Compact Dual Block AES core on FPGA for CCM Protocol

João Carlos C. Resende Ricardo Chaves

TÉCNICO LISBOA

inesc id lisboa

Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode
- State of the Art in AES implementations on FPGA
- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution
- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art
- Conclusions

Digital Security Today

Encryption

Authentication

Integrity

Non-repudiation

Digital Security Today

Encryption

Authentication

Integrity

Non-repudiation

- Ciphers
- Hash functions
- Higher Lvl Protocols

Digital Security Today

Encryption

Authentication

Integrity

Non-repudiation

- Ciphers
- Hash functions
- Higher Lvl Protocols

- Ciphers + Hash
  - 2 cores

Digital Security Today

Encryption

Authentication

Integrity

Non-repudiation

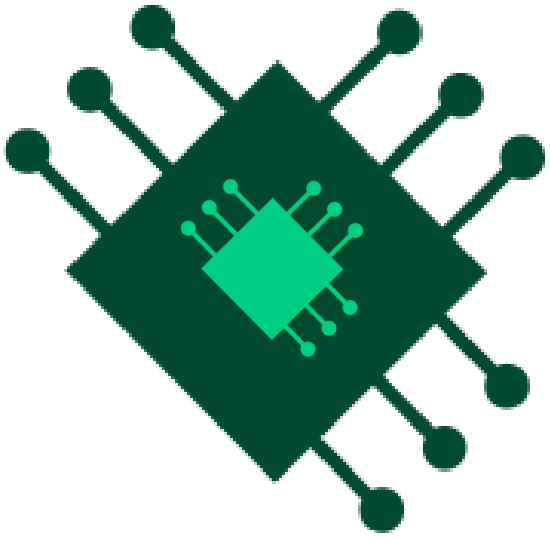
- Ciphers
- Hash functions
- Higher Lvl Protocols

- Ciphers + Hash
  - 2 cores

- Ciphers + Cipher Modes
  - CCM
  - GCM

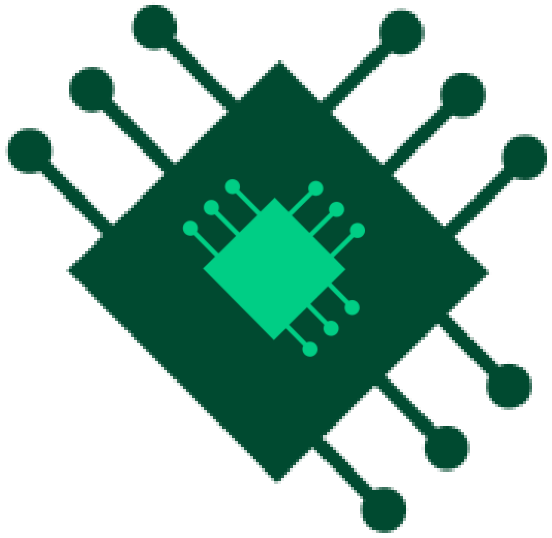
Digital Security Today (AES-CCM)

- Cipher Modes (more easily embeddable & efficient)
  - It specifies the order in which blocks are encryption
  - AES-CCM most common:
    - **A**dvanced
    - **E**ncryption
    - **S**tandard
    - **C**ounter with
    - **C**BC-**M**AC



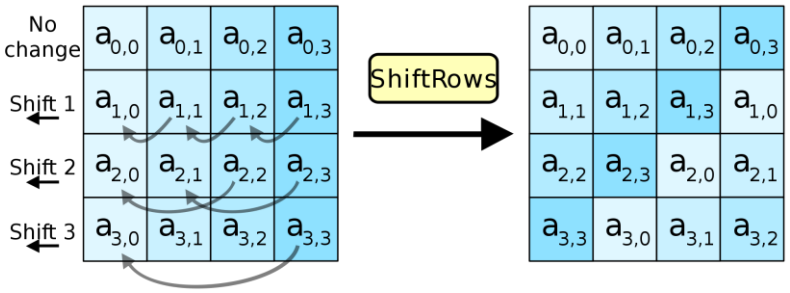
Digital Security Today (AES-CCM)

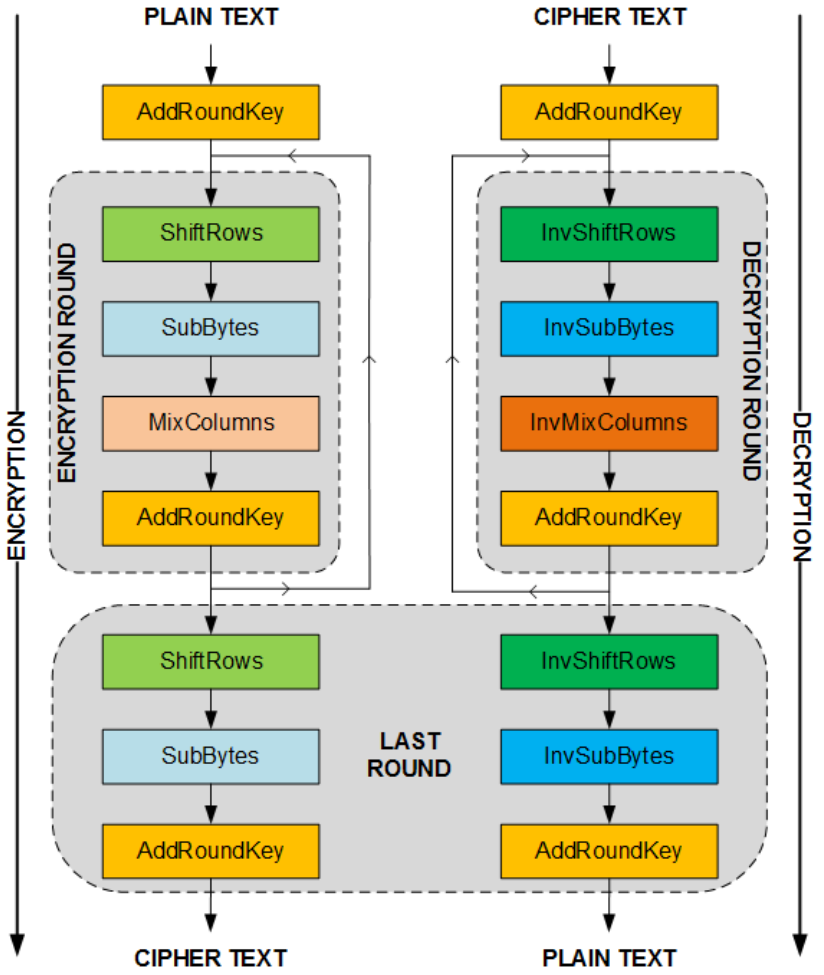
- Cipher Modes (more easily embeddable & efficient)
  - It specifies the order in which blocks are encryption
  - AES-CCM most common:
    - **A**dvanced
    - **E**ncryption
    - **S**tandard
    - **C**ounter with
    - **C**BC-**M**AC
  - Used in:
    - IEEE 802.11 (WLAN)
    - IEEE 802.16 (Broadband Wi-Fi)
    - IPSec
    - TLS 1.2



