One Core Fit All:
Towards Merging block ciphers on FPGA

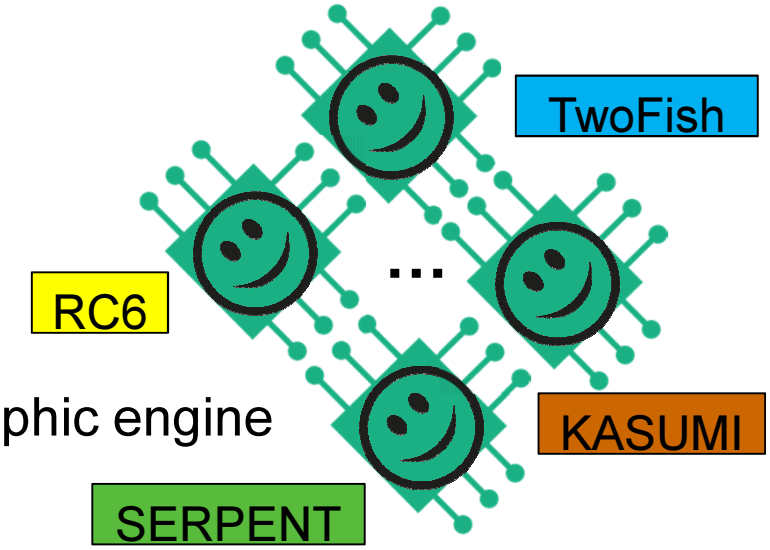
João Carlos C. Resende Shivam Bhasin
Francesco Regazzoni Ricardo Chaves

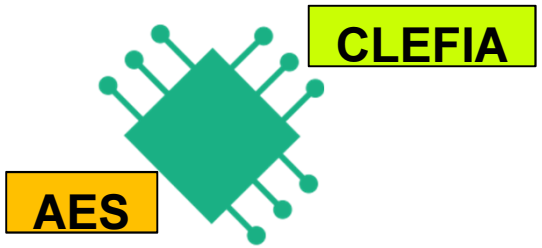
TÉCNICO LISBOA

inesc id lisboa

A Dual CLEFIA & AES Cipher Core on FPGA

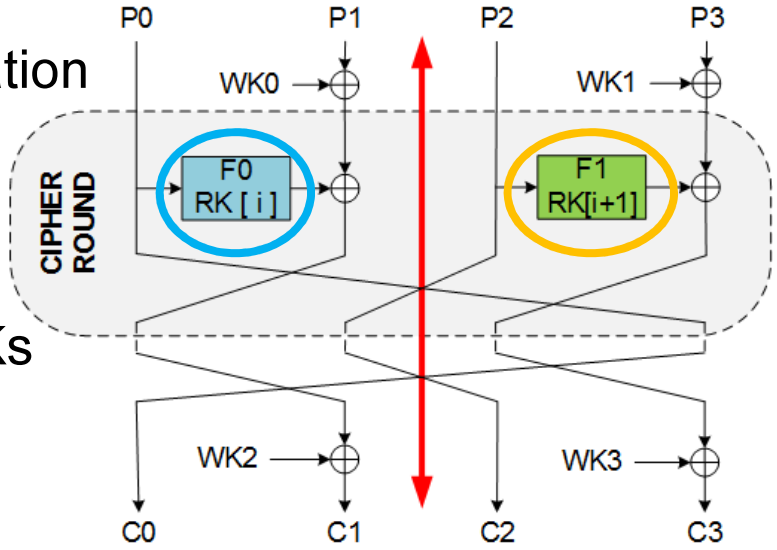
- Cryptographic Engine
  - Circuit capable of applying cipher(s)
- Our objective:
  - To create a multi algorithm cryptographic engine
- In this work:
  - To create an efficient and compact cryptographic engine supporting CLEFIA and AES.

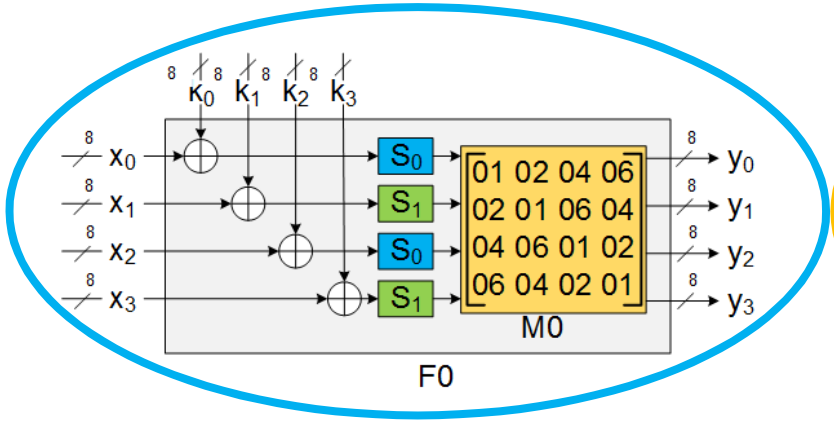


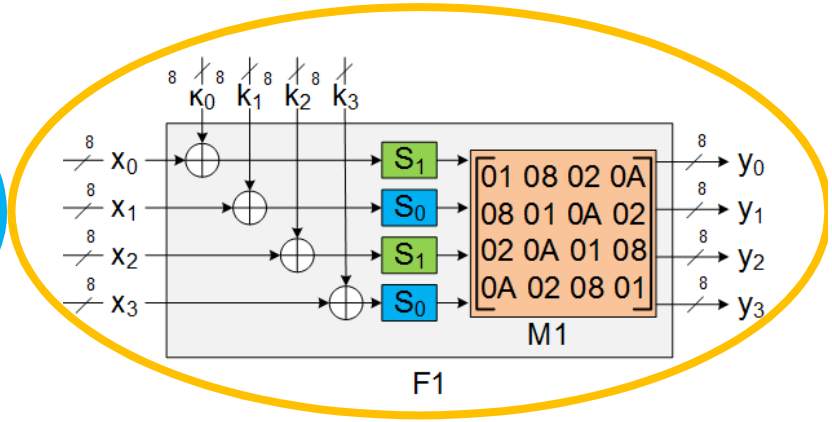


The CLEFIA Block Cipher

- New 128-bit block cipher by Sony Corporation
  - (*Shirai et al.* 2007)
- Lightweight cipher
  - ISO/IEC 23132-2 (2012)
- Strong against Linear and Differencial ATKs
- 18, 22 or 26 iterative rounds

