

---

Fully pipelined AES with speed  
exceeding 20 Gbps using *logic-only*  
implementation of S-box

Presented by

Karthick Ramu  
Chethan Ananth

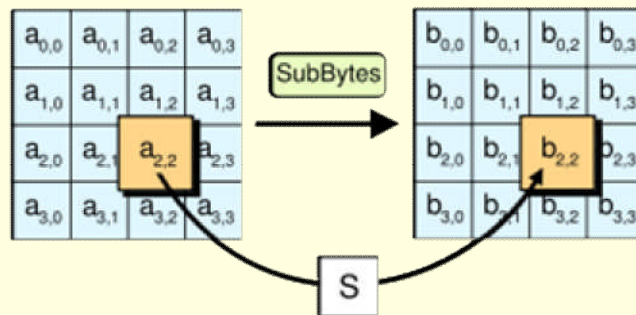
# Background

---

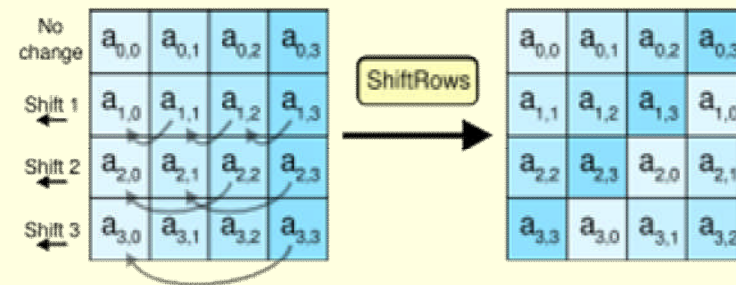
- Requirement of high-throughput rates with the advancement in technology.
- Requirement of low memory (BRAM) utilization in FPGAs.
- Currently throughput rates are limited due to memory access latencies.