The AES Block Cipher

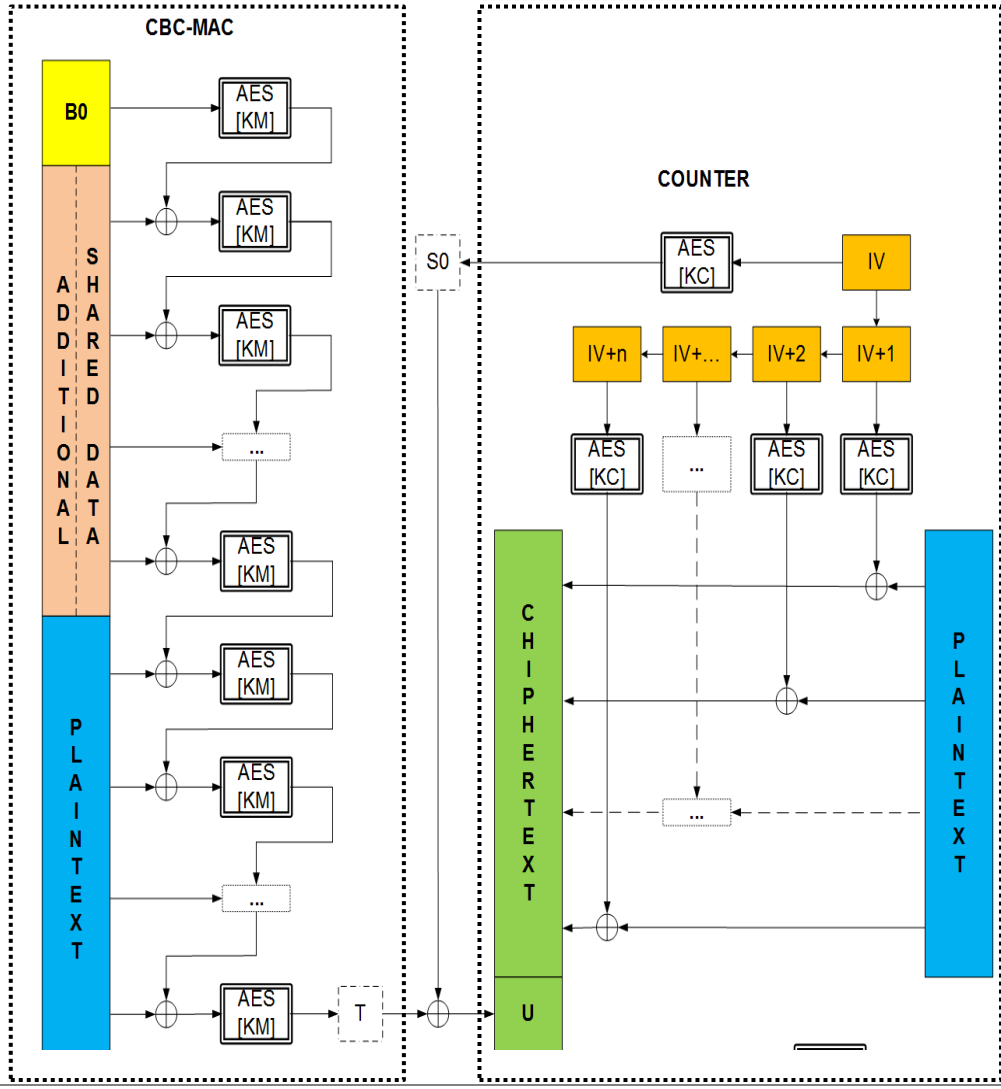
- Official NIST standard since 2001
  - FIPS 197
- 128-bit block cipher
- Logic or Table implementation
- Shared structure for Enc/Dec
- Input keys of 128,192 or 256 bits
  - 10, 12 or 14 iterative rounds





The Counter with CBC-MAC Protocol

- Original submission 2002
  - RFC 3610
- Encryption; Authentication; Integrity for any block cipher
  - Typically AES



The Counter with CBC-MAC Protocol

- Two stream chains
  - **Counter:** non-feedback mode

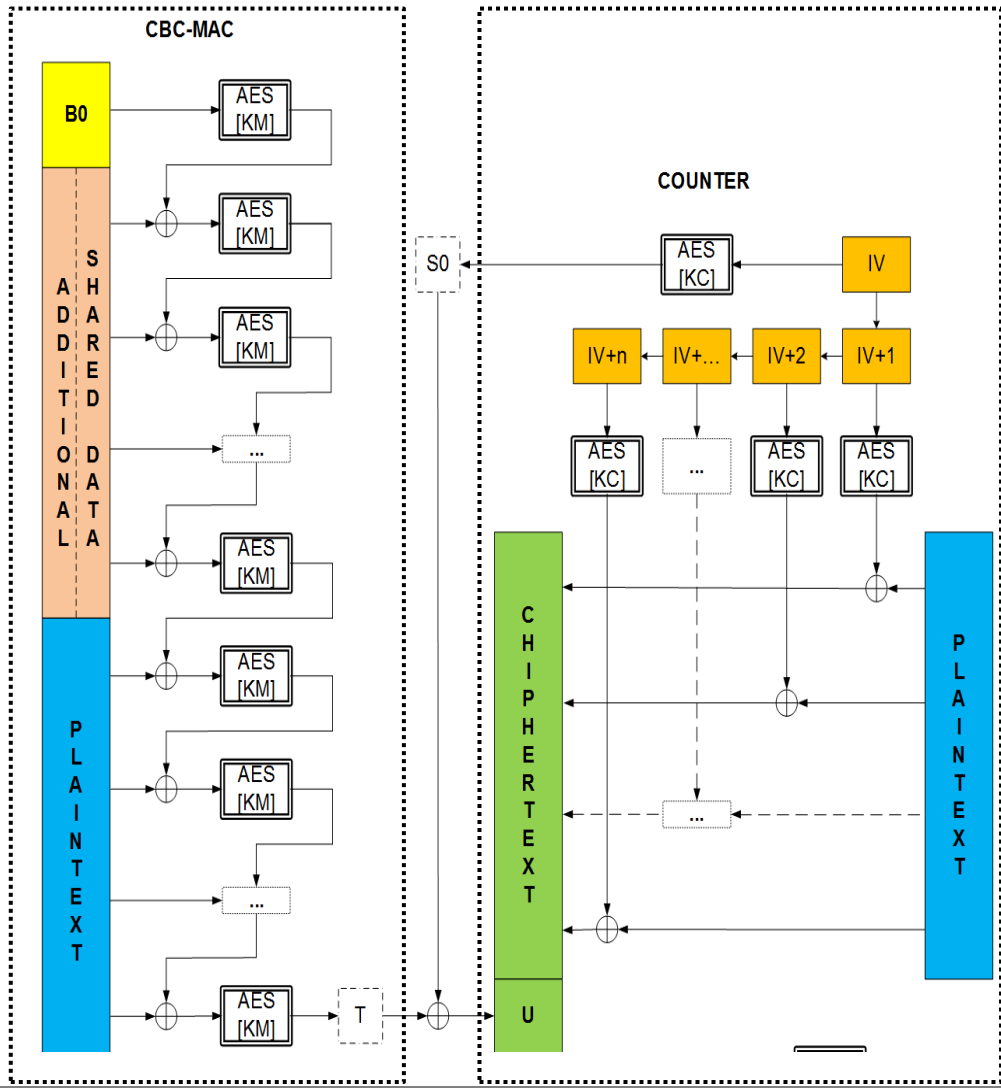
  Counter tags for each independent Plaintext block

  - **CBC-MAC:** feedback mode

  Chainned and dependent Plaintext encryption

- Cipher's decryption is not required
- Additional Shared Data

for extra security

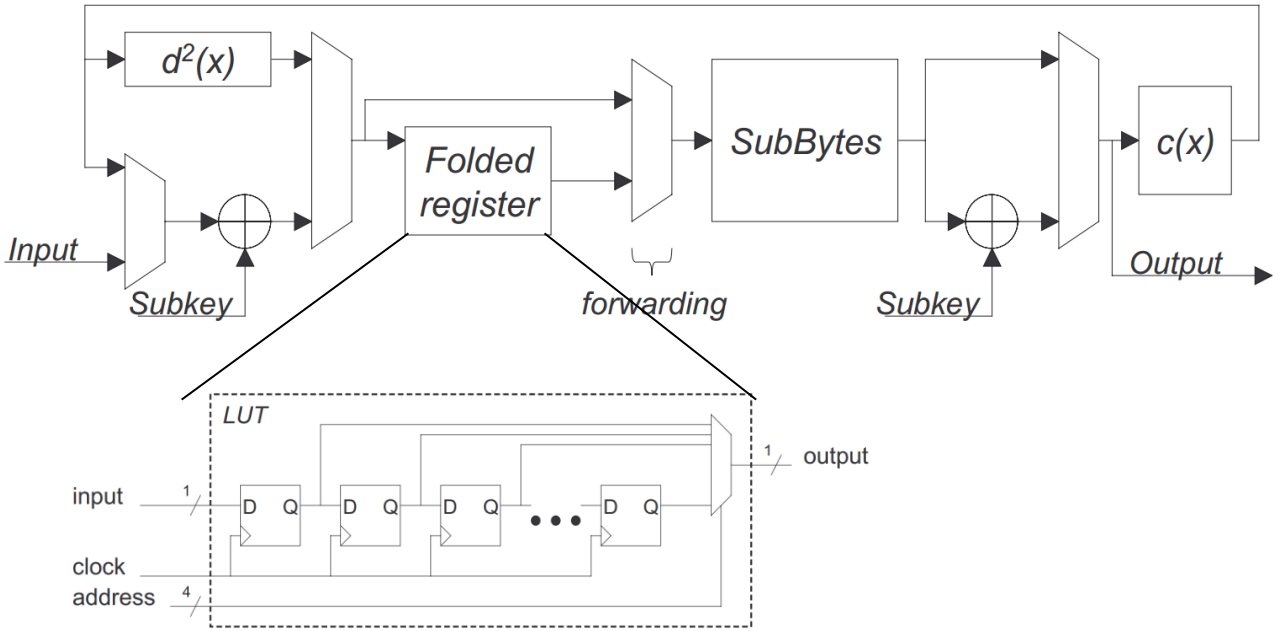


Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode
- State of the Art in AES implementations on FPGA
- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution
- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art
- Conclusions