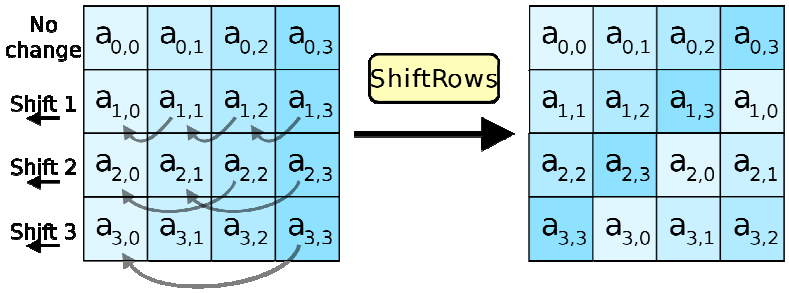


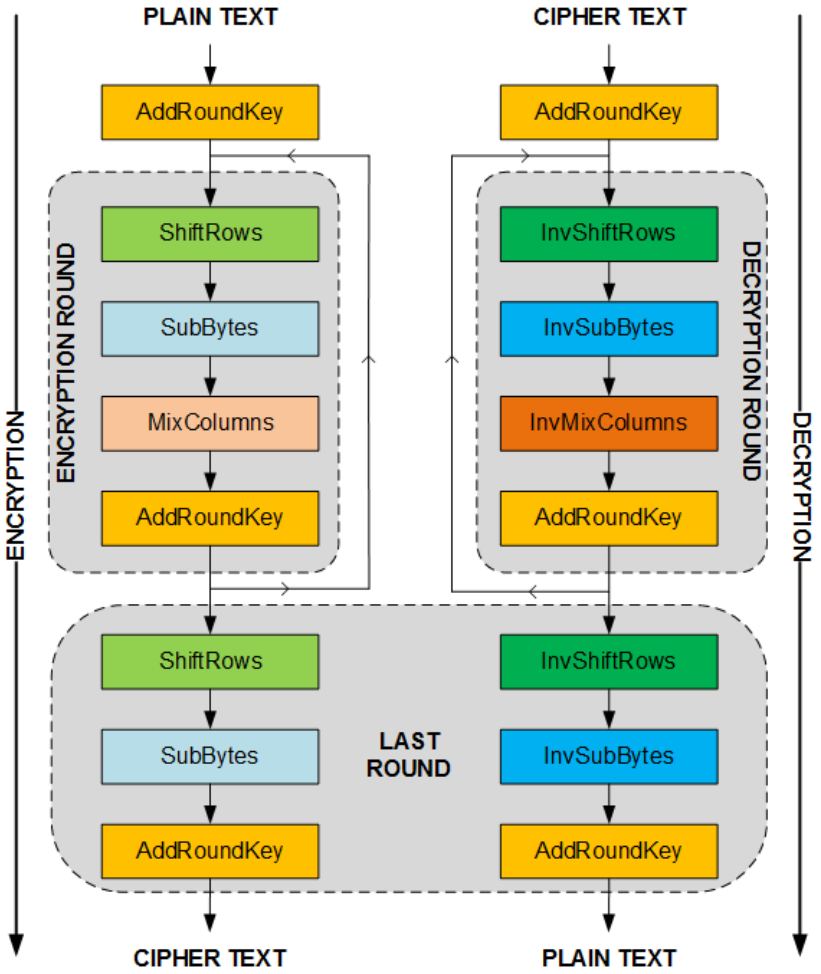




The AES Block Cipher

- Official NIST standard since 2001
  - FIPS 197
- 128-bit block cipher
- Shift Rows structure
- Input keys of 128,192 or 256 bits
- 10, 12 or 14 iterative rounds





AES vs. CLEFIA

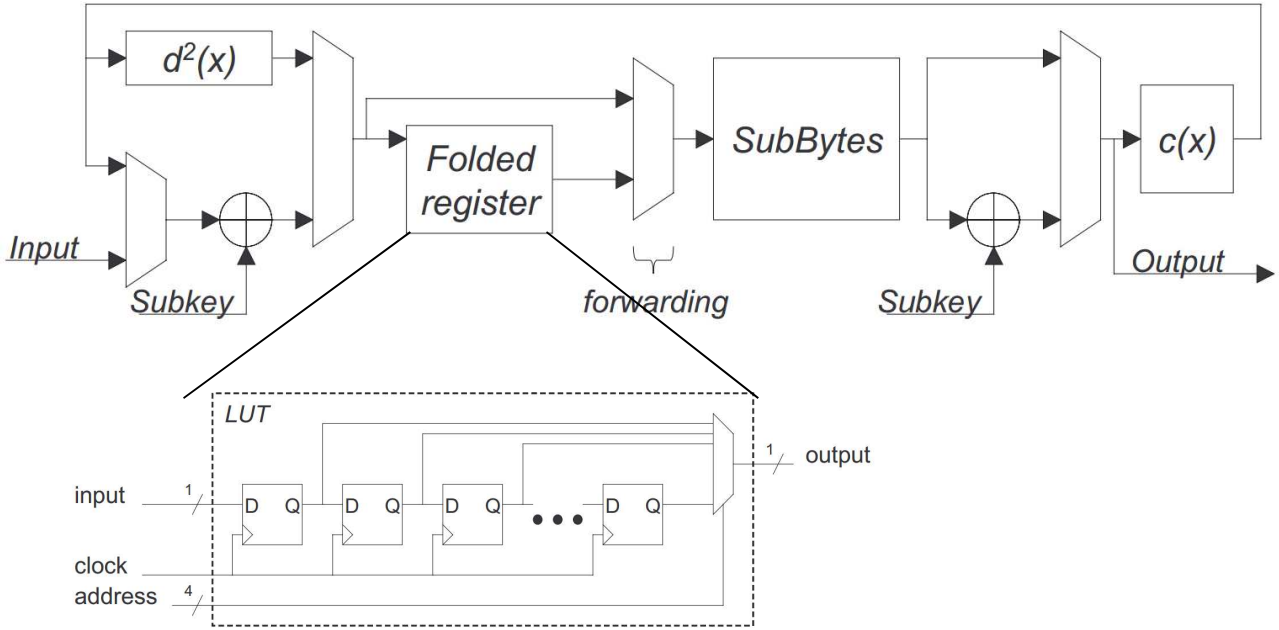
- AES Cipher
  - Symmetric 128-bit block cipher
  - Substitution-Permutation Structure
  - Whitening Keys
  - AddRoundKey
  - SubBytes (1x S-Box)
  - MixColumns (1x matrices)
  - ShiftRows
  - 10, 12, 14 Rounds
- CLEFIA Cipher
  - Symmetric 128-bit block cipher
  - Feistel Structure
  - Whitening Keys
  - AddRoundKey
  - S-funtions (2x S-Box)
  - Diffusion Matrix (2x matrices)
  - Feistel Word Swap&Add
  - 18, 22, 28 Rounds

Outline

- Introduction & Motivation
  - Main Concepts
  - The CLEFIA Block Cipher
  - The AES Block Cipher
- State of the Art in FPGA Implementations
- Proposed Architecture: Description and Implementation
  - Combining Solutions
  - Improving Solution
- Result Analysis
  - Resource requirements and performance
  - Comparison with related State of the Art
- Conclusions