# AES- Operations

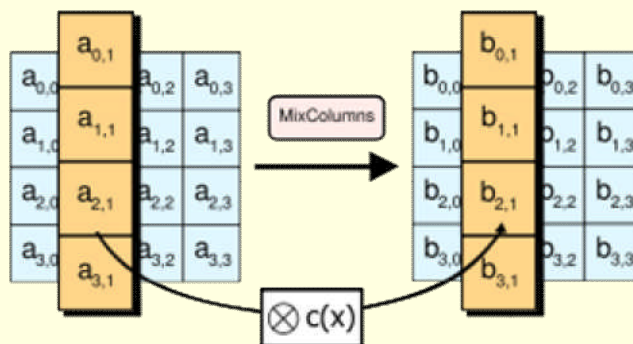
## ■ Subbytes



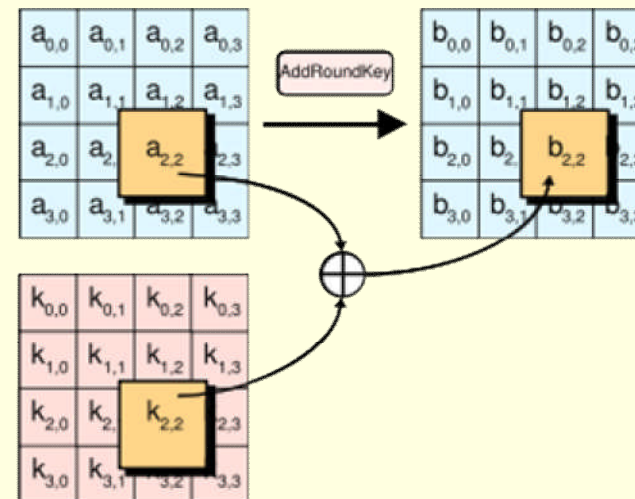
## ■ Shiftrows



## ■ Mixcolumns



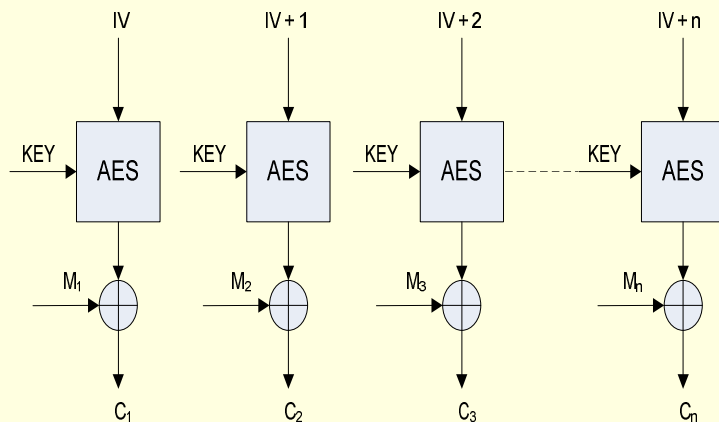
## ■ Addroundkey



# AES – Modes of Operation

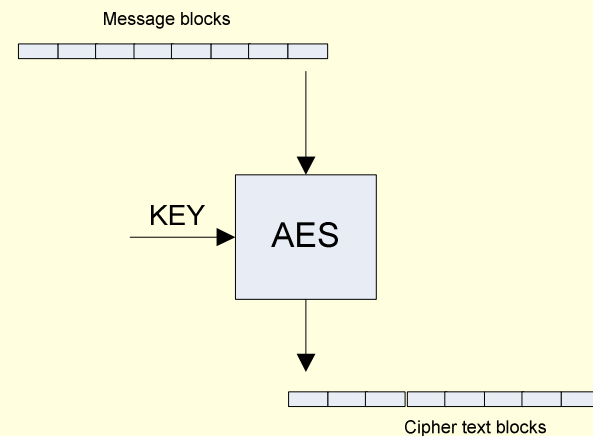
## AES – CTR

- Encrypts successive values of a counter (IV).
