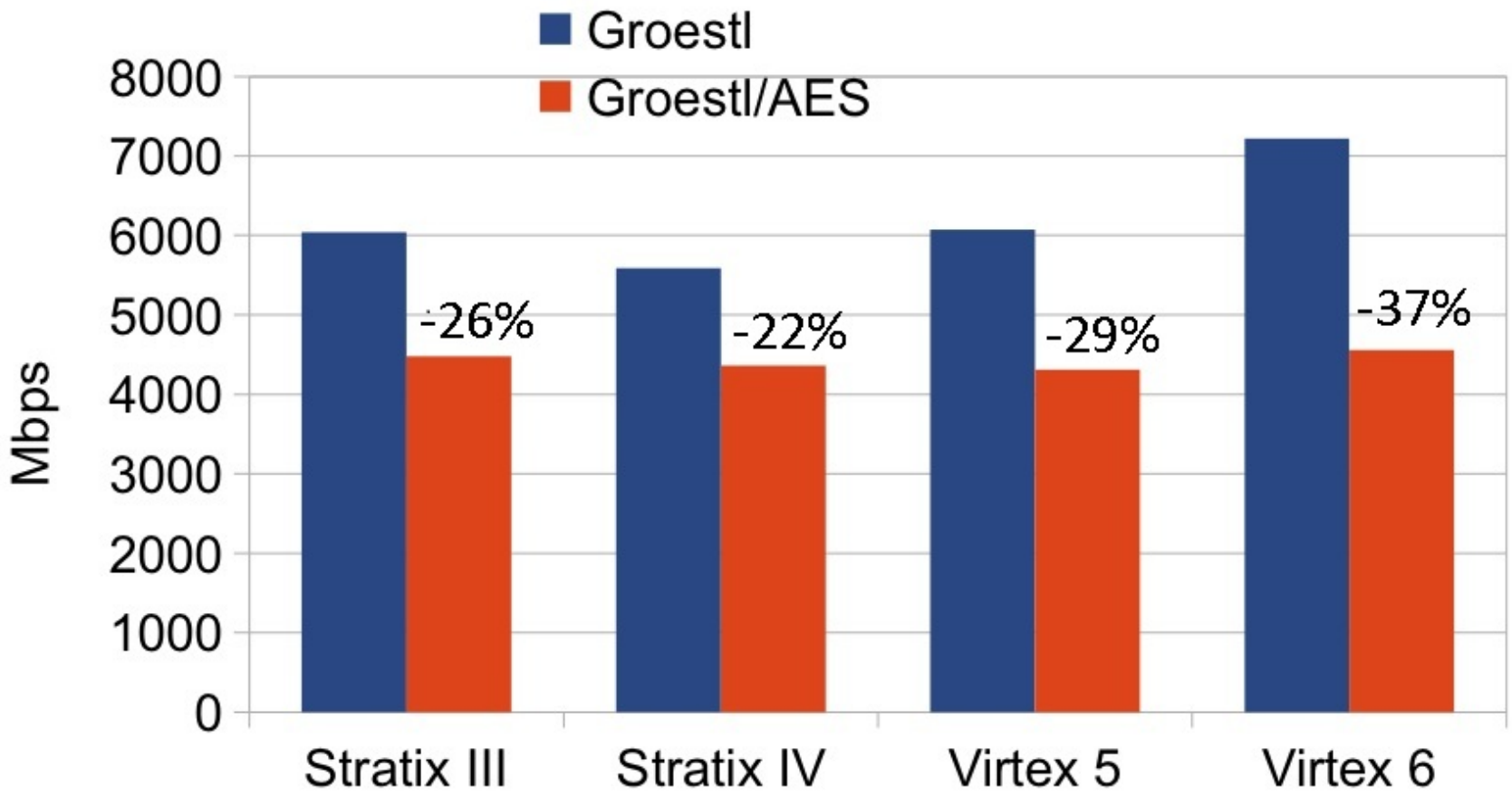
High-Speed FPGA - Area



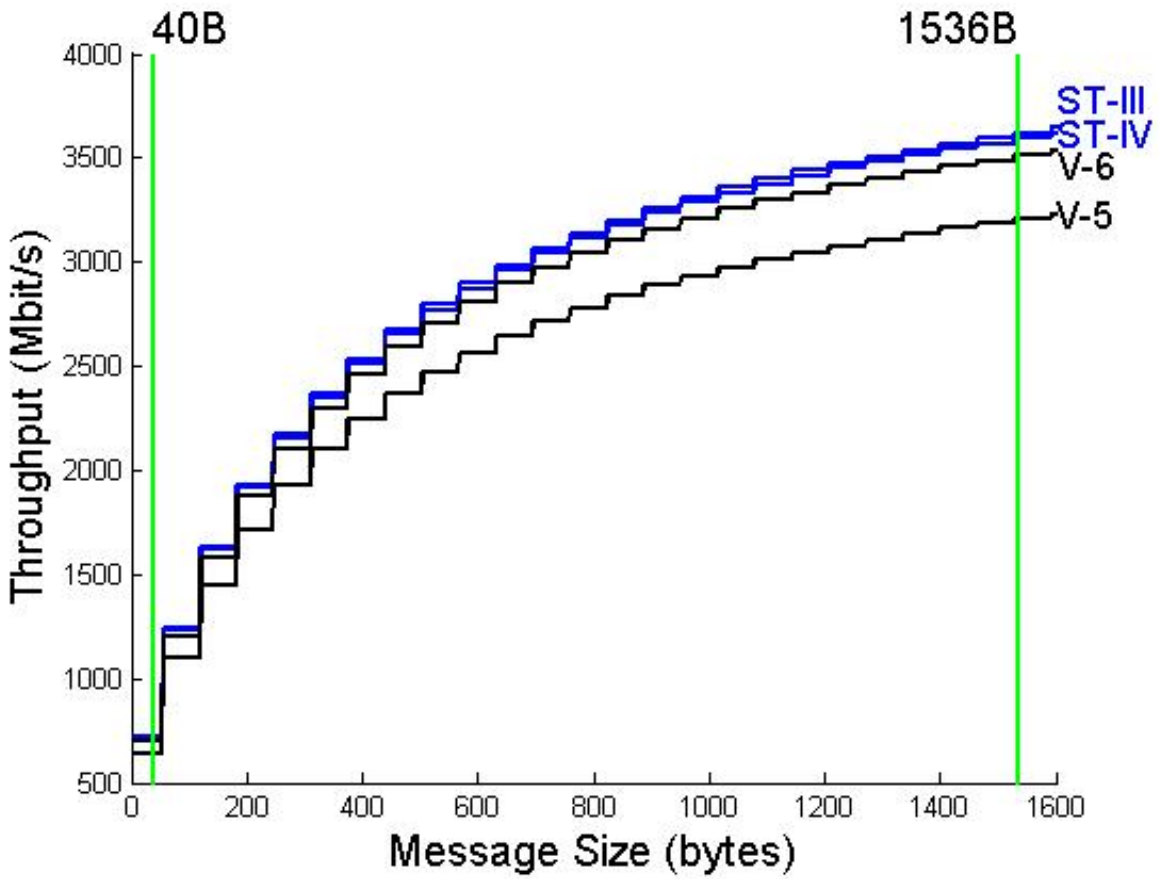
High-Speed FPGA - Frequency



High-Speed FPGA - Throughput for long messages



HMAC-Grøstl for short messages



Conclusions

- Coprocessor with 3 pipeline stages pays relatively small penalty in terms of extra circuitry (+31% in Virtex-5) and throughput drop (-29% in Virtex-5)
- Proposed coprocessor can be used directly for IPSec HMAC-Grøstl with AES-CTR and possibly any non-feedback mode
- It can be implemented even on the smallest device in high-speed families from Altera (Stratix-III, Stratix-IV) and Xilinx (Virtex-5 and Virtex-6)
- Altera Cyclone III-based coprocessor outperform alternative design by 57% and 11% in case of authenticated encryption (ESP) and authentication (AH), respectively
- Grøstl's similarity to AES will be beneficiary in hardware in case of "SHA-3 $\leftarrow$ Grøstl"

Thank you!