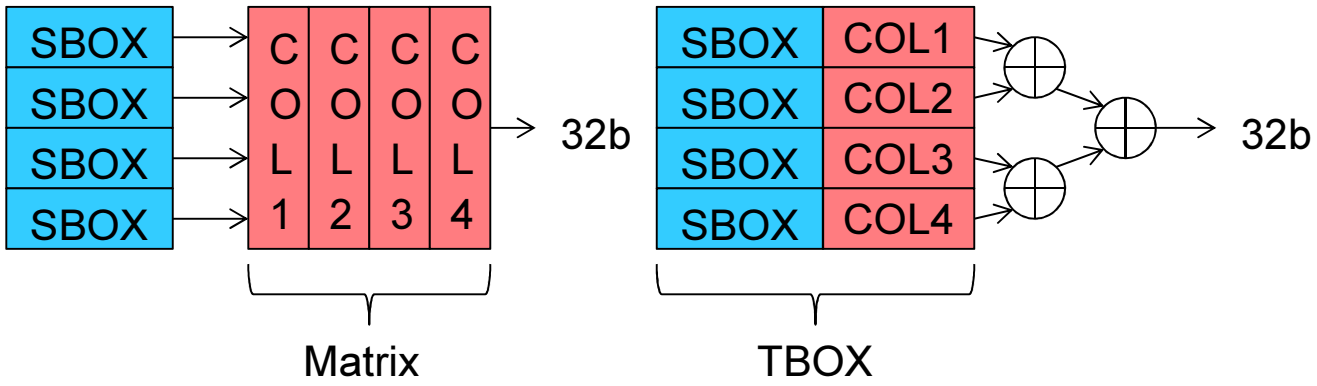
State of the Art in AES implementations

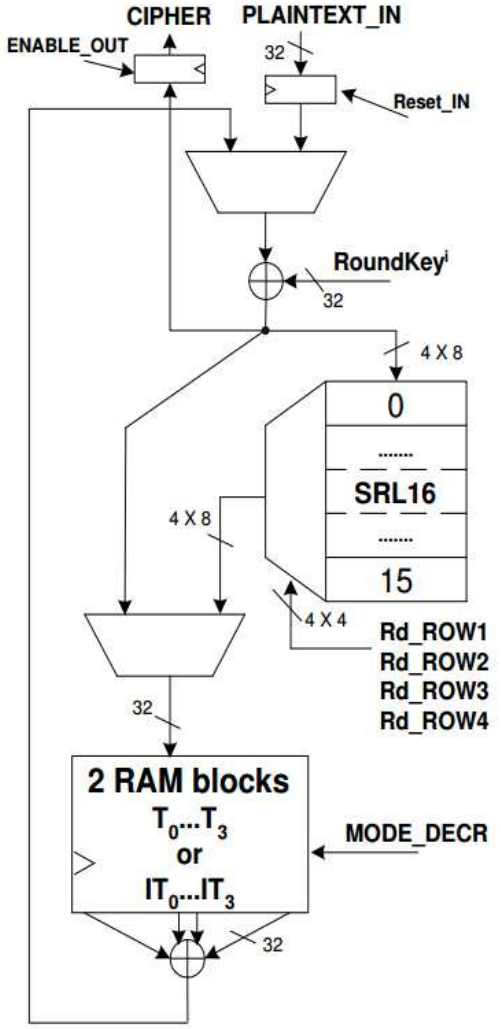
- Chodowiec and Gaj [2003]
  - ShiftRows performed by addressable Shift Register
  - SubBytes performed by BRAM-based S-Boxes
  - MixColumns performed by logic



State of the Art in AES implementations

- 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





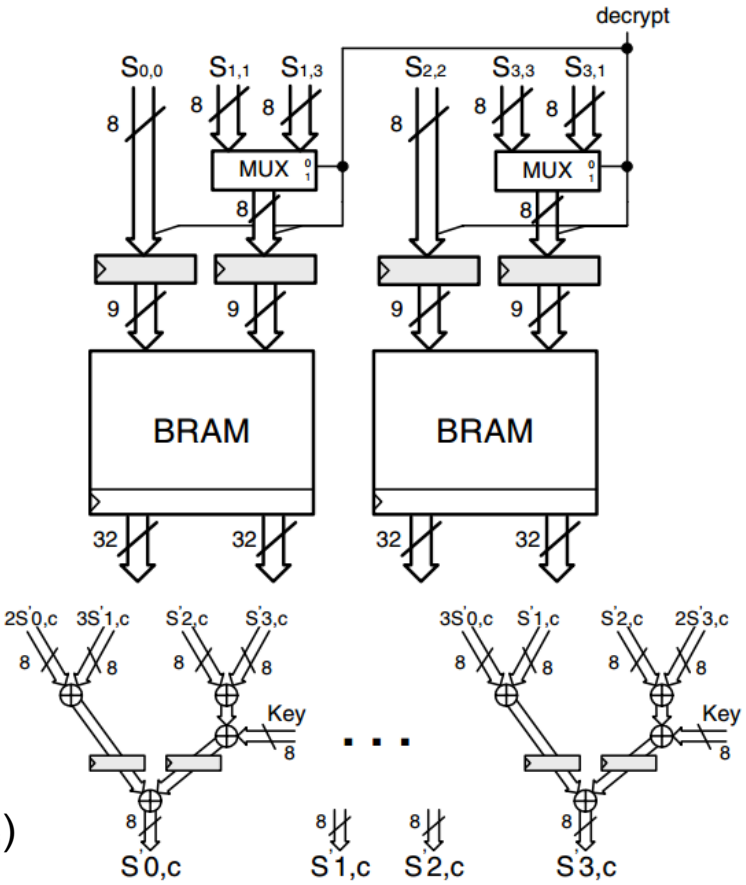
State of the Art in AES implementations

- Chaves et al. [2006]
  - Multiplexed ShiftRows operation
  - SubBytes & MixColumns by BRAM based T-Boxes
  - Improved Last Round

MixC $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$ $\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$ InvMixC

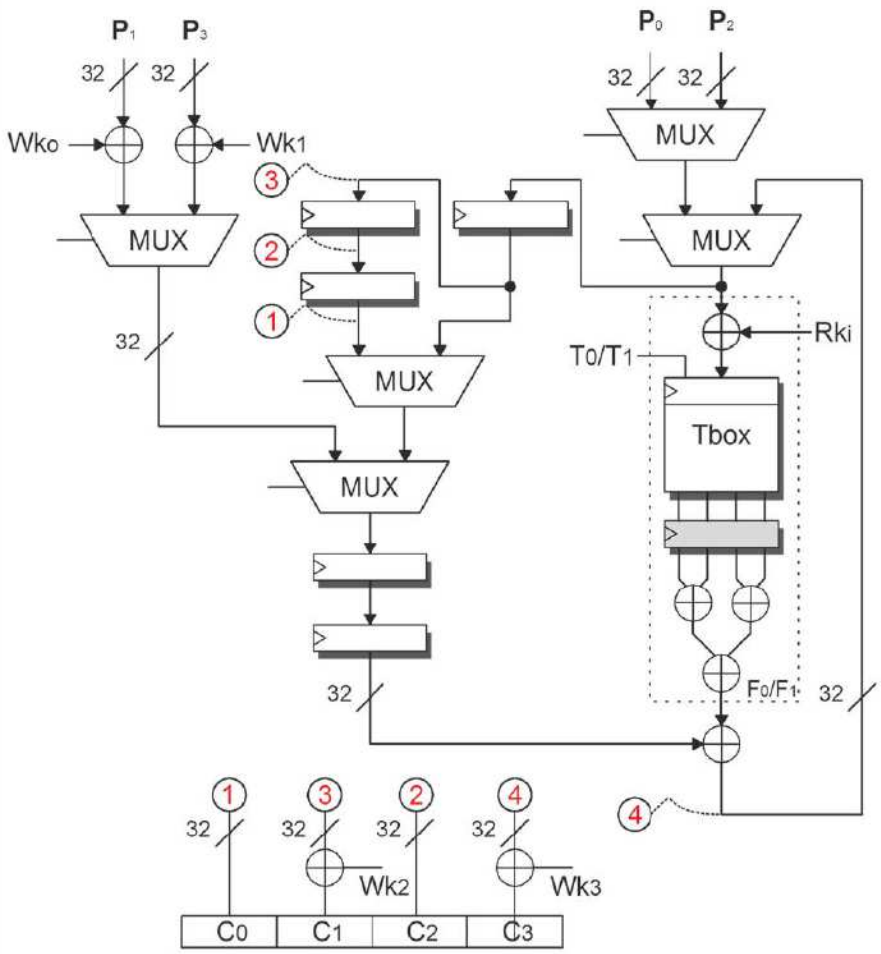
$SB(a_i) = 02\ SB(a_i) \oplus 01\ SB(a_i) \oplus 01\ SB(a_i) \oplus 03\ SB(a_i)$

