Efficient Hardware Accelerator for AEGIS-128 Authenticated Encryption

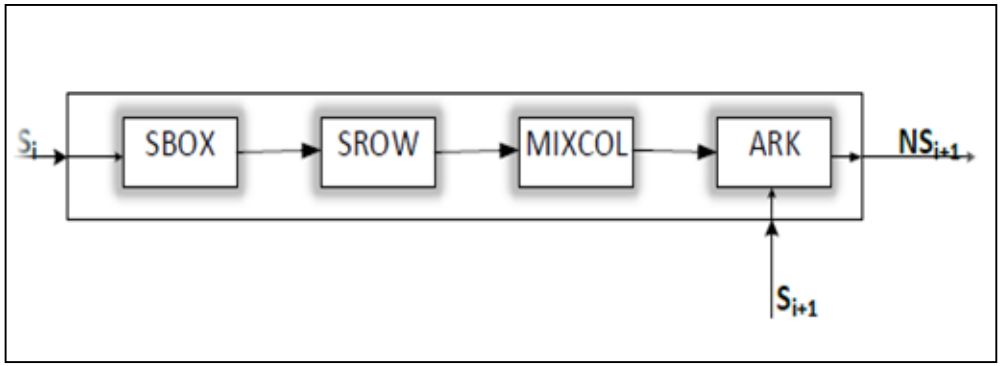
Debjyoti Bhattacharjee and Anupam Chattopadhyay

KAAI Research Group

School of Computer Engineering, NTU, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY

A brief introduction of AEGIS-128



AES Round Operation

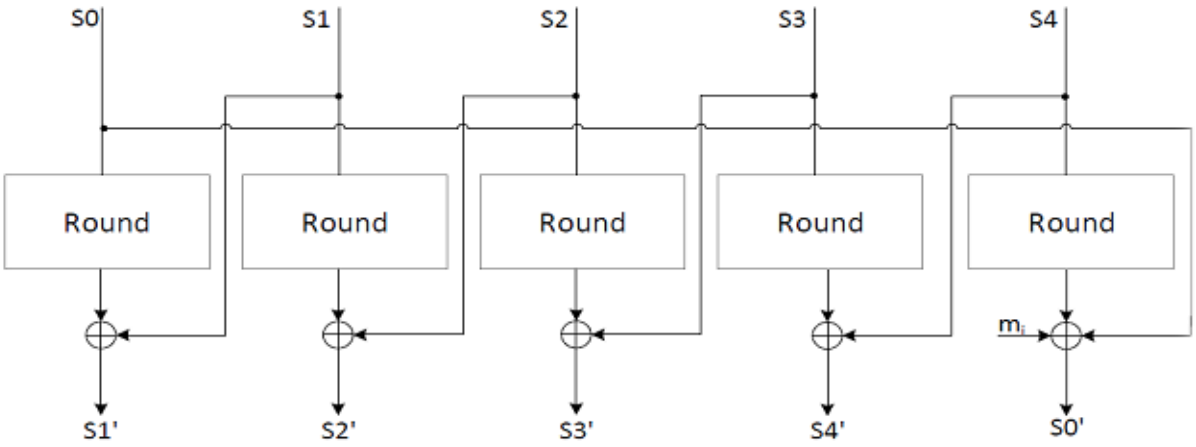
- Authenticated encryption algorithm in the currently ongoing CAESAR competition.
- Processes 80-byte state vector in a state update operation
- State update uses **5 AES rounds** in parallel to update the 80-byte state.

Motivation

- Among nearly 50 entries reported to CAESAR, nearly 1/5th are based on AES .
- High-performance and area-efficient AES-based authenticated encryption schemes have been reported, which makes AEGIS an important candidate in the current port-folio of CAESAR.
- No attacks on AEGIS have been reported so far.

Theoretical Analysis of AEGIS for Cycle-per-Byte

- *msglen* = length of plaintext
- *adlen* = length of associated data
- Assume 128-bit tag generation by AEGIS-128.



StateUpdate128 operation

Theoretical Analysis of AEGIS for Cycle-per-Byte

No of cycles required to complete one round of StateUpdate128

Process Associated data

$$cpb = n(10 + \left\lceil \frac{adlen}{128} \right\rceil + \left\lceil \frac{msglen}{128} \right\rceil + 7)/(\frac{msglen}{8})$$