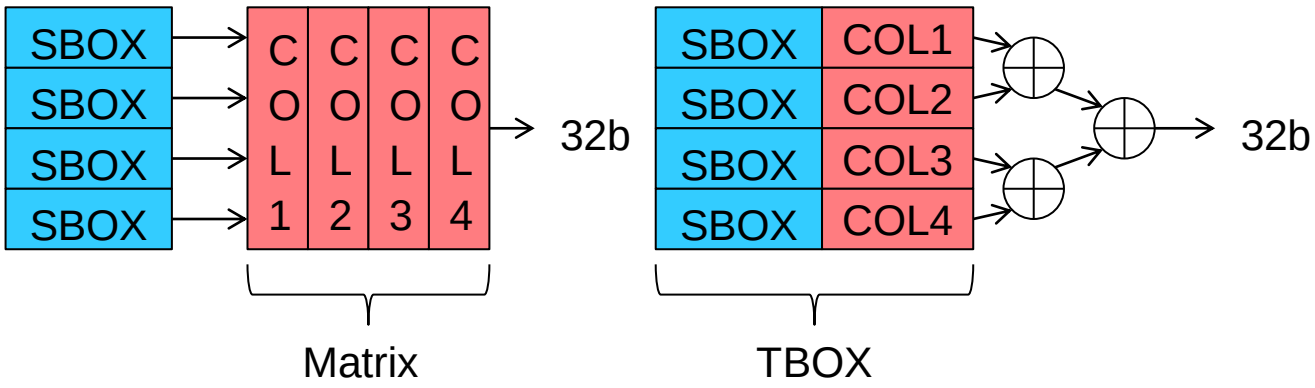
State of the Art in AES implementations on FPGA

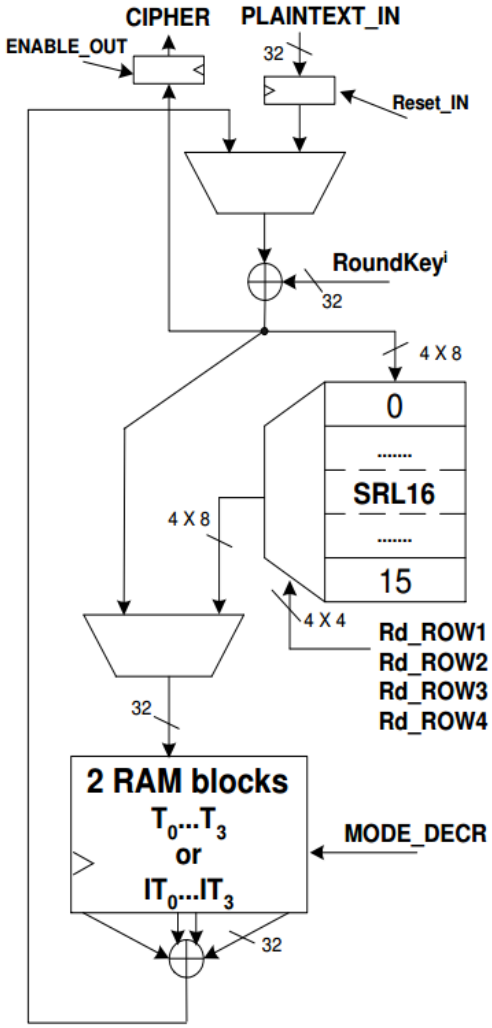
- Chodowiec and Gaj [2003]
  - ShiftRows performed by addressable Shift Register
  - SubBytes performed by BRAM-based S-Boxes
  - MixColumns performed by logic



State of the Art in AES implementations on FPGA

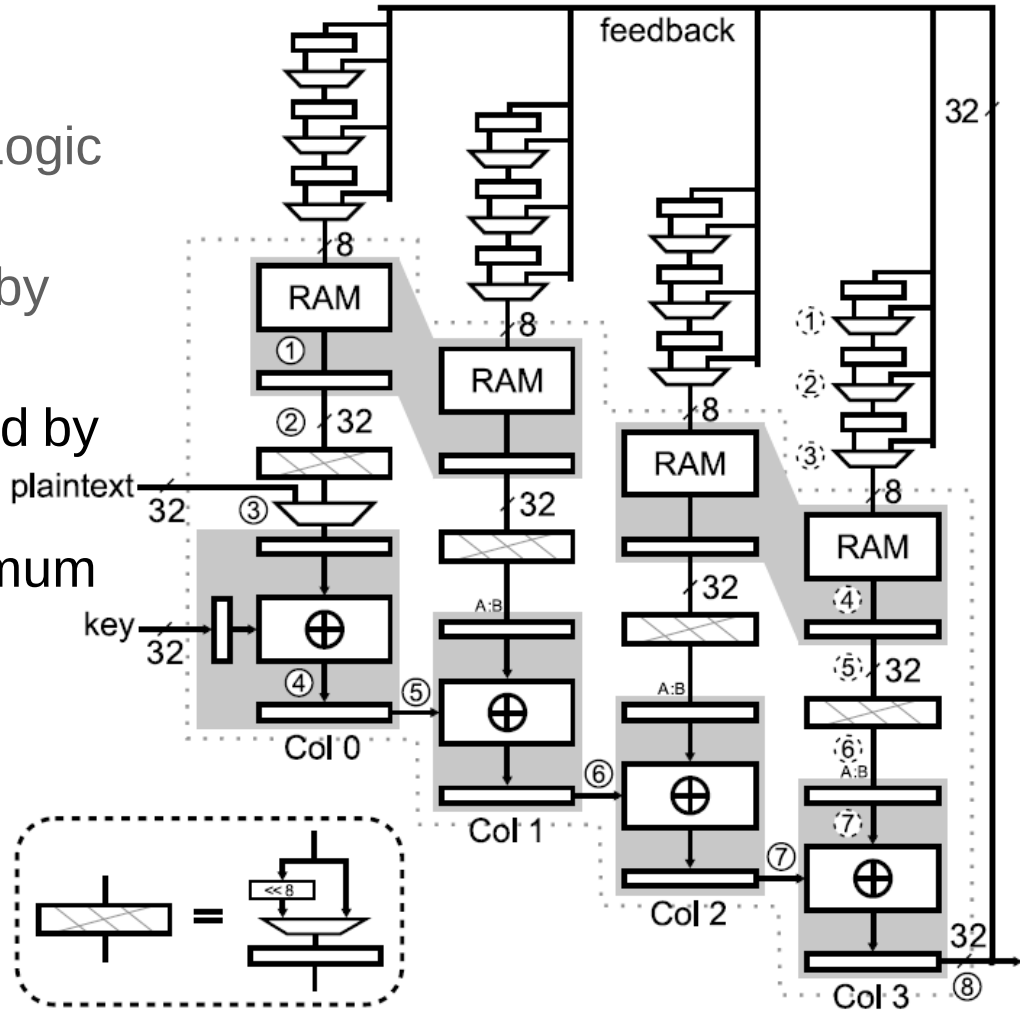
- Rouvroy et al. [2004]
  - ShiftRows performed by Shift Register
  - SubBytes & MixColumns performed by BRAM-based T-Boxes
  - Extra InvS-Box in BRAM for decryption
  - Embedded Key Scheduler