$ISB(a_i) = 0E\ ISB(a_i) \oplus 09\ ISB(a_i) \oplus 0D\ ISB(a_i) \oplus 0B\ ISB(a_i)$



State of the Art in CLEFIA implementations

- Proença and Chaves [2011]
  - Proper scheduling allows for fast folded rounds
  - First compact implementation of CLEFIA in FPGA
  - F-functions performed through TBoxes

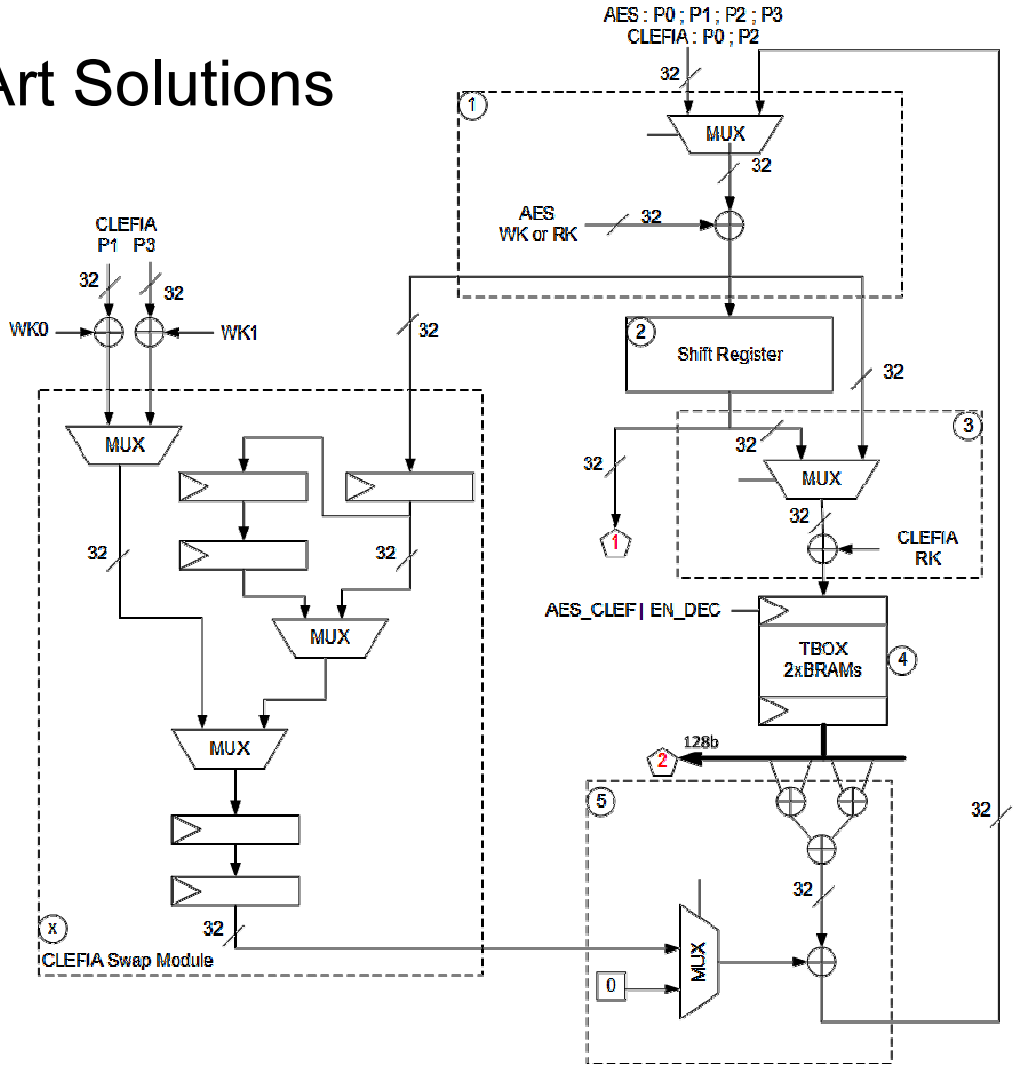


Proposed Architecture: Methodology

- Proposed Solution:
  - Combine the most compact State of the Art solutions
  - Improve efficiency through:
    - Resource sharing
    - Improved Scheduling
    - Improved performance in FPGA