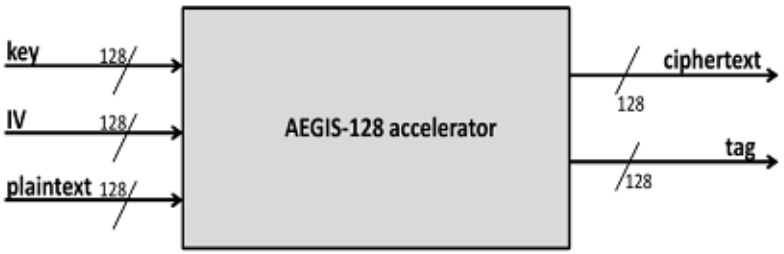
initialization

Encryption

Finalization

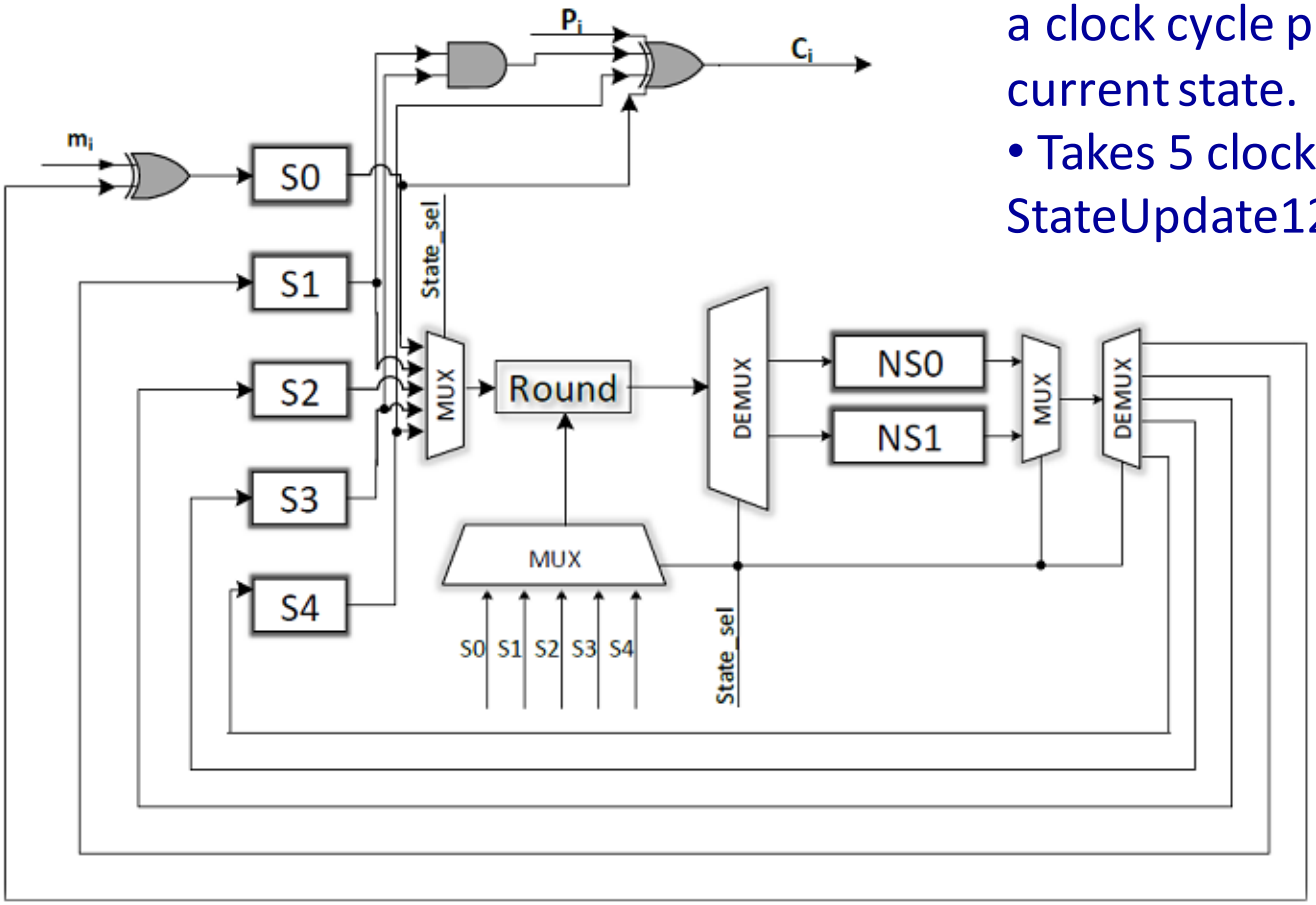
Accelerator Implementation of AEGIS-128

Top Level Structure of AEGIS-128



- Same top-level structure used for all the design variants.
- Theoretical guidelines for improving cpb are used.
- Possibilities for reducing the storage are explored.