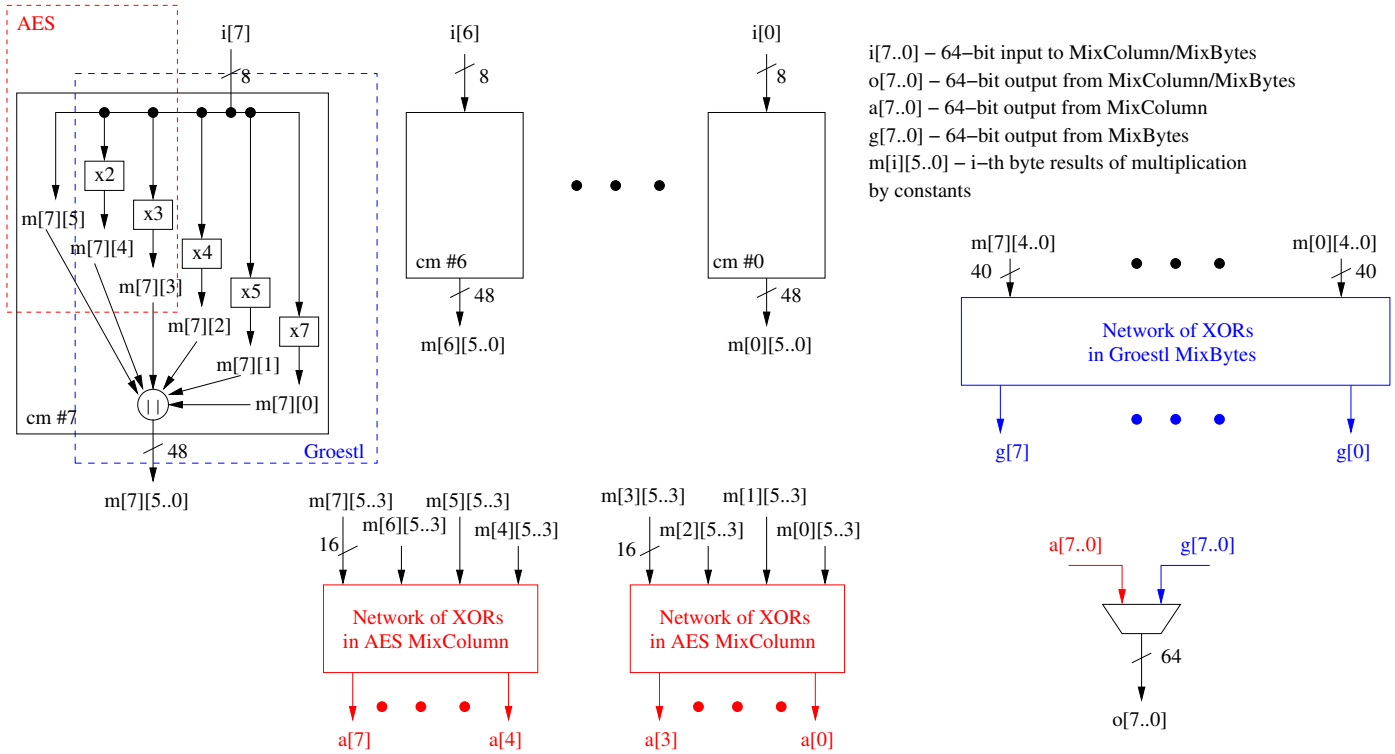
Our resources:

CERG: `https:/cryptography.gmu.edu`
ATHENa: `https:/cryptography.gmu.edu/athena`
ATHENaDB: `https://cryptography.gmu.edu/athenadb`