- Message XORed with the encrypted output to produce the cipher text
- Same unit for both encryption and decryption



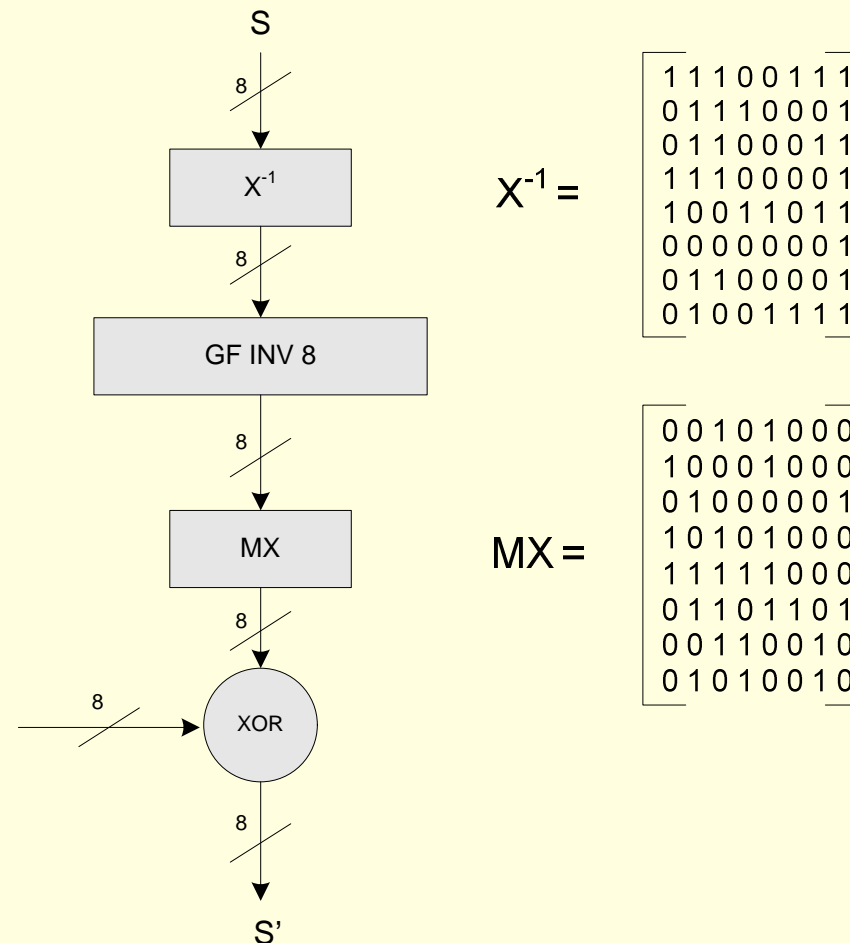
## AES – ECB

- Message divided into blocks and each block encrypted separately
- Disadvantage is that identical plaintext blocks produce identical ciphertext blocks.