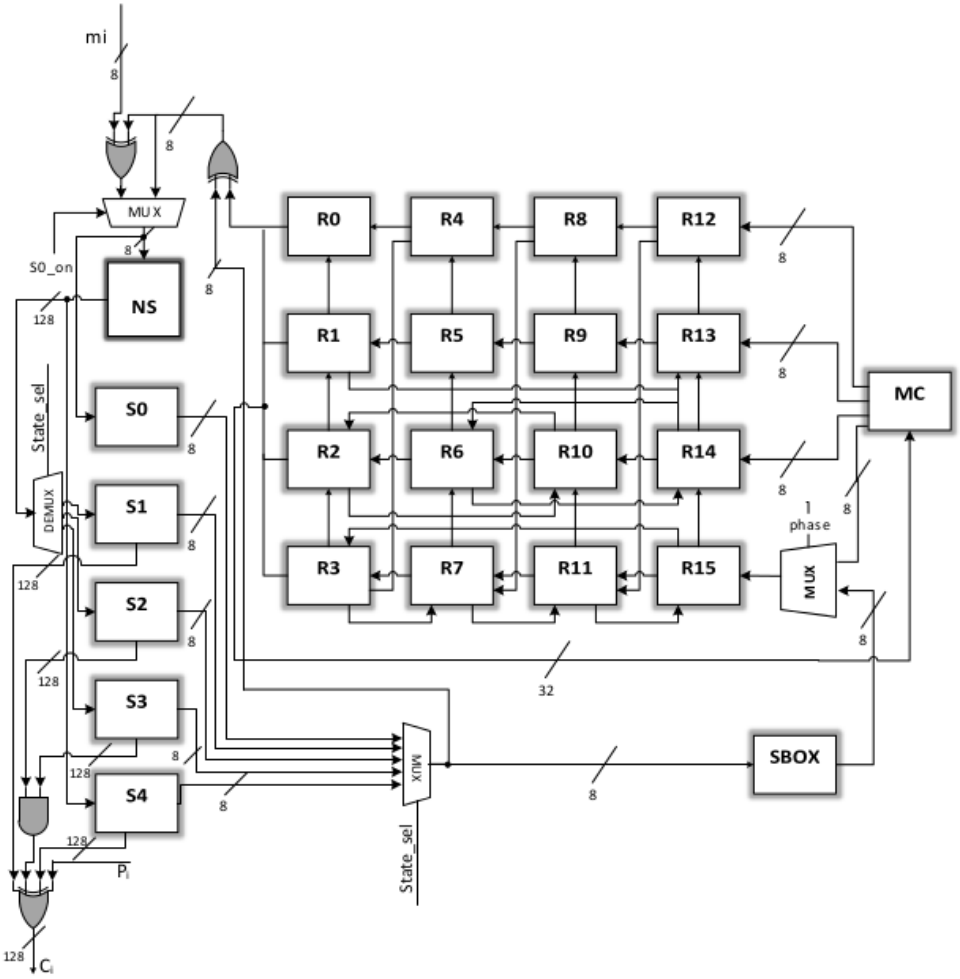
Base Implementation



- A single AES Round is executed in a clock cycle processing 128-bit of current state.
- Takes 5 clock cycles to complete a StateUpdate128 operation

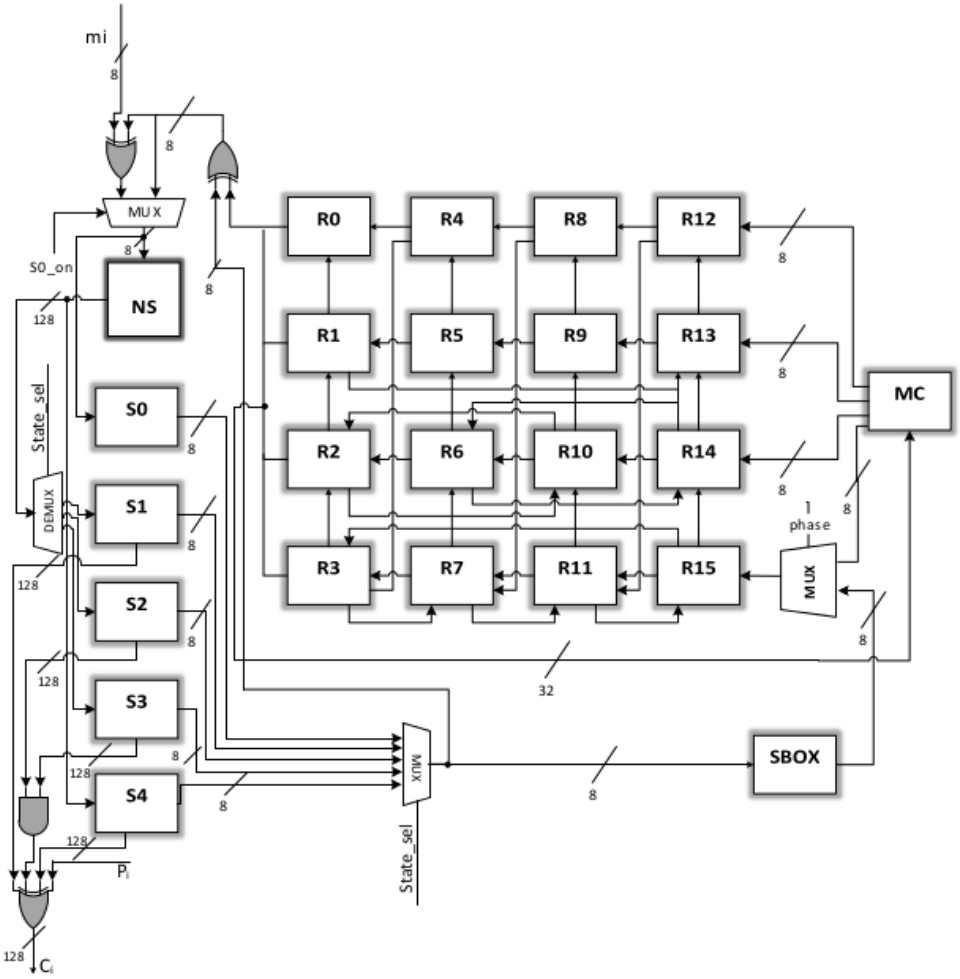
3 out of 5 next state registers have been removed by optimization.