State of the Art in AES implementations on FPGA

- Drimer et al. [2010]
  - ShiftRows performed by Logic Shift Register
  - SubBytes & MixColumns by BRAM based T-Boxes
  - XOR operations performed by Cascade of 4 DSPs
  - 8-stage Pipeline for maximum clock frequency

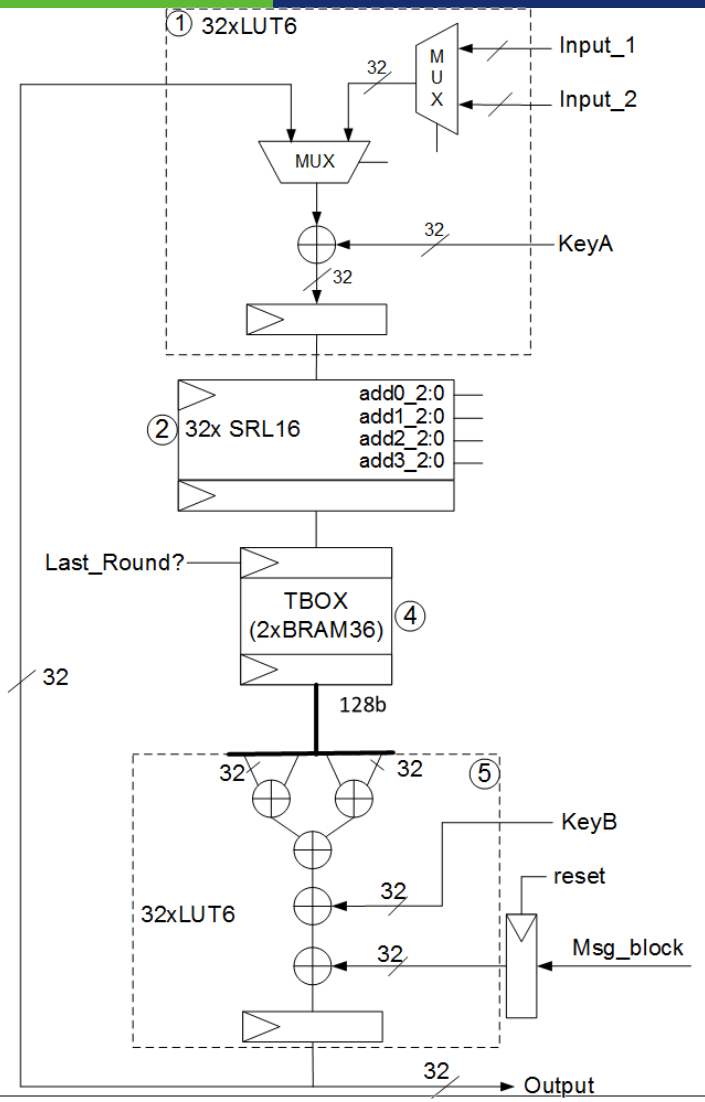


Outline

- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode
- State of the Art in AES implementations on FPGA
- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution
- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art
- Conclusions

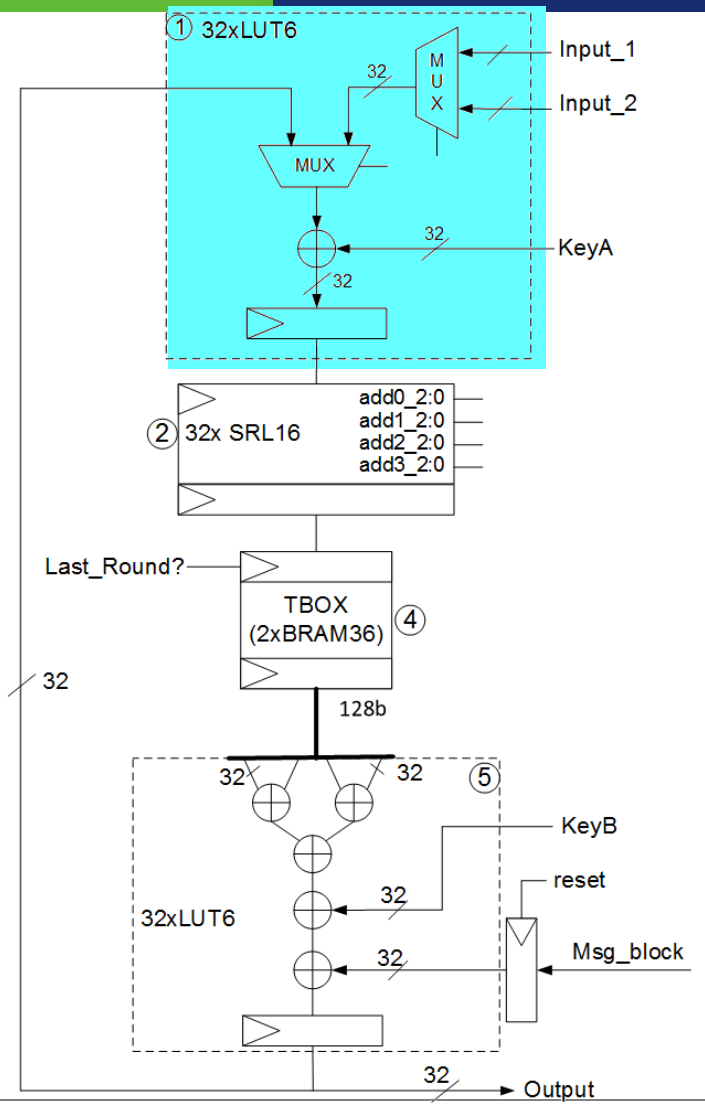
Proposed Architecture: Description and Implementation

- Proposed Structure
  - Combine solutions from State of the Art
  - Improve efficiency through:
    - Removal of DSPs
    - Most use of LUT6 technology
    - Improved Scheduling/Pipelining
    - Minimize Critical Path



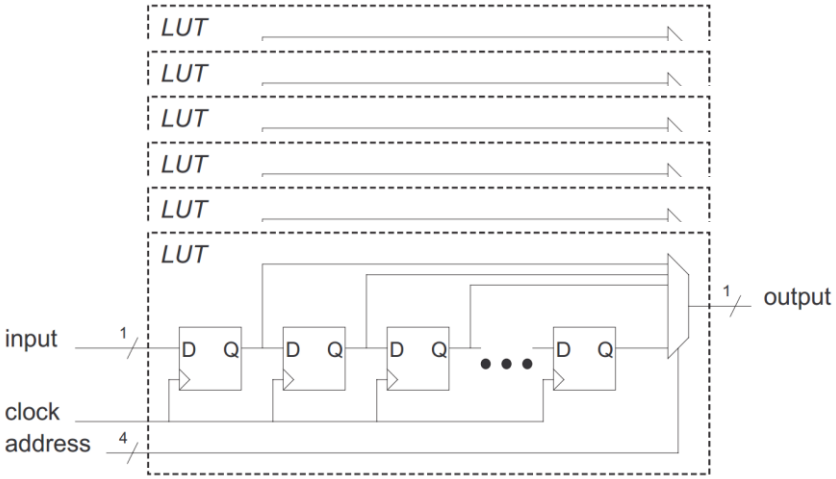
Proposed Architecture: Description and Implementation