Proposed Architecture: Combined Solutions

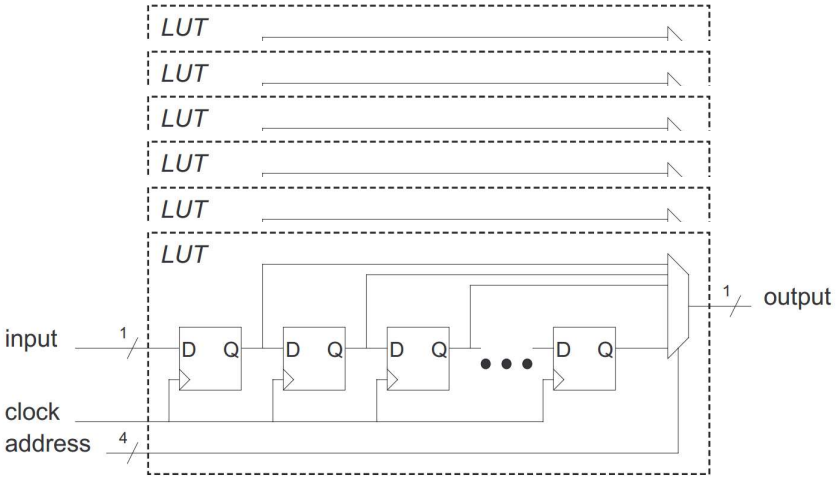
- Combining State of the Art Solutions



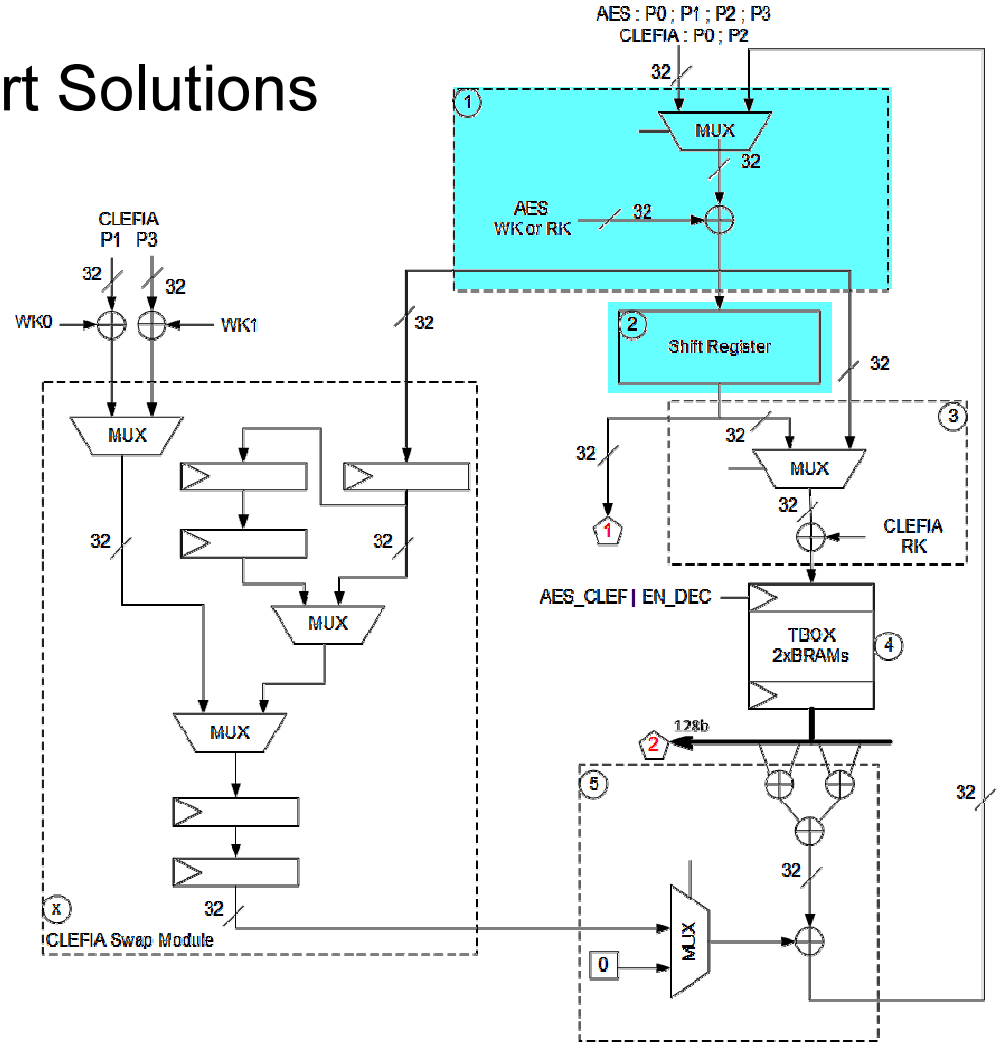
Proposed Architecture: Combined Solutions

- Combining State of the Art Solutions
  - Initial Whitening Keys
  - Shift Register for AES

  (by Chodowiec et al.)



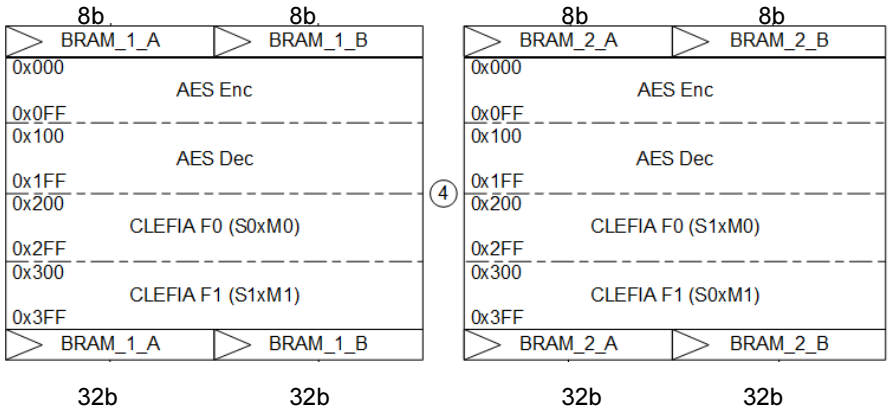
x32 bits

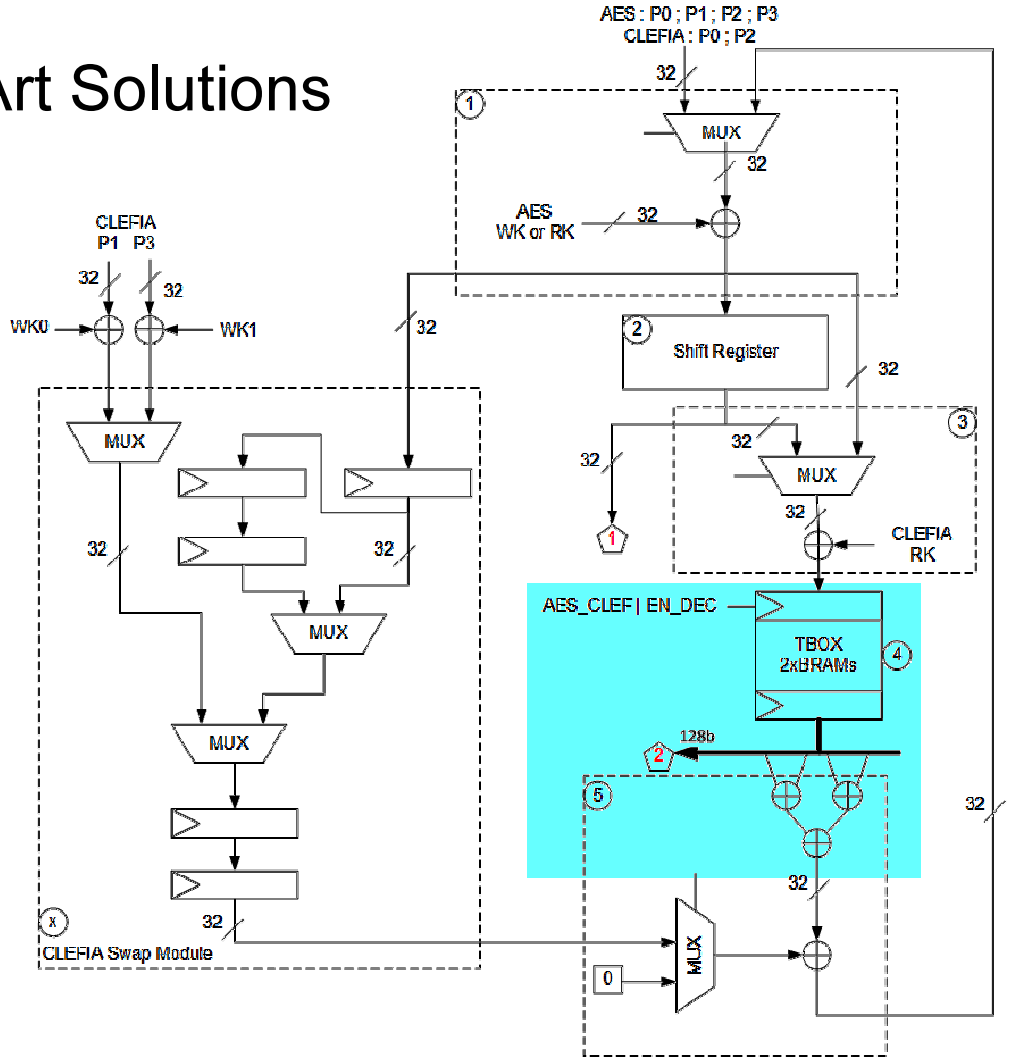


Proposed Architecture: Combined Solutions

- Combining State of the Art Solutions
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes

(Rouvroy et al. / Chaves et al.)