Area Optimized Design Point AO_1



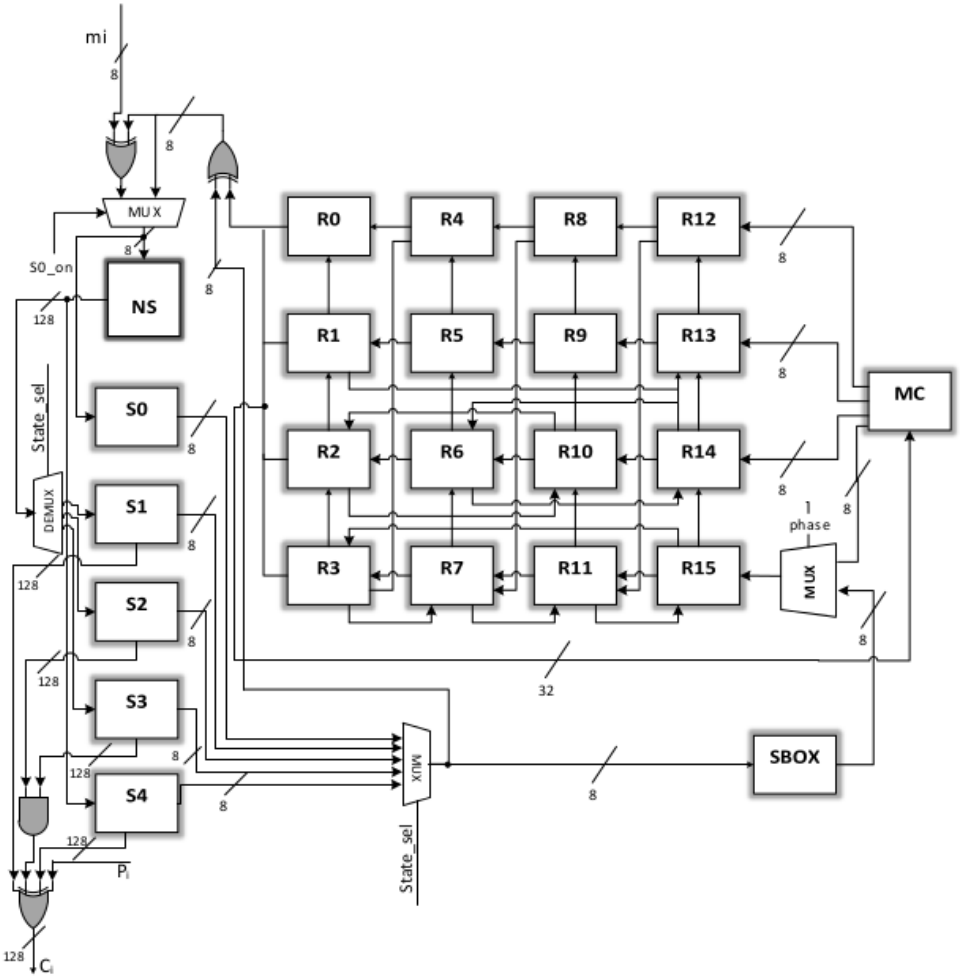
- Canright's implementation of SBOX is used to process 8 bits of state/cycle.
- 16 clock cycles required to load the SBOX result of a 128-bit state Si to the sixteen 8-bit registers R0· · · R15.
- Perform Shift Rows operation in 1 clock cycle, since it just involves data shuffling among the registers.