- Step-by-step components
  - Initial Whitening Keys

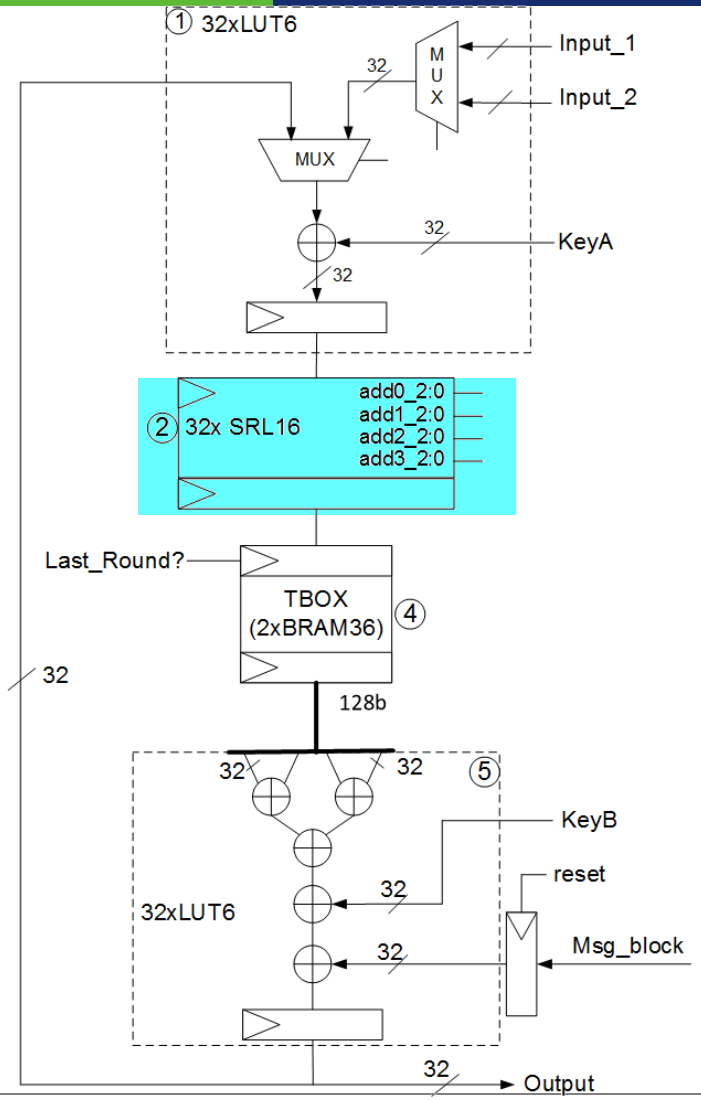


Proposed Architecture: Description and Implementation

- Step-by-step components
  - Initial Whitening Keys
  - Shift Register for AES

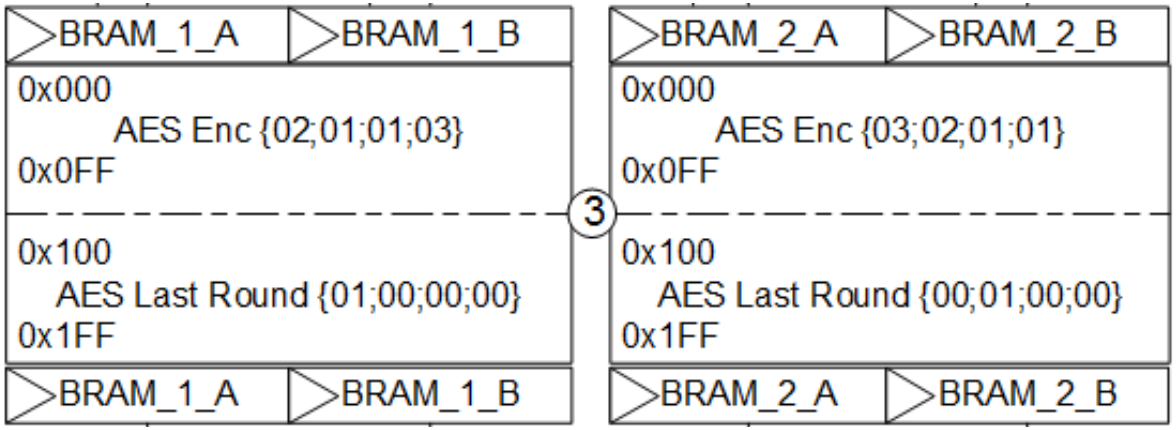


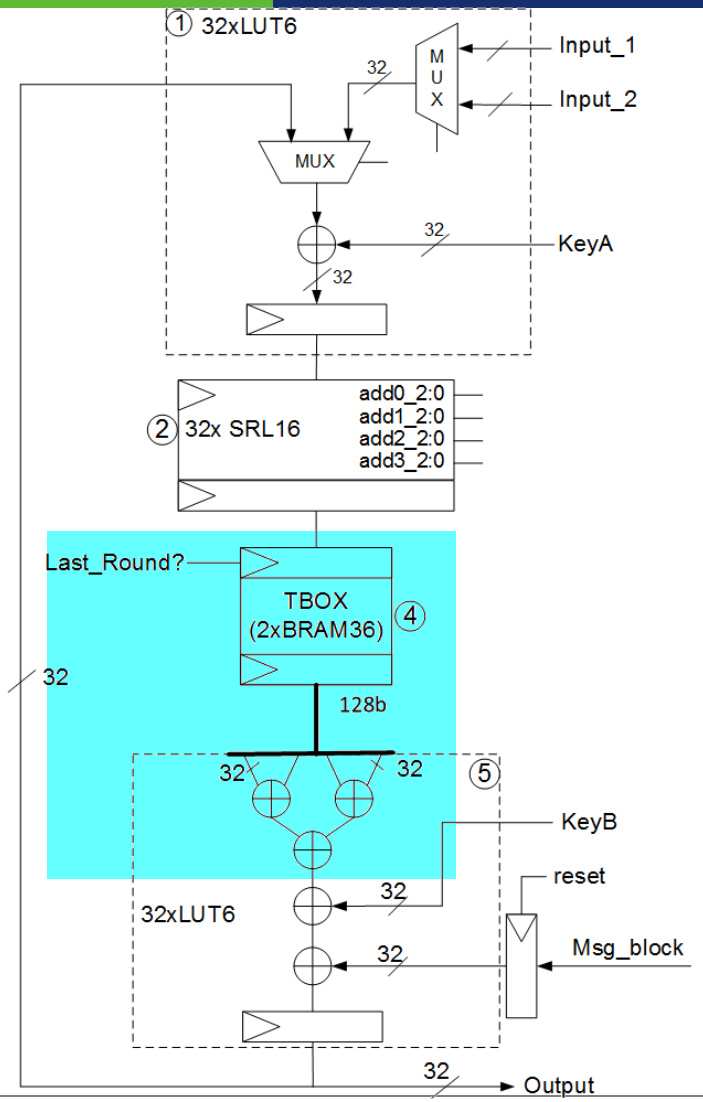
x32 bits



Proposed Architecture: Description and Implementation

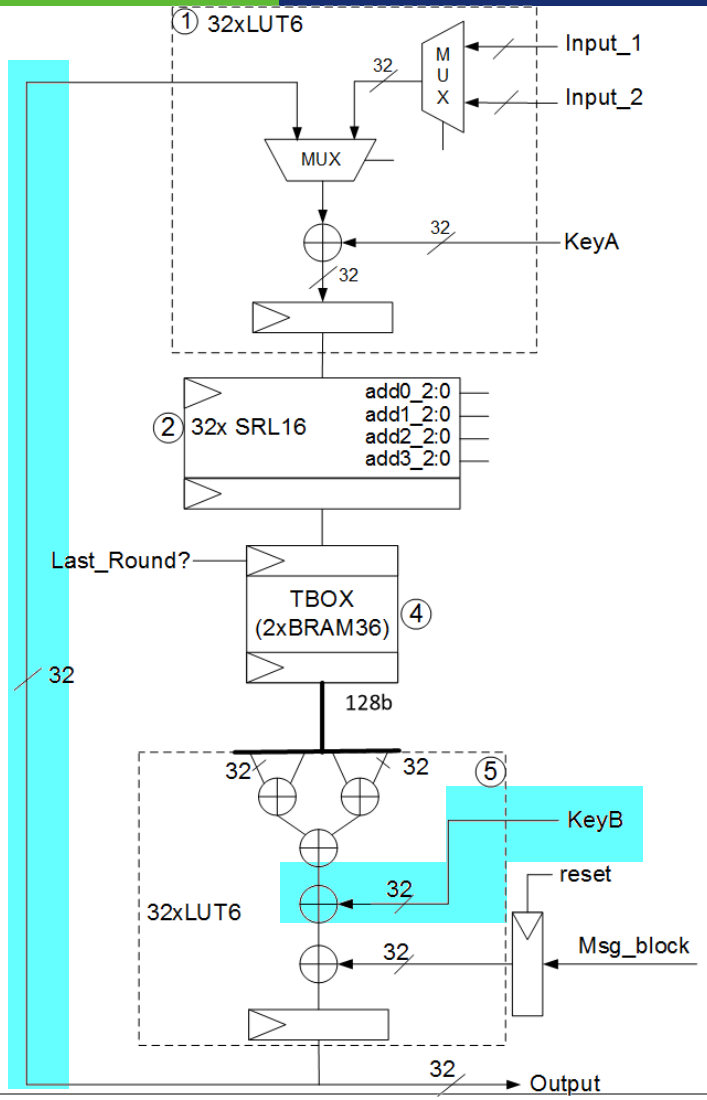
- Step-by-step components
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes