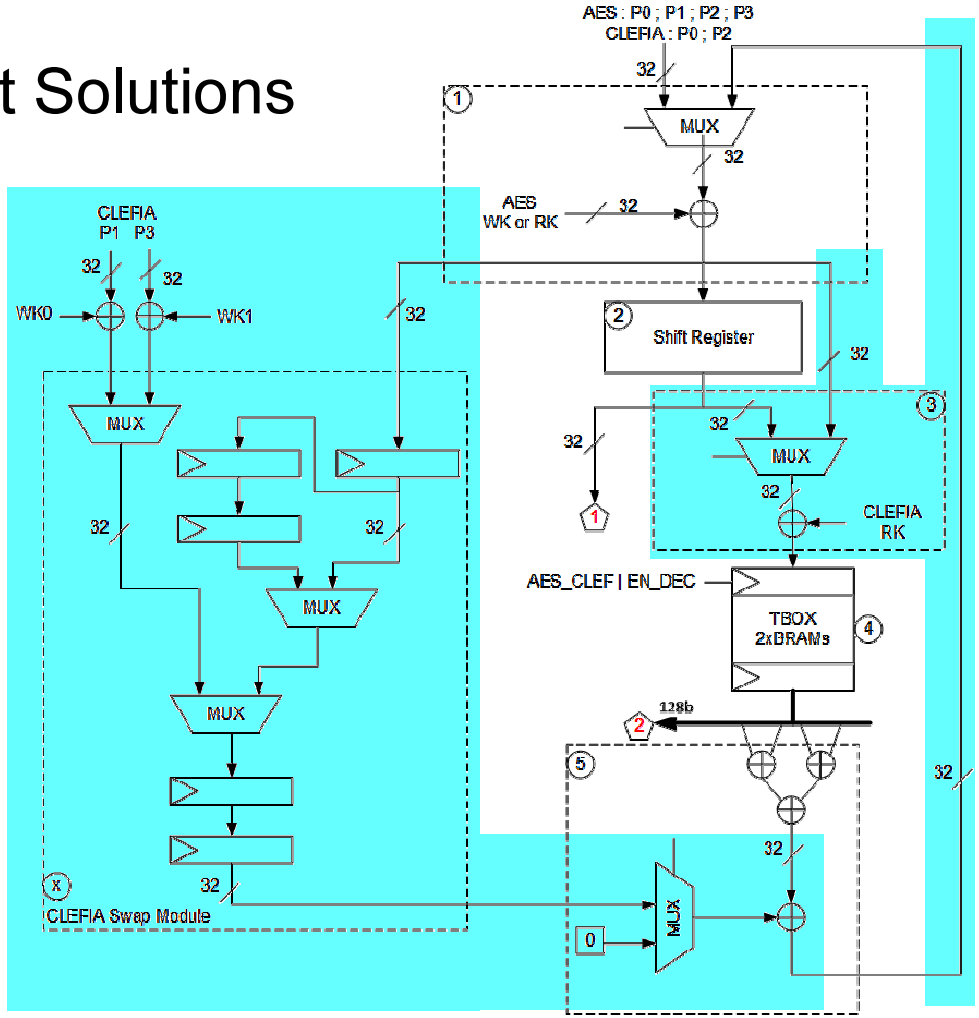




Proposed Architecture: Combined Solutions

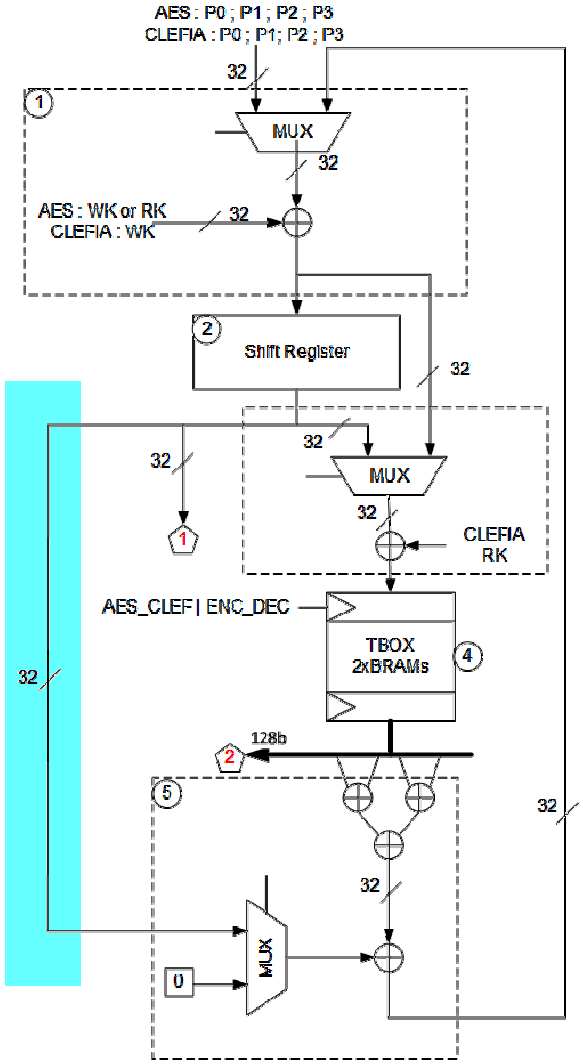
- Combining State of the Art Solutions
  - Initial Whitening Keys
  - Shift Register for AES
  - BRAM based T-Boxes
  - Feedback and Forwarding
  - CLEFIA Feistel Word Swap

(by Proença et al.)



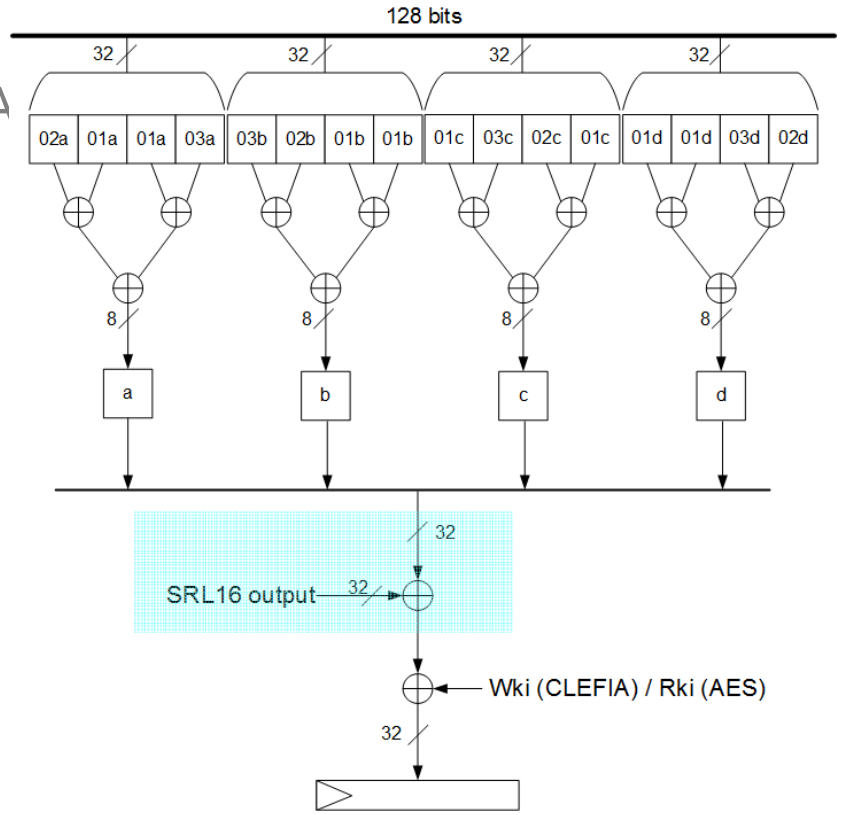
Proposed Architecture: Improved Solution