Area Optimized Design Point AO_1



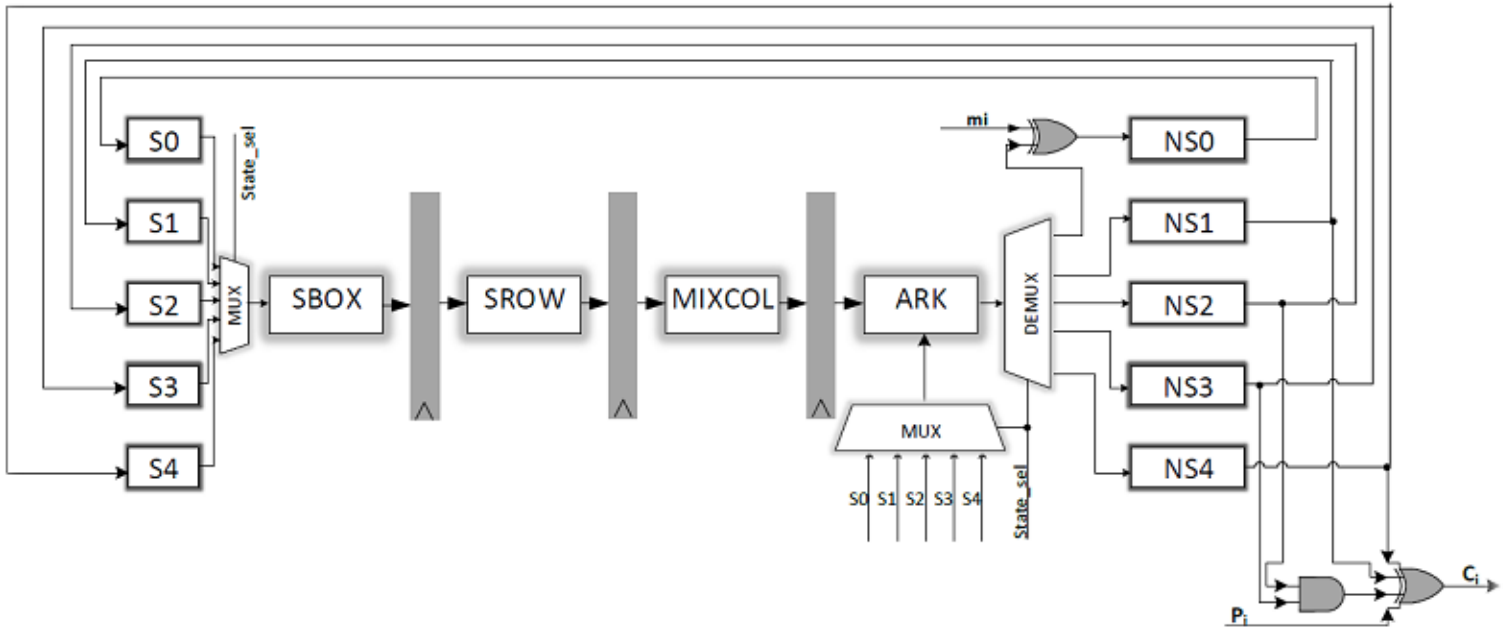
- Left shift the registers column-wise, shifting out the registers [R0,R4,R8,R12], which serves as input to mix columns(MC) logic block.
- 32-bit output of MC logic block in each clock cycle, is loaded back to the register column [R3,R7,R11,R15].
- Requires 4 cycle for MC to complete.