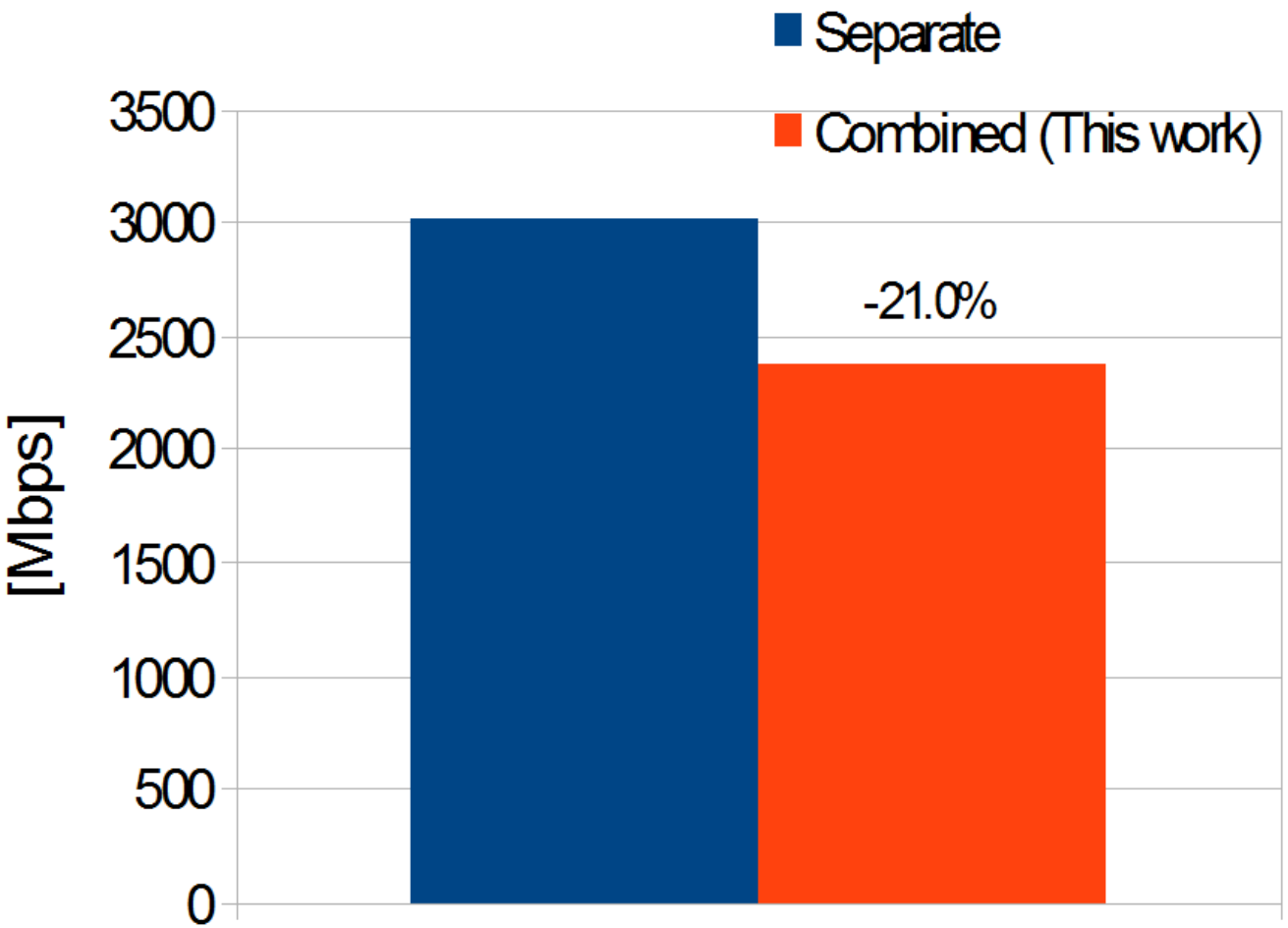
Backup slides

Backup slides from here

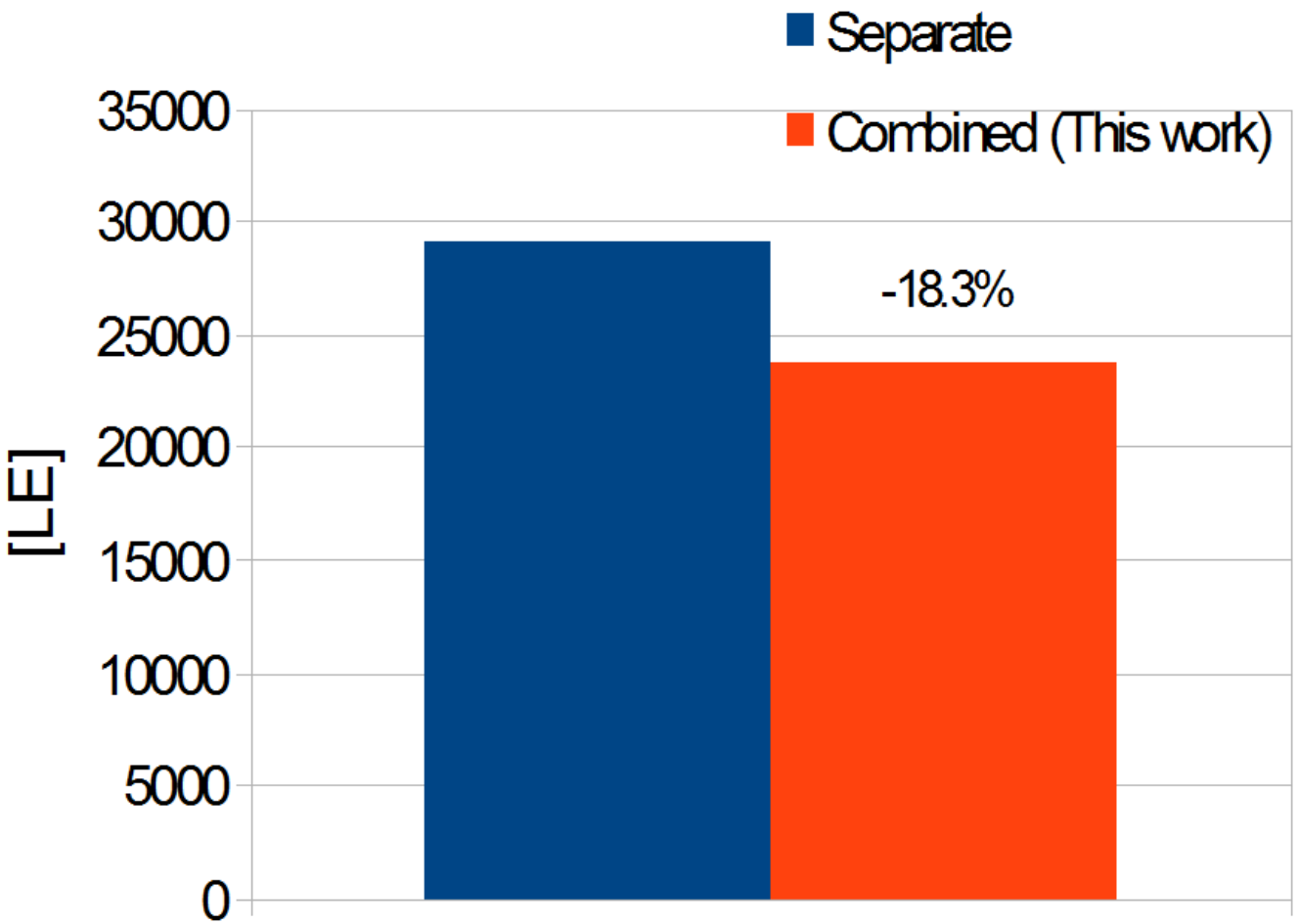
AES/Grøstl together - Shared MixBytes



Comparison to Groestl and 2xAES-CTR Separately on Cyclone III - Throughput



Comparison to Groestl and 2xAES-CTR Separately on Cyclone III - Area



Comparison to Groestl and 2xAES-CTR Separately on Cyclone III - Throughput/Area