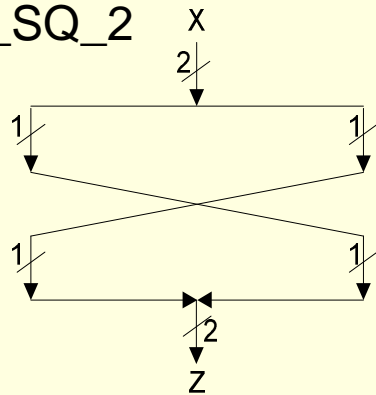
# Subbytes using logic (1)

- Involves computation of multiplicative inverse in  $GF(2^8)$ , affine transformation
- All operations performed on the fly.

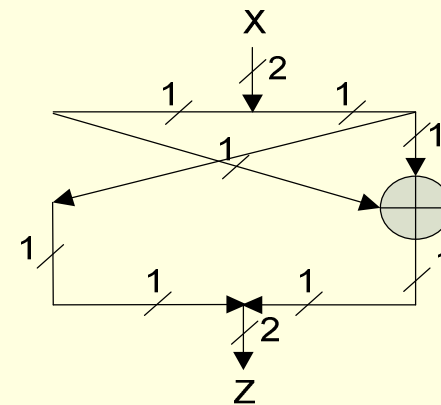


# Subbytes using logic (2)

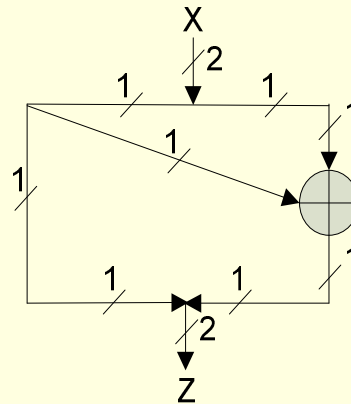