Proposed Architecture: Description and Implementation

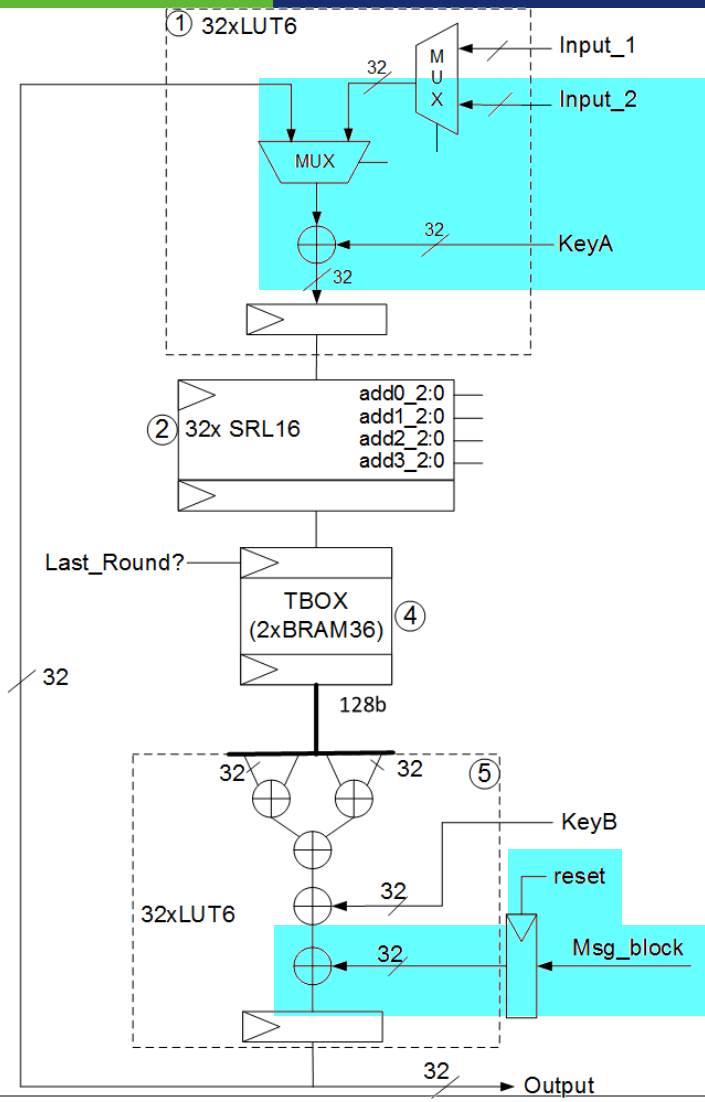
- Step-by-step components
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes
  - AddRoundKey and Feedback



Proposed Architecture: Description and Implementation

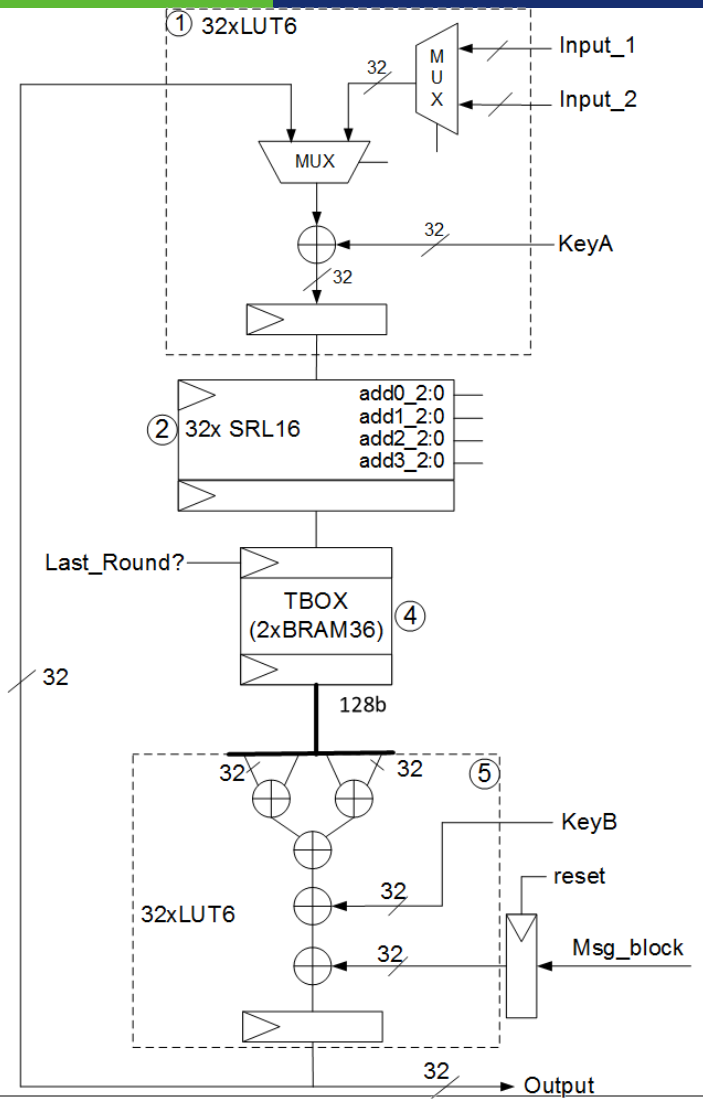
- Step-by-step components
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes
  - AddRoundKey and Feedback
  - Output Block Addition

  // Imediate load of new Block (Counter)



Proposed Architecture: Description and Implementation

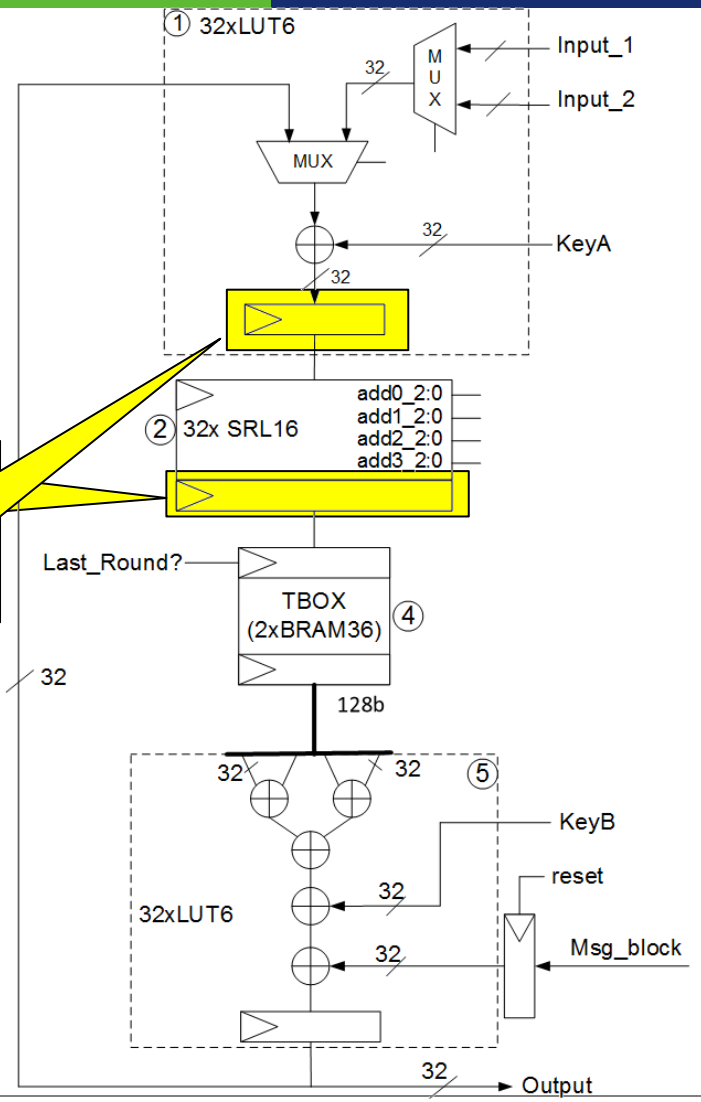
- Scheduling
  - Each block takes 9 cycles to process & re-store.
  - There are 2 blocks = 8 Words (32 bits)
  - 1 dead cycle = 1 register too many