Area Optimized Design Point AO_1



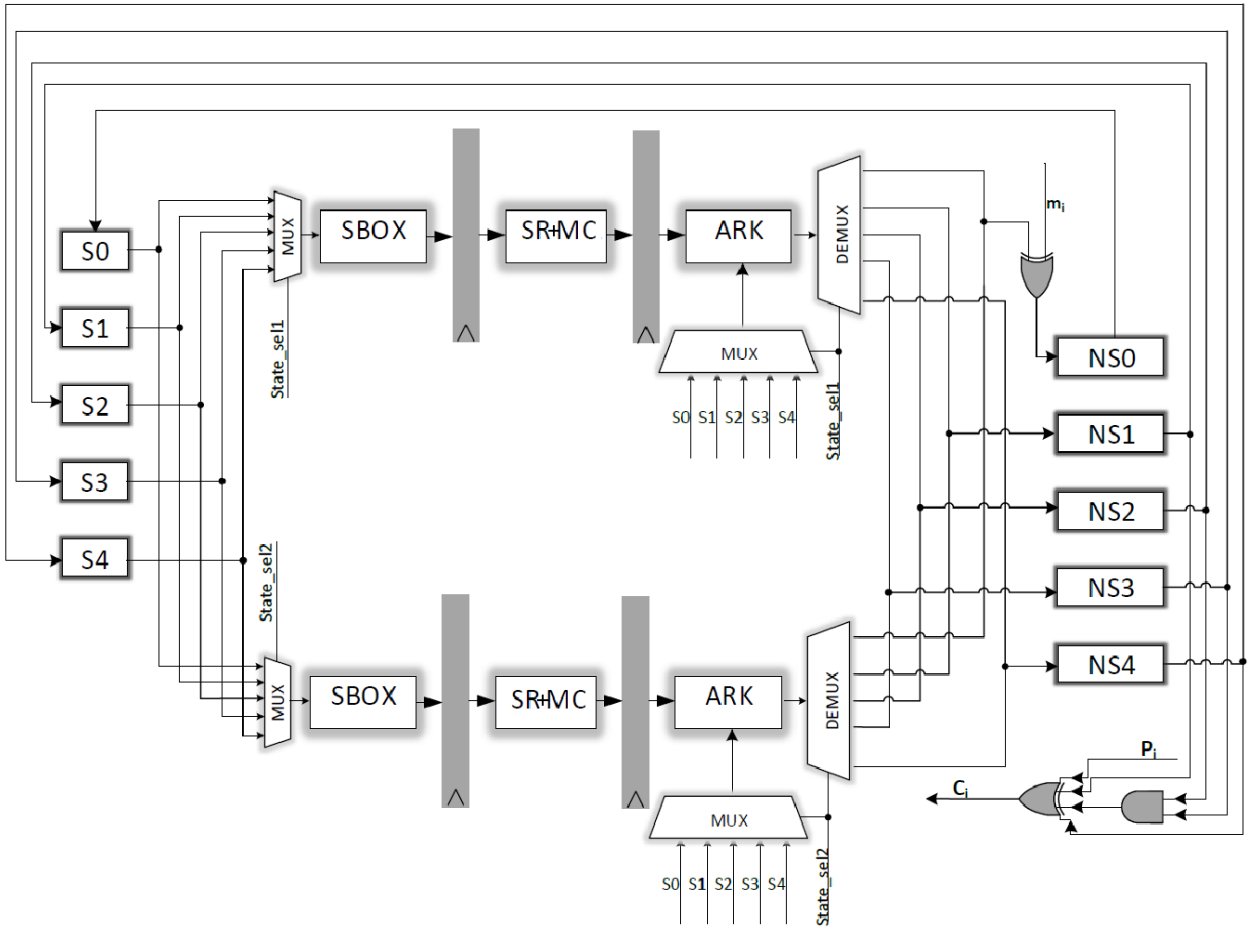
- Add Round Key (ARK) step is executed 8-bit at a time.
- Requires 16 clock cycles to complete update of the 128-bit state Si.
- Single next state register used in this design. (kindly refer to the paper for details).

Area Optimized Design Point AO_2



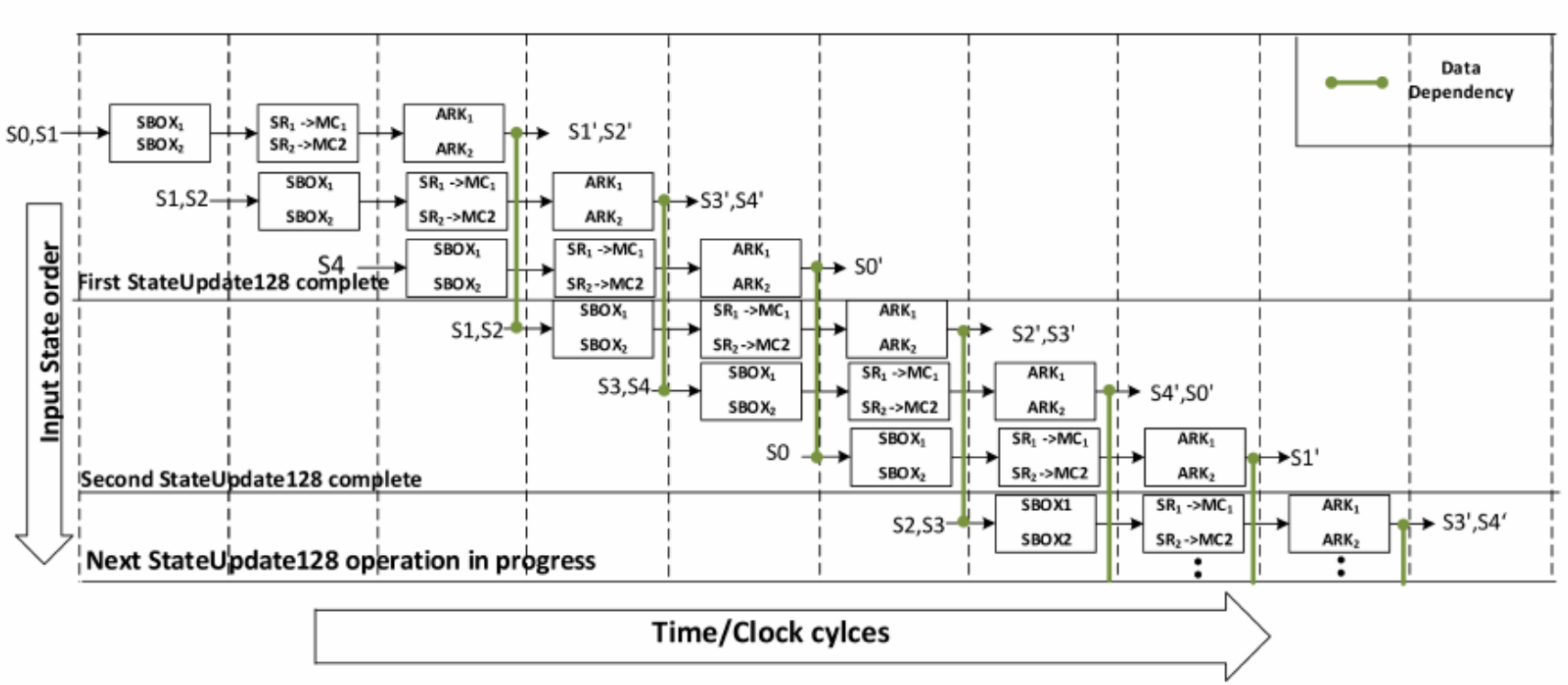
- Uses a 4-stage pipeline.
- Improves on the maximum operating frequency
- 128-bit data-path.
- Each stage requires a single clock cycle to process its input.