- GF\_INV\_2 and GF\_SQ\_2



- GF\_SCL\_2

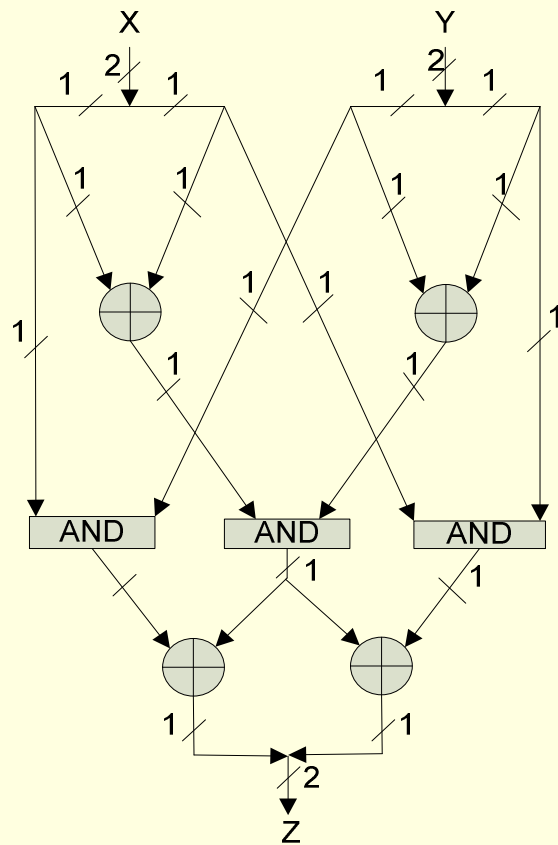


- GF\_SQ\_SCL\_2

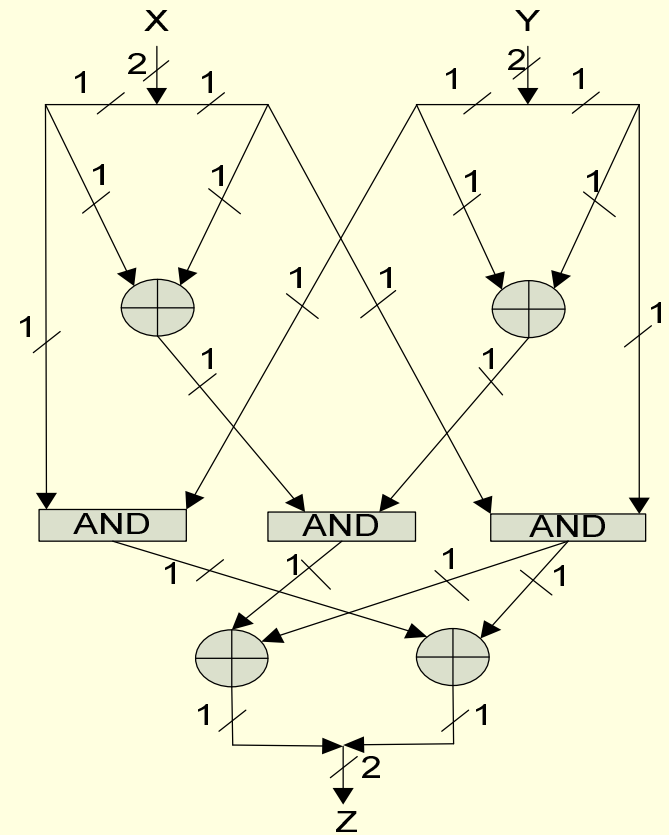


# Subbytes using logic (3)

## ■ GF\_MUL\_2

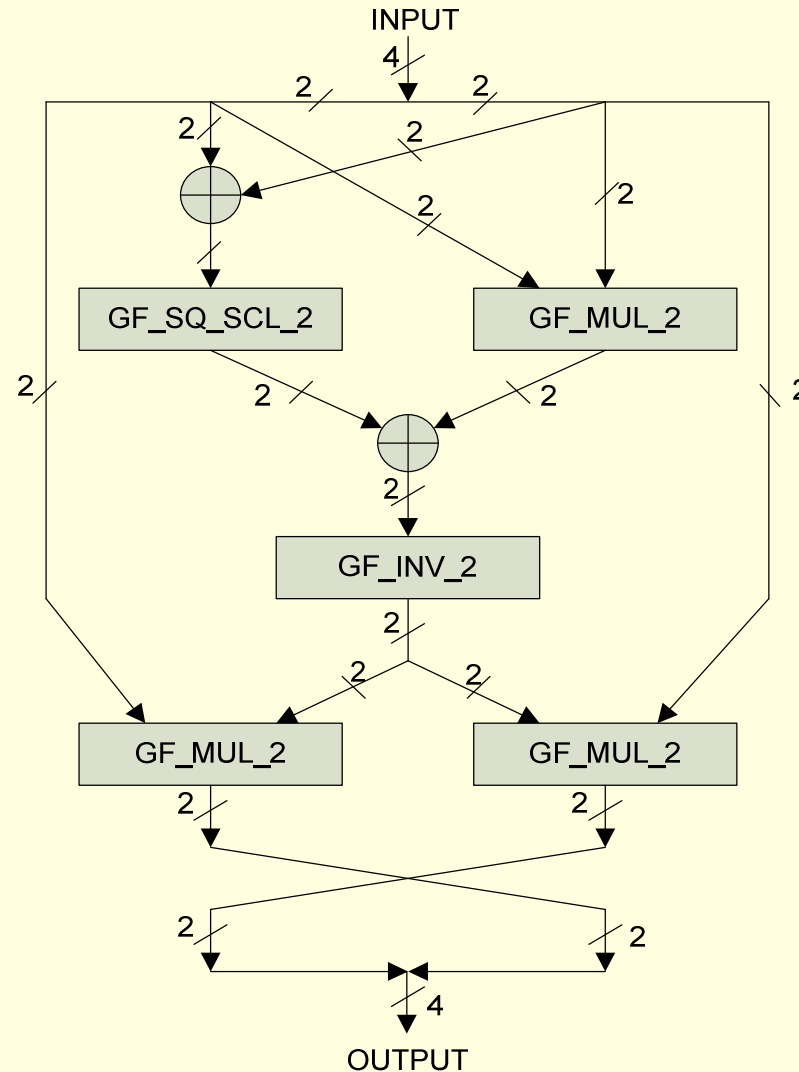


## ■ GF\_MUL\_SCL\_2



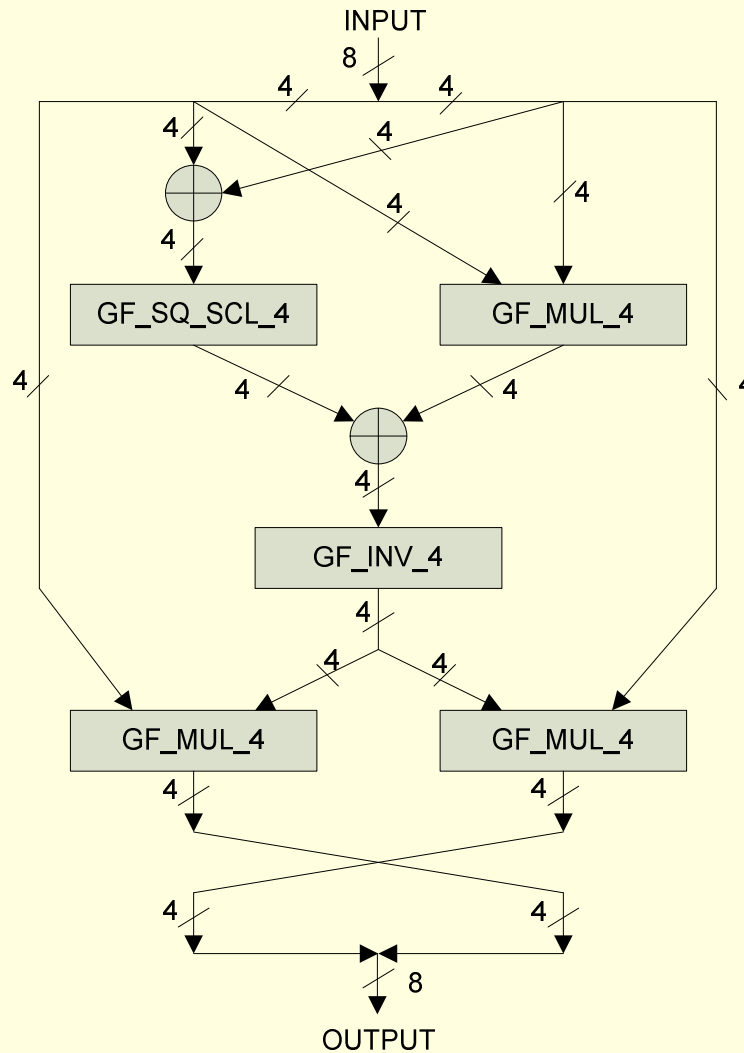
# Subbytes using logic (4)