Proposed Architecture: Description and Implementation

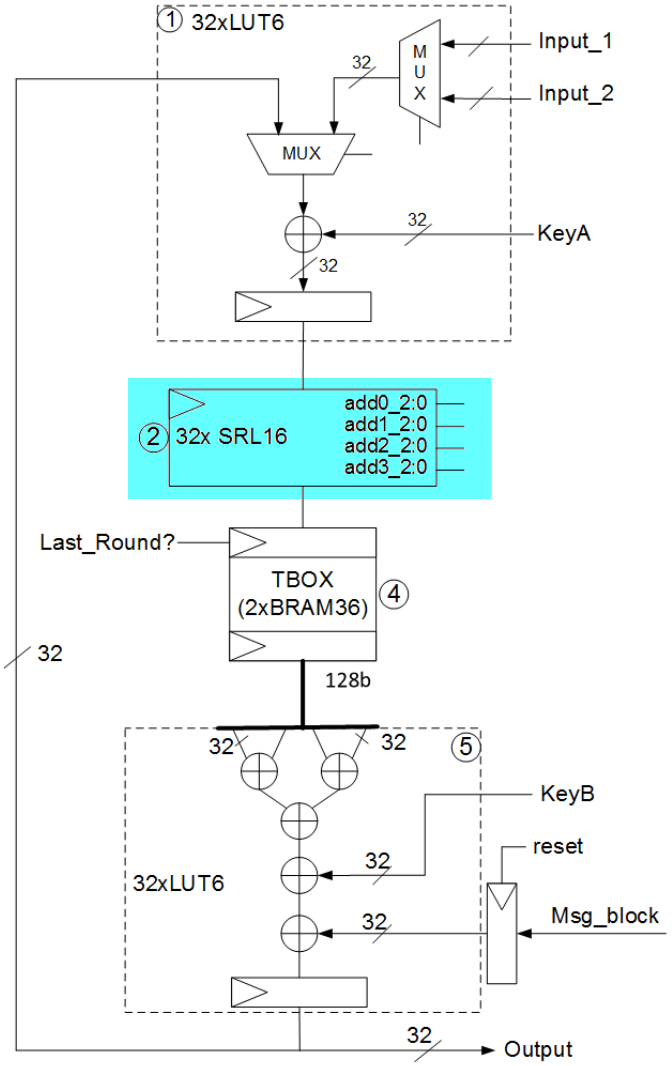
- Scheduling
  - Each block takes 9 cycles to process & re-store.
  - There are 2 blocks = 8 Words (32 bits)
  - 1 dead cycle = 1 register too many

Two viable solutions



Proposed Architecture: Description and Implementation

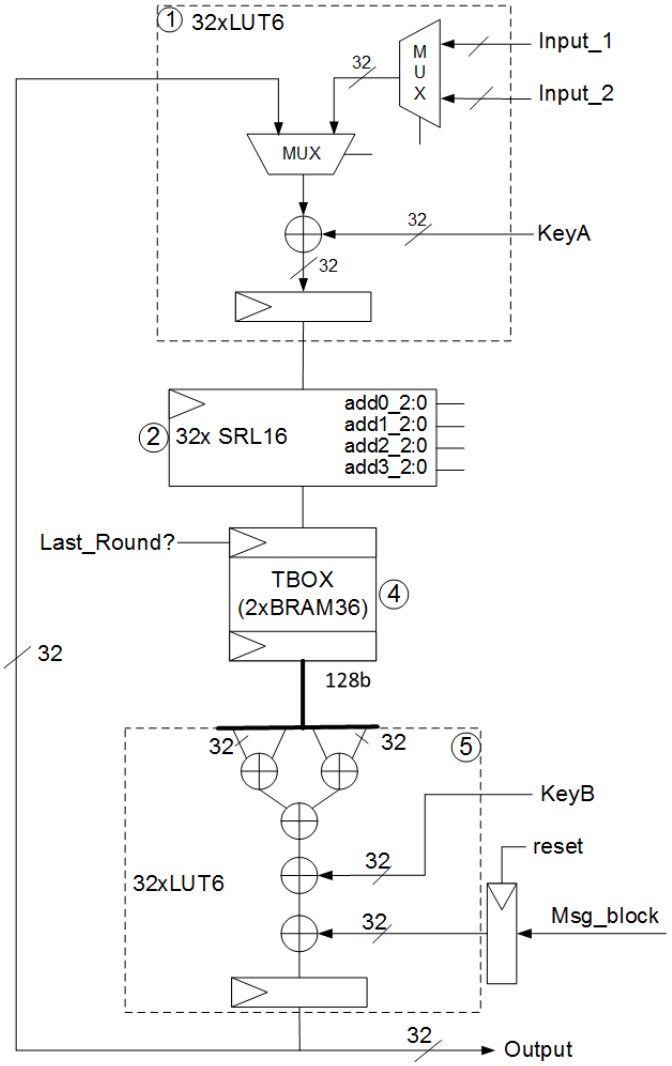
- Scheduling
  - ~~Each block takes 9 cycles to process & re-store.~~
  - ~~There are 2 blocks = 8 Words (32 bits)~~
  - ~~1 dead cycle = 1 register too many~~
  - Removal of the SRL ouput register
    - Shorter propagation signal
  - Each block takes 8 cycles to process & re-store.
  - There are 2 blocks = 8 Words (32 bits)
  - 0 dead cycles



Proposed Architecture: Description and Implementation

- Compact Double Block AES FPGA core.
  - Double Input (Counter or CBC-MAC)
  - Shift Register for Shift Rows
  - BRAM-based TBoxes
  - Output Stage with Final block addition
  - **Overlapping Input/Output cycles**
  - Critical Path = 1 Logic level + routing
  - Total of 96 LUTs + 2 BRAMs

  (+32 isolated FFs)