Throughput optimized design point TO_1

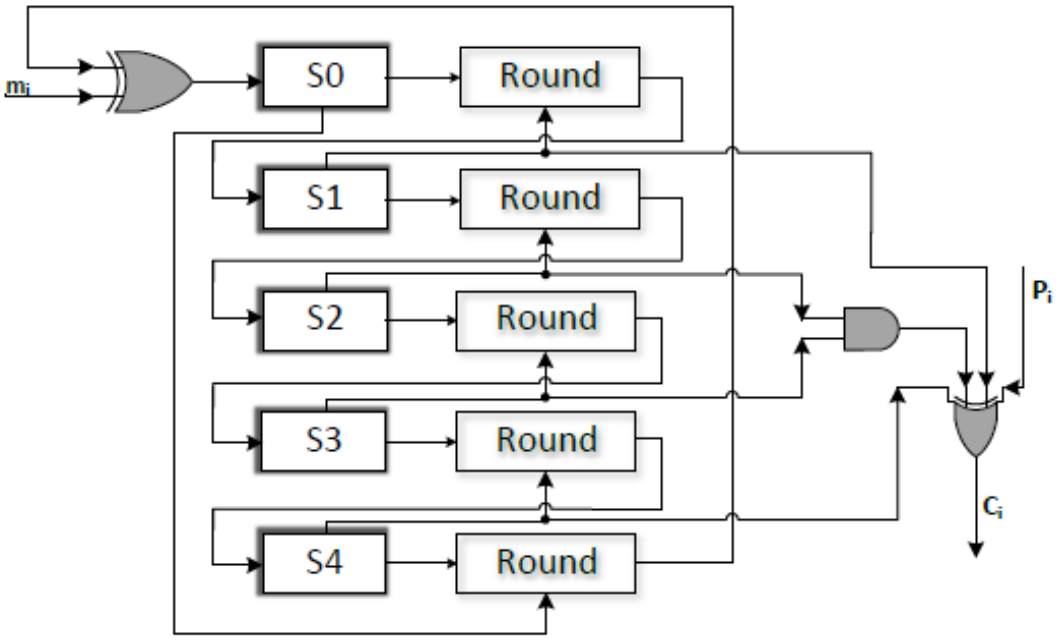


- Equipped with two parallel pipelines for higher throughput.
- 3 pipeline stages namely SBOX, SR+MC,ARK.
- 2 identical functional units in each stage.