## ■ GF\_INV\_4

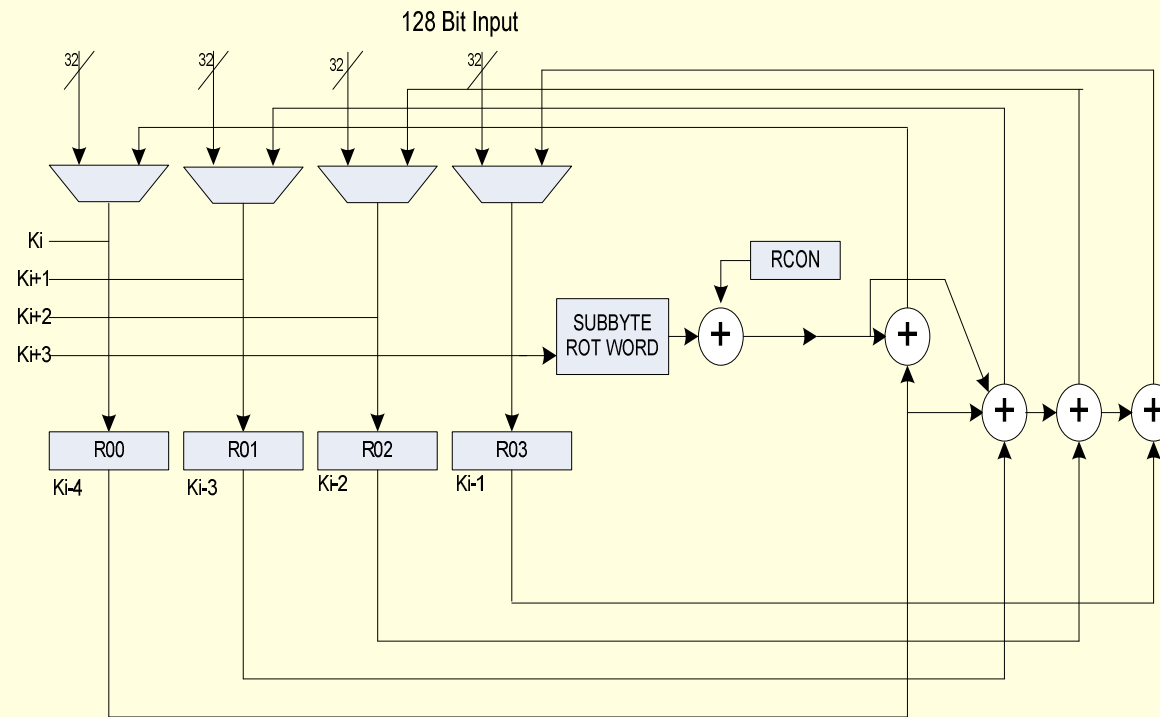


# Subbytes using logic (5)

## ■ GF\_INV\_8

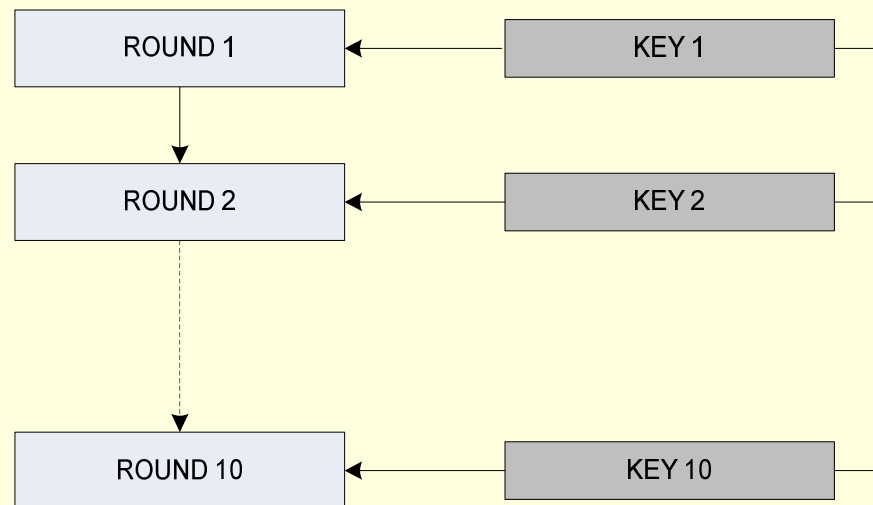


# Round key Generation

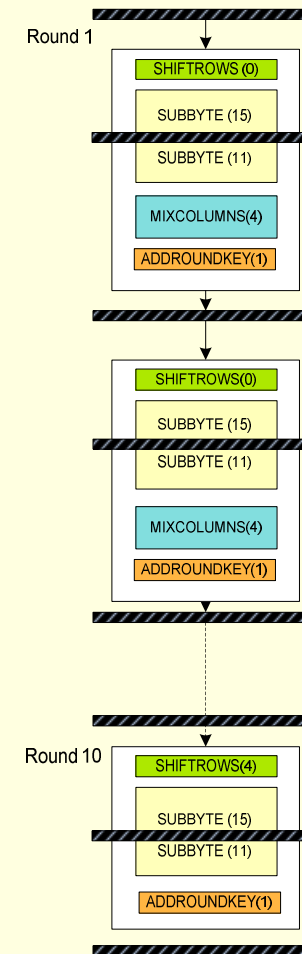
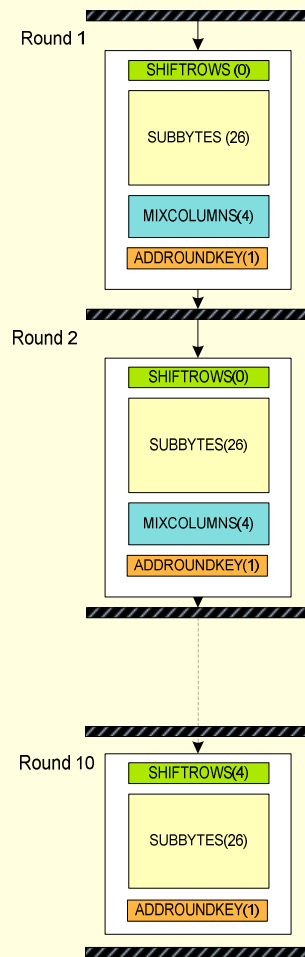