- Combining State of the Art Solutions
  - Initial Whitening Keys
  - Shift Register for AES & CLEFIA (this work)
  - BRAM based T-Boxes
  - Feedback and Forwarding



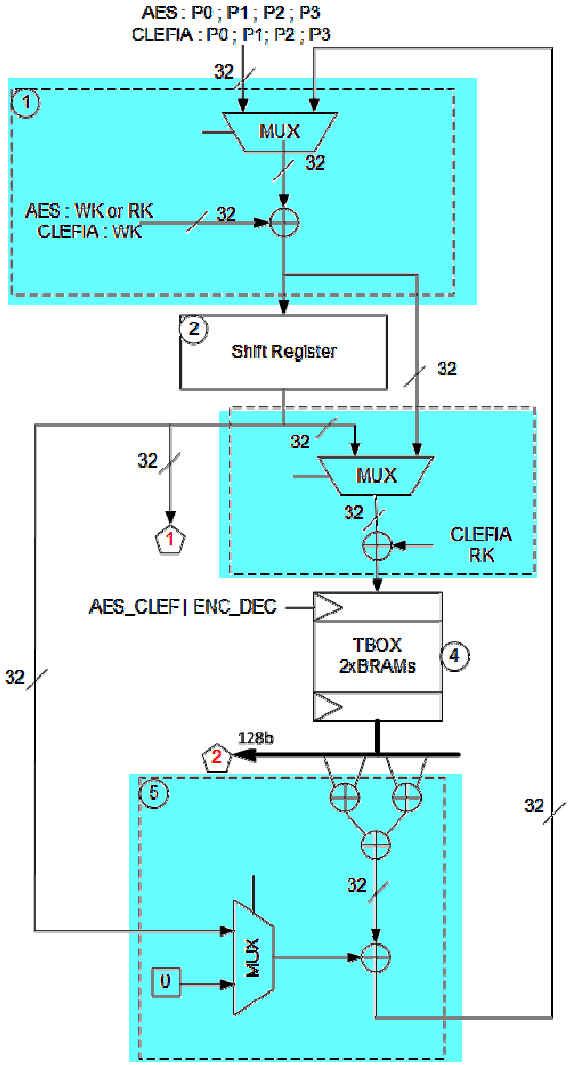
Proposed Architecture: Improved Solution

- Combining State of the Art Solutions
  - Initial Whitening Keys
  - Shift Register for AES & CLEFIA
  - BRAM based T-Boxes
  - Feedback and Forwarding
  - CLEFIA Round Key
  - CLEFIA Feistel Word Swap
  - Reduced Output Stage (LUT6)



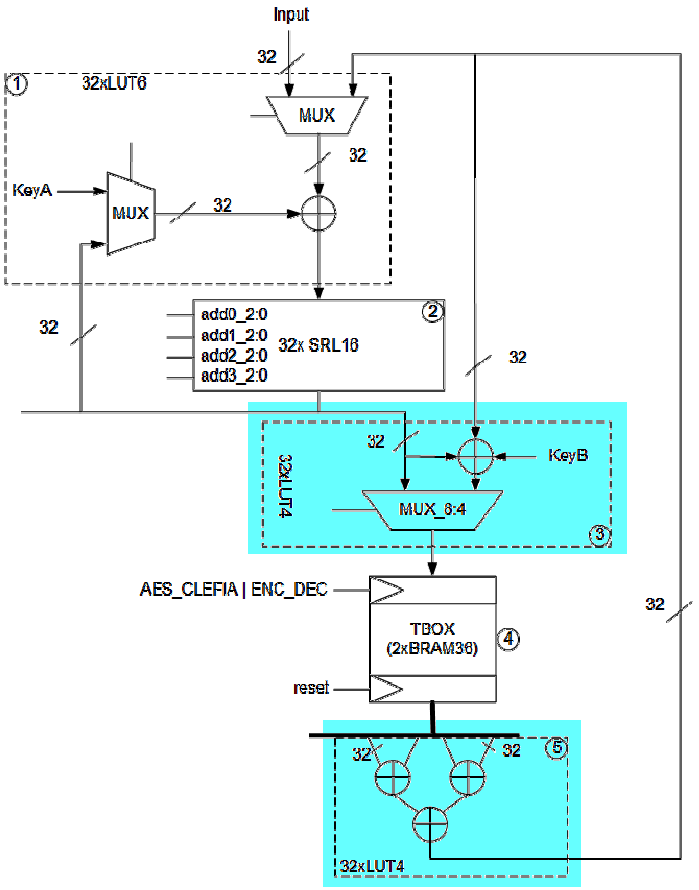
Proposed Architecture: Improved Solution

- Improving and Implementing
  - Shift Register for AES & CLEFIA
  - Reduced Output Stage
  - Reducing Critical Path
    - 3 levels of logic



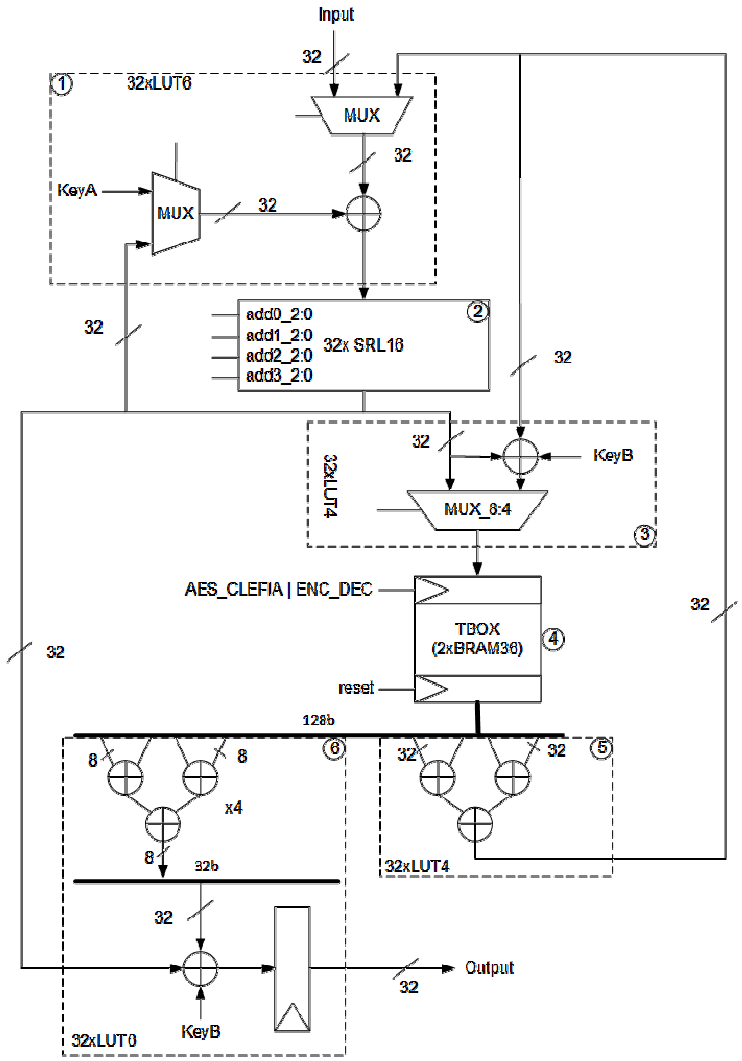
Proposed Architecture: Improved Solution