Pipeline Schedule of design point TO_1

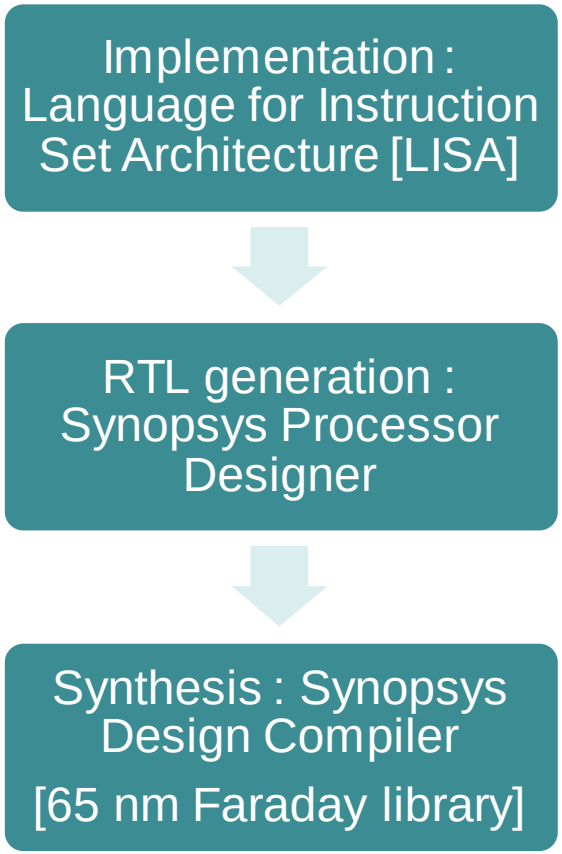


Throughput optimized design point TO_2



- Writes back the updated state value into the state registers directly.
- Control logic is minimal when compared to the other implementations.
- Requires a single clock cycle for the StateUpdate128 operation.

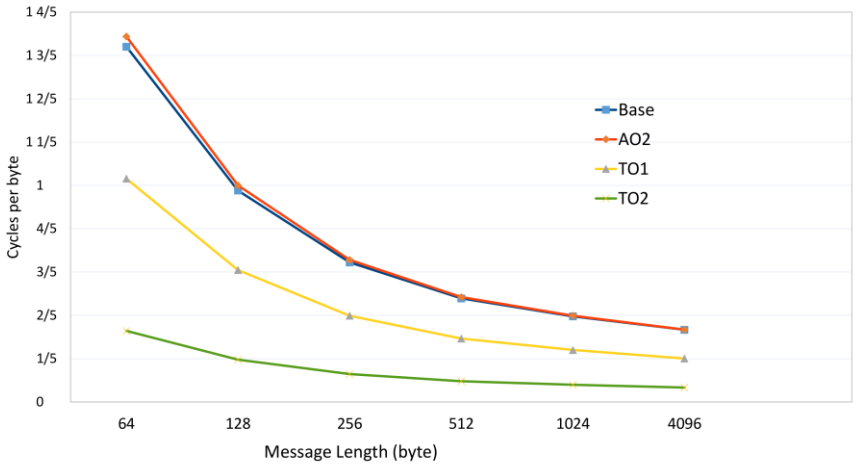
Hardware implementation details



Performance of AEGIS-128 accelerator in cycles per byte

Design	Message Length					
	64B	128B	256B	512B	1024B	4096B
Base Implementation	1.64	0.98	0.64	0.48	0.40	0.33
Area optimization						
AO_1	33.06	19.66	12.95	9.60	7.93	6.67
AO_2	1.69	1.00	0.66	0.48	0.40	0.33
Throughput optimization						
TO_1	1.03	0.61	0.40	0.29	0.24	0.20
TO_2	0.33	0.20	0.13	0.10	0.08	0.07
Software Implementation						
AEGIS(EA)[3]	3.37	1.99	1.30	0.96	0.8	0.66

Table 2. Performance of AEGIS architectures in cycles per byte



Performance of AEGIS-128 architectures

Design	Optimization	Clock Frequency (MHz)	Area (KGE)	Throughput (Gbps)	Efficiency (Gbps/kGE)	Total Power (mW)	Energy Efficiency (pJ/bit)
Base Implementation	Speed	915	59.34	17.04	0.29	74.41	4.07
	Area	915	57.01	17.04	0.30	64.65	1.06
AO_1	Speed	1435	20.55	1.35	0.07	21.96	15.17
	Area	1410	18.72	1.32	0.07	21.58	15.17
AO_2	Speed	2010	60.88	37.44	0.61	33.08	0.82
	Area	1962	56.65	36.55	0.65	34.21	0.87
TO_1	Speed	1725	88.91	53.55	0.60	28.33	0.49
	Area	1700	84.71	52.77	0.62	28.33	0.50
TO_2	Speed	1300	172.72	121.07	0.70	232.75	1.79
	Area	1300	172.72	121.07	0.70	232.75	1.79

Table 1. *Performance of AEGIS-128 architectures*

Reported performance of some CAESAR entries

- ICEPOLE :
  42 Gbps – Xilinx Virtex 6
  38.78 Gbps – Altera Stratix IV FPGA.
- Minealpher v1 - 45 nm tech node
  High Speed Core
  -> 6.1 Gbps – timing optimized
  -> 9.1 Gbps – area optimized
- Scream10(2R/cycle) – 65 nm tech node
  5.19 Gbps, 17292 µm^2
- iScream(2R/cycle) – 65 nm tech node
  4.41 Gbps, 17024 µm^2

Conclusion

- Detailed implementation study of AEGIS-128 authenticated encryption algorithm.
- Diverse design points with various performance metrics are implemented
- Pre-layout implementation reports using an ASIC technology library.
- Implementation results are competitive in terms of area
- Significantly superior in terms of throughput.