# Key Scheduling

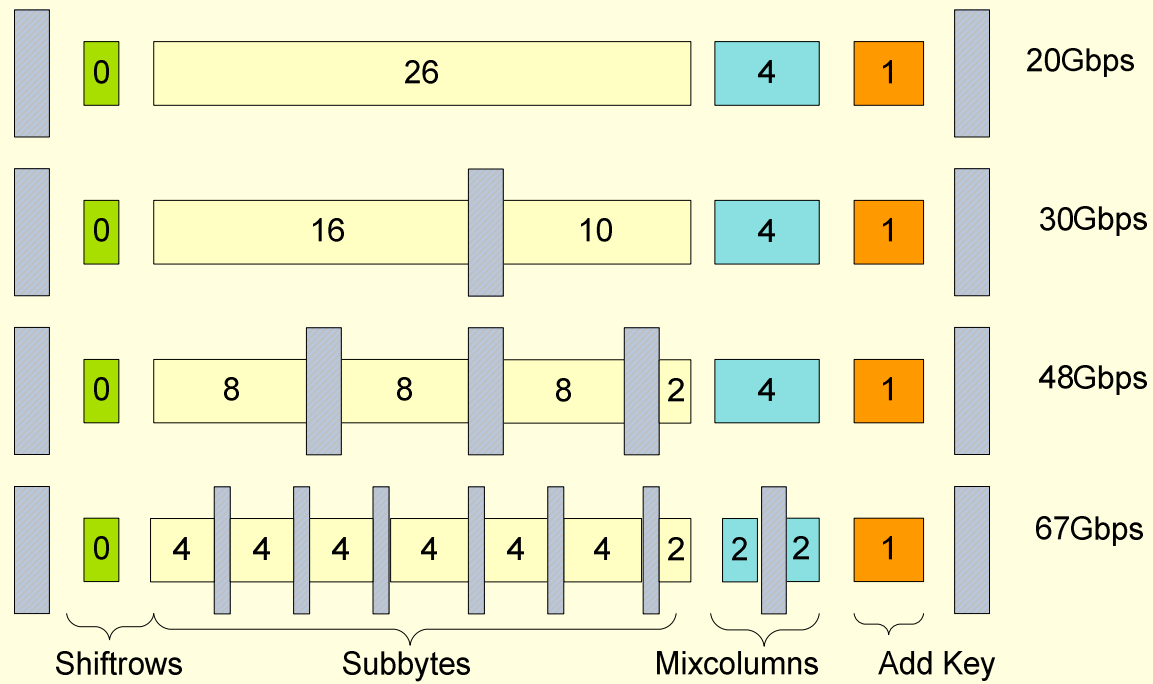
---



# Fully Unrolled and Pipelined



# Balanced Pipelining (ECB)



# Resources

## Tools used

Xilinx 10.1	Synthesis and Implementation
Active HDL 7.2 Modelsim PE	Simulation
Active HDL 7.2	Editor