Outline

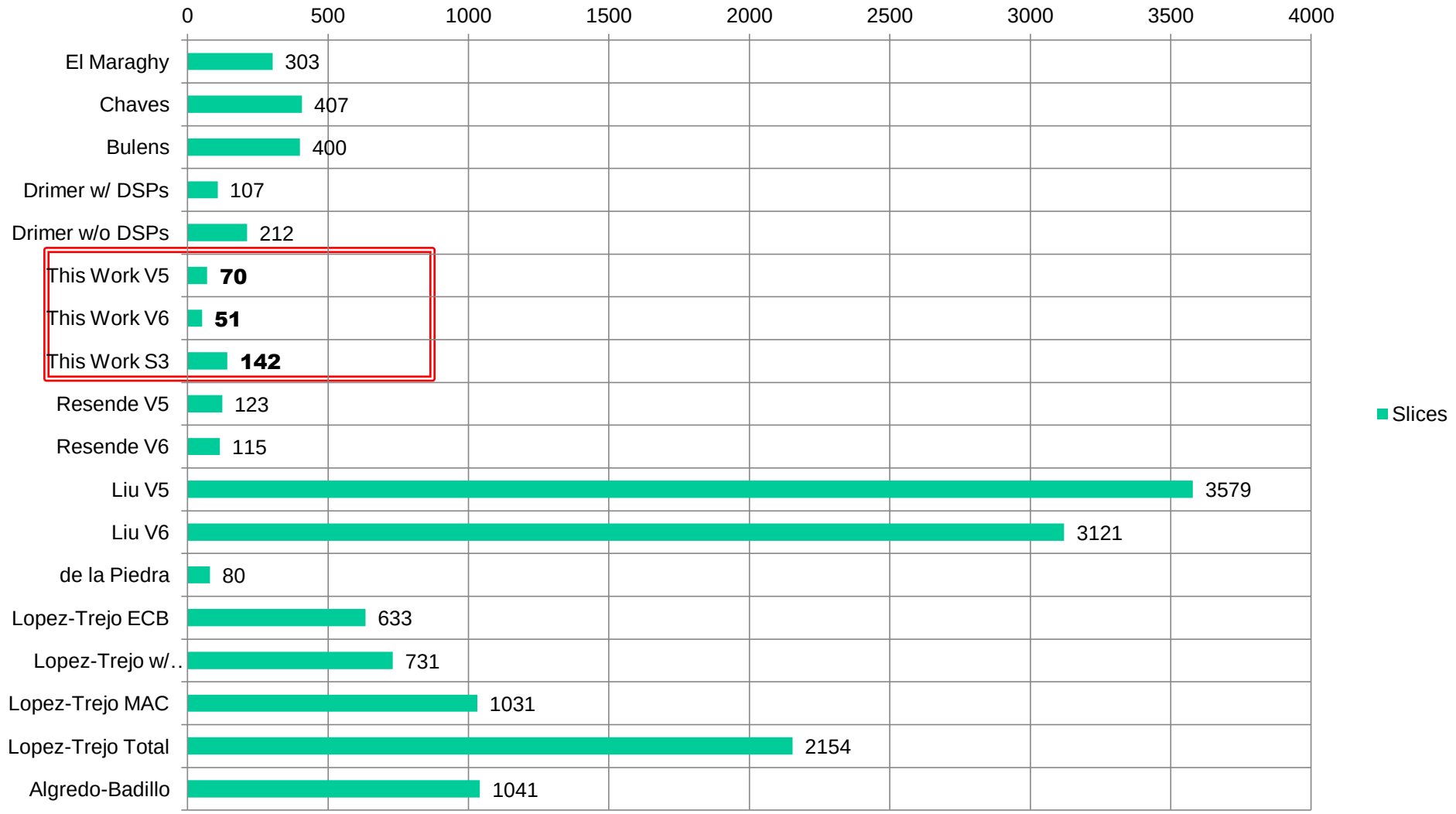
- Introduction & Motivation
  - Digital Security Today
  - The AES Block Cipher
  - The CCMP Encryption mode
- State of the Art in AES implementations on FPGA
- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improved Solution
- **Result Analysis**
  - Resource requirements and performance
  - Comparison with related State of the Art
- Conclusions

Result Analysis

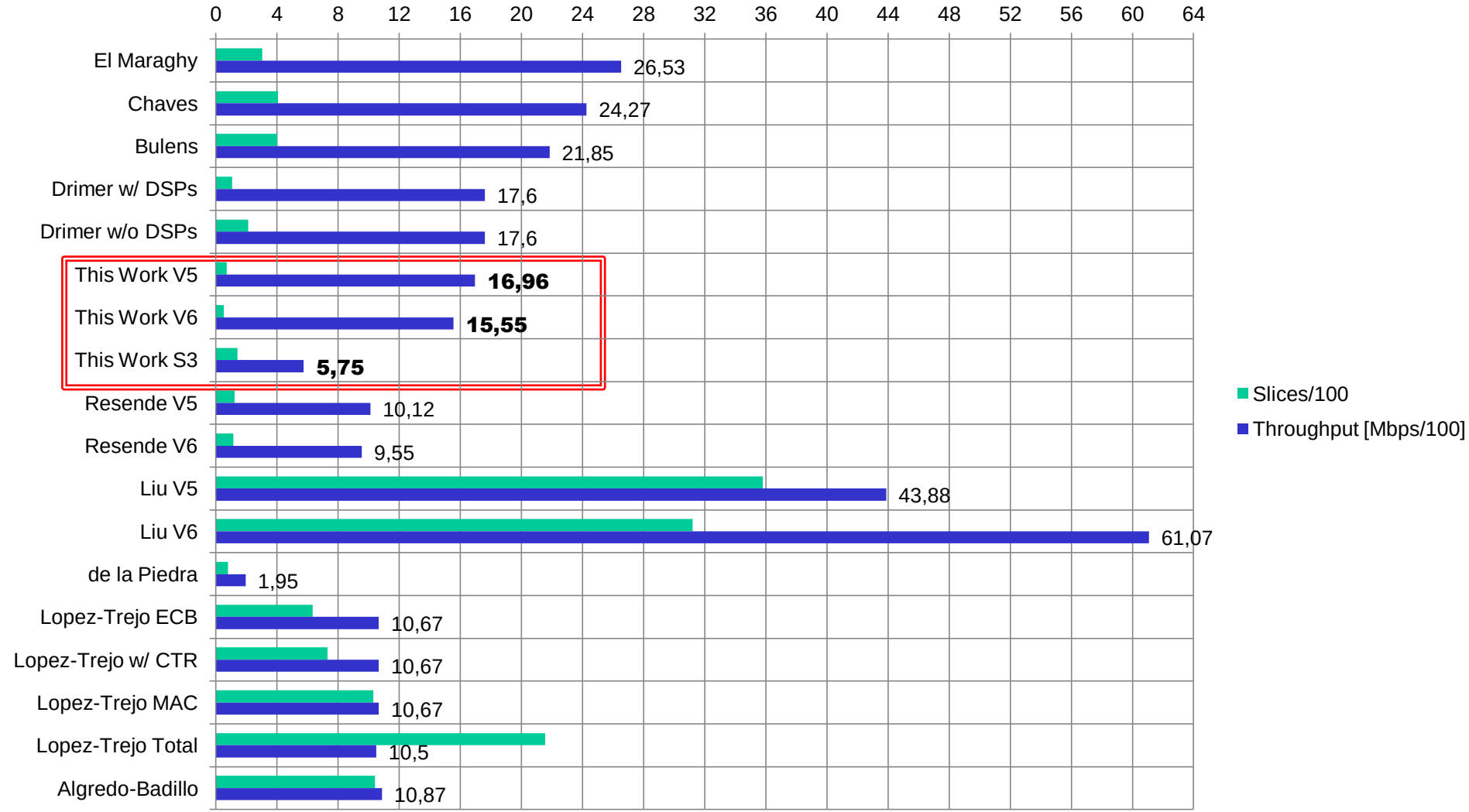
- State of the Art Comparison (double block)

		Round Structure	Device	Resources			Throughput	Efficiency
				Slices	BRAMs	DSPs	[Gbps]	[Mbps/S]
El Maraghy		Rolled(128b)	V5	303	8+2	0	1,327 **(2,653)**	4,38 (8,75)
Chaves		Rolled(128b)	V5	407	8+2	0	**2,427**	5,96
Bulens		Rolled(128b)	V5	400	0	0	2,185	5,46
Drimer		Rolled(32b)	V5	107	2+1	4	1,76	16,45
				212		0		8,30
This Work		Rolled(32b)	V5	**70**	2+1	0	1,696	**24,22**
			V6	**51**			1,555	**30,49**
			S3	142			0,575	4,05
Resende		Rolled(32b)	V5	123	2+1	0	1,012	8,23
			V6	115			0,955	8,3
Liu		Unrolled	V5	3579	0	0	**4,388**	1,22
			V6	3121			**6,107**	1,95
de la Piedra		Rolled(128b)	A7	80	11	15	0,195	2,44
Lopez-Trejo	ECB	Unrolled	S3	633	53	0	1,067	1,68
	w/ CTR			731				1,45
	MAC			1031				1,03
	Total	2xUnrolled		2154	106		1,05	0,49
Algredo-Badillo		2xRolled(128b)	S3	1041	18	0	1,087	1,04

Result Analysis



Result Analysis



Result Analysis

Conclusions

- **Compact** Double Block AES core on FPGA for CCMP
  - Processing of 2 data streams
  - **51 Slices+3 BRAMs** ; 486 MHz ;
  - 1,55 Gbps ; **30,49 Mbps/Slice**

- Improvements (Virtex 5)
  - **Smallest 32-bit structure to date**
  - **Most efficient AES structure in the state of the art**

		Resources	Throughput	Efficiency
32-bit	de La Piedra “16xDSPs”	-12,5%	+770%	+892%
	Drimer “4xDSPs”	-34%	-4%	+47%
	Drimer “0xDSPs”	-67%		+177%
128-bit	El Maraghy	-76%	-36%	+176%

Thank you!

Questions?

Email:
joaocresende@tecnico.ulisboa.pt
ricardo.chaves@inesc-id.pt