- Improving and Implementing
  - Shift Register for AES & CLEFIA
  - Reduced Output Stage
  - Reducing Critical Path
    - 2 levels of logic (LUT4)



Proposed Architecture: Improved Solution

- Compact CLEFIA & AES Dual Cipher FPGA core.
  - Shift Register for AES & CLEFIA
  - Reduced Output Stage
  - Reduced Critical Path
  - Total of 160 LUTs + 2 BRAMs



Result Analysis

- State of the Art Comparison (single block)

		Round Structure	Device	Resources		Throughput	Efficiency
				Slices	BRAMs	[Gbps]	[Mbps/S]
Kryjak		Unrolled	V5	2479	0	**1,188**	0,48
Proença		Rolled(128b)	V5	170	4+1	1,707	**10,04**
		Rolled(32b)		**86**	2+1	1,301	**15,13**
Ours	CLEFIA	Rolled(32b)	V5	123	2+1	1,073	**8,72**
	AES					0,85	**6,91**
	CLEFIA		V6	115		1,012	**8,80**
	AES					0,802	**6,97**
Chaves		Rolled(32b)	V5	407	8+2	**2,427**	5,96
Drimer		Rolled(32b)	V5	107	2+1	0,88	8,22
				212	2+1	0,88	4,15
Liu		Unrolled	V5	3579	0	**2,305**	**0,64**
			V6	3121		**3,206**	**1,03**
Bulens		Rolled(128b)	V5	400	0	1,07	2,67
				550		1,07	1,94

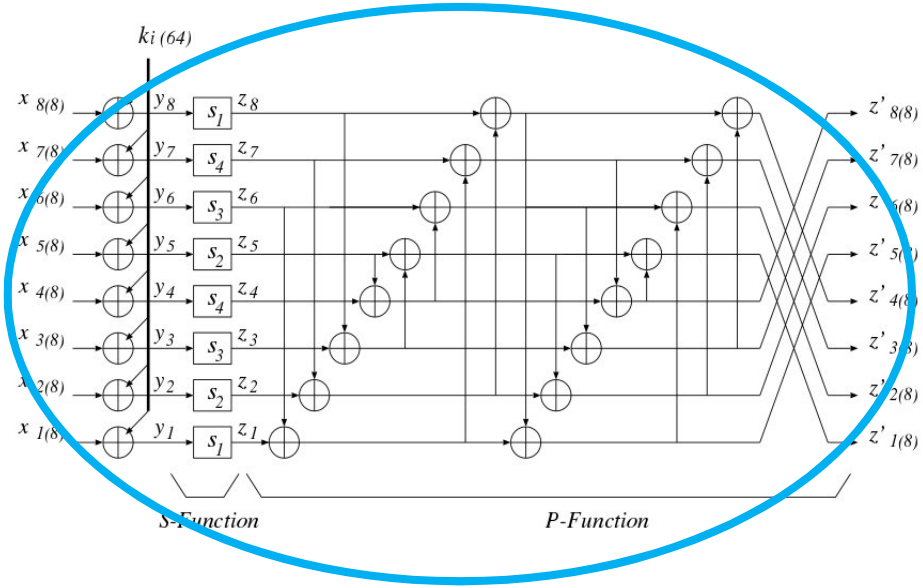
Conclusions

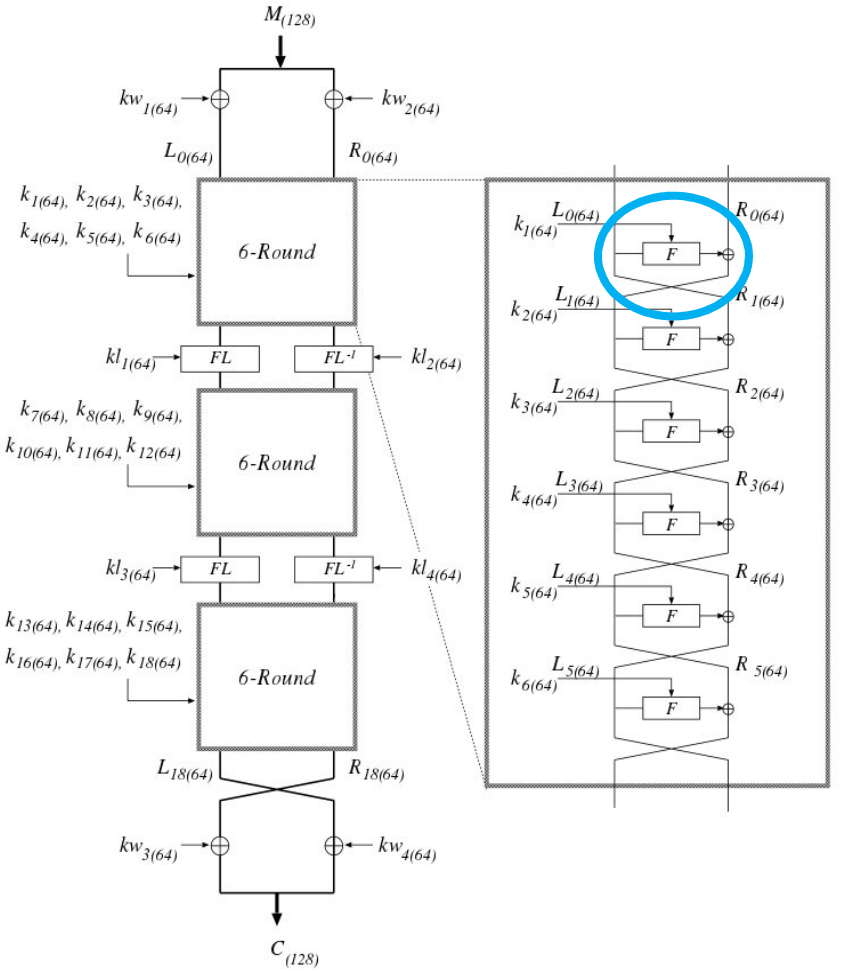
- Compact Dual-Cipher CLEFIA & AES FPGA Core
  - 2 Algorithms
  - 123 Slices+3 BRAMs
  - Max. Freq.: 352 MHz
- Througputs
  - AES: 0,8 Gbps (33% less than best rolled implementation)
  - CLEFIA: 1 Gbps (no alternative surpasses the 2Gbps mark)
- Efficiency
  - AES: Best efficiency with 6,91 Mbps/Slice
  - CLEFIA: 8.72 Mbps/Slice (42% less than best fully dedicated)

Future work

The CAMELLIA Block Cipher

- CAMELLIA
  - Feistel cipher
  - 2 x 64 bit datapath
  - Main operations:
    - Sbox, XORs, and permutations





From: http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/06_01espec.pdf

Future work

The PRESENT Block Cipher

- PRESENT
  - Ligtweight block cipher
  - Block Size 64 bits
  - Main operations:
    - Sbox, XORs, and permutations