## Device Specification

Device	Vertex 5
Family	XC5VLX110T
Speed	-2
Package	FX1136
IO Pins	>1136

# Results

## CTR Mode

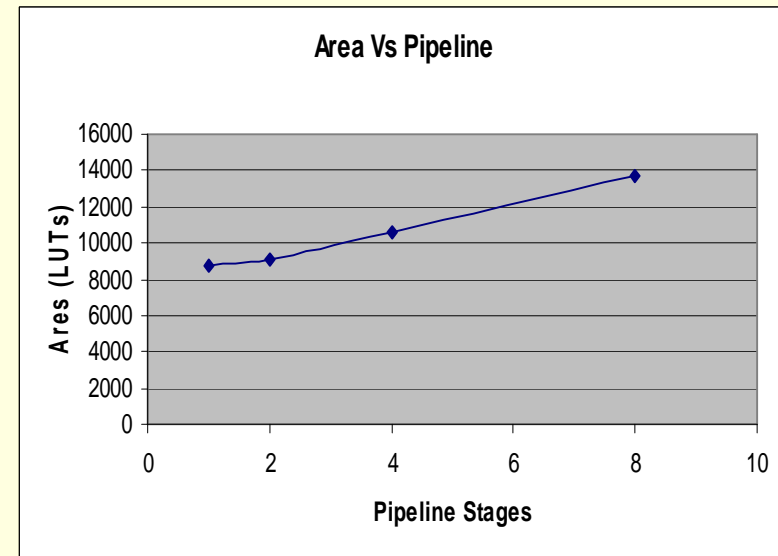
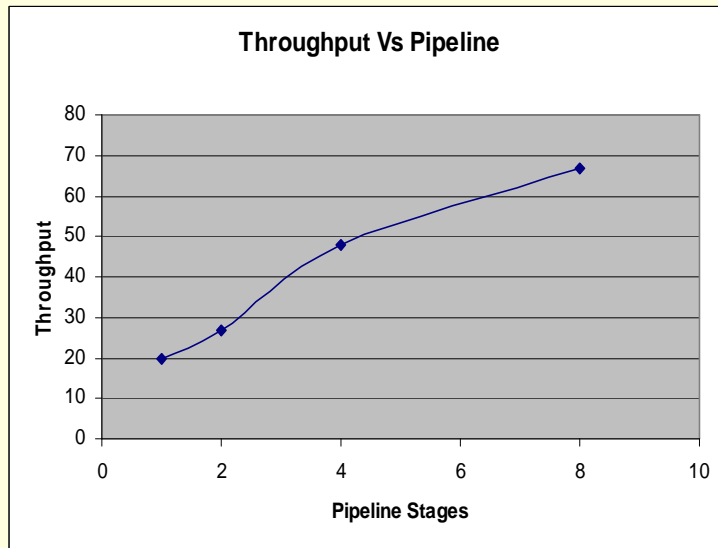
Pipeline K (stages)	Latency (ns)	Throughput (gbps)	Area (slices)	BRAM Utilization
K= 1	<6.250	>20	9,100	0%
K=8	4.545	28	14,100	0%

## ECB Mode

Pipeline K (stages)	Latency (ns)	Throughput (gbps)	Area (slices)	BRAM Utilization
K = 1	<6.250	>20	8,800	0%
K = 2	4.67	27	9,086	0%
K = 4	2.777	48	10,561	0%
K = 8	1.905	67	13,649	0%

K -> Number of pipeline registers in one round

# Observations (ECB Mode)



# Observations

---

## Problems Encountered

- Unable to achieve throughput greater than 28gbps in CTR mode due to the limitation of iv incrementer.
- Pipelining subbytes was not trivial.

## Future Work

- To implement other modes of AES (OFB,CBC).
- To achieve comparable throughput with CTR mode by replacing adders/incrementer with high performance adders (kogge stone).

# Conclusion

---

- More than 20gbps of throughput is achievable with logic only substitution of subbytes.
- Rounds should be unrolled and fully pipelined.
- Throughput increases with increase in pipeline stages in a balanced manner
- Area occupied by unrolling AES to 10 rounds is balanced by using logic only subbytes.
- Absolutely 0% BRAM utilization.



# Questions

???

