



# FPGA Bitstream Security EAX Mode of Operation

Milind M. Parelkar

# FPGA Bitstream Security Issues

## ■ Confidentiality – *Encryption of Bitstream*

- *Decryption Engines on Xilinx FPGAs*

*Xilinx Virtex II Pro – 3DES with 2 keys*

*Xilinx Virtex 4 – AES with 256-bit key*

## ■ Integrity – *Authentication of Bitstream*

- *No Provably Secure Authentication Engine on current generation of FPGAs.*
- *32 bit Checksum for Error Checking*

# Is Encryption Sufficient?

- *Active attacks – Bitstream Tampering  
Bitstream Fabrication*
- *Tampered bitstreams decrypt to gibberish*
- *Gibberish still does **something** on the FPGA*
- *Certain “malignant” bit streams may damage the FPGA*
- *FPGA Virus!!!*

# Authentication Options

- Message Authentication Codes (MACs)
- *Authenticated Encryption Modes of Operation using Symmetric Key Cipher*

# Authenticated Encryption Modes

- ***Authenticated Encryption (AE)***
  - Encrypt for confidentiality
  - Authenticate for integrity
- ***Authenticated Encryption with Associated Data (AEAD)***
  - Supports *associated data* (e.g. packet headers) that should be authenticated but not encrypted

# Generic Composition Schemes

- Separate Algorithm for Encryption and Authentication
- Encrypt – then – Authenticate
  
- Advantages
  - + *Provably Secure*
  - + *Can support Associated Data – AEAD scheme*
  - + *Unpatented*
  
- Disadvantages
  - *Strict IV Requirements*
  - *Separate Keys for Encryption and Authentication*
  - *Longer key-setup time*
  - *No standard, User's choice of algorithms*

# Provably Secure One-Pass AE Schemes

- Examples – IAPM, OCB, XCBC
- Advantages
  - + *Encrypt and authenticate in one pass*
  - + *Fast* – takes about  $n$  block cipher calls to process  $n$  blocks of data
- Disadvantages
  - *Some modes cannot handle Associated Data*
  - *Patent encumbered*

# Unpatented Two-Pass AEAD Schemes

- Examples –

**CCM** (*CTR + CBC-MAC*)

**EAX** (*CTR + OMAC*)

- Advantages

- + *Single Key for Encryption and Authentication*

- + *Less Parameters of User's Choice, hence more secure*

- Disadvantages

- *Two-pass modes are typically ~ 2x slower than one-pass modes, in software*

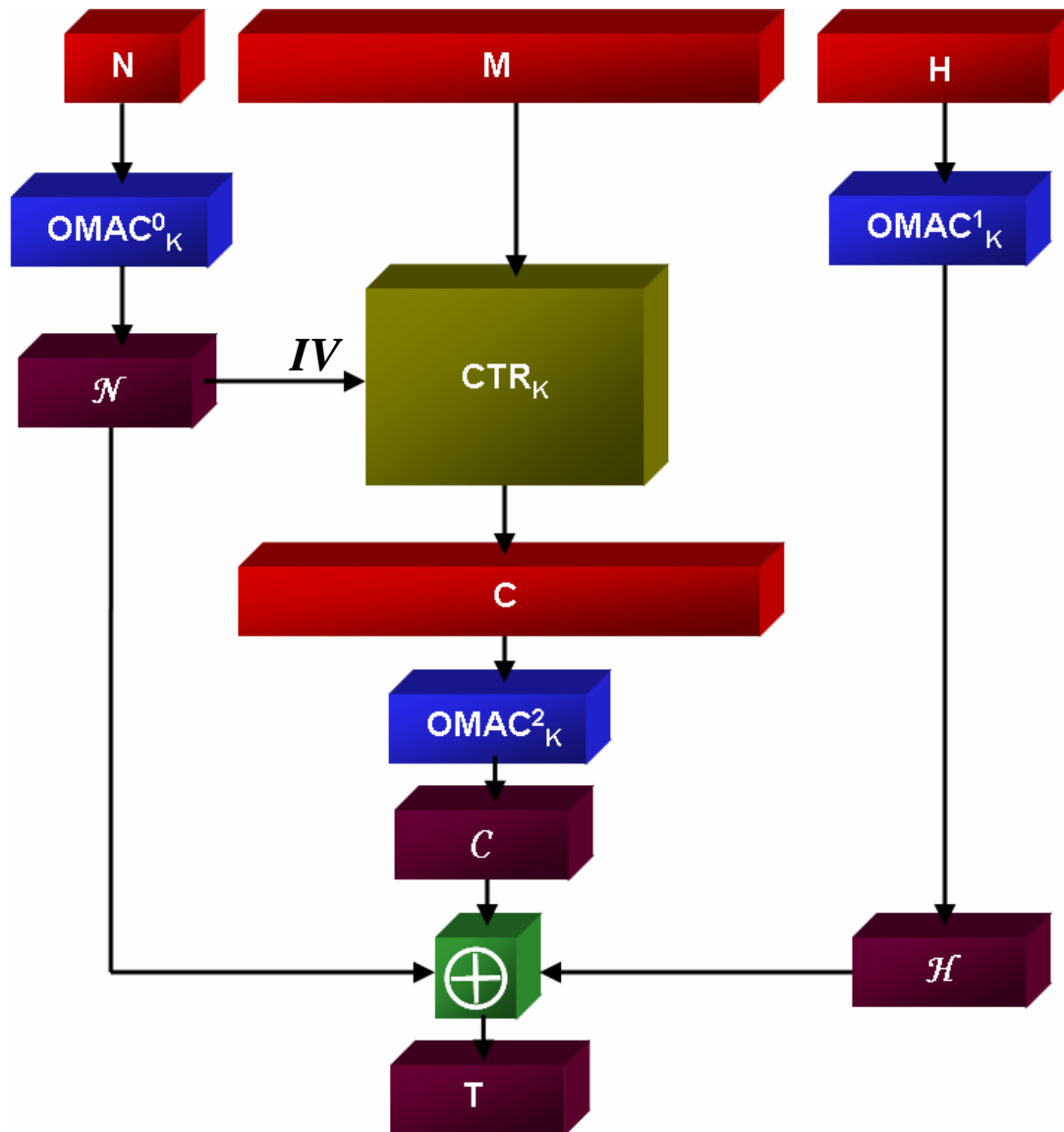
# Comparison of Two-Pass AEAD Schemes

	<b>CCM</b>	<b>EAX</b>
Provably secure?	✓	✓
Unpatented?	✓	✓
Any length nonce?	✗	✓
One key?	✓	✓
On-line?	✗	✓
Can preprocess static headers/AD?	✗	✓
Fully parallelizable?	✗	✗
Preserves alignment?	✗	✓
Fully specified?	✓	✓

# Tasks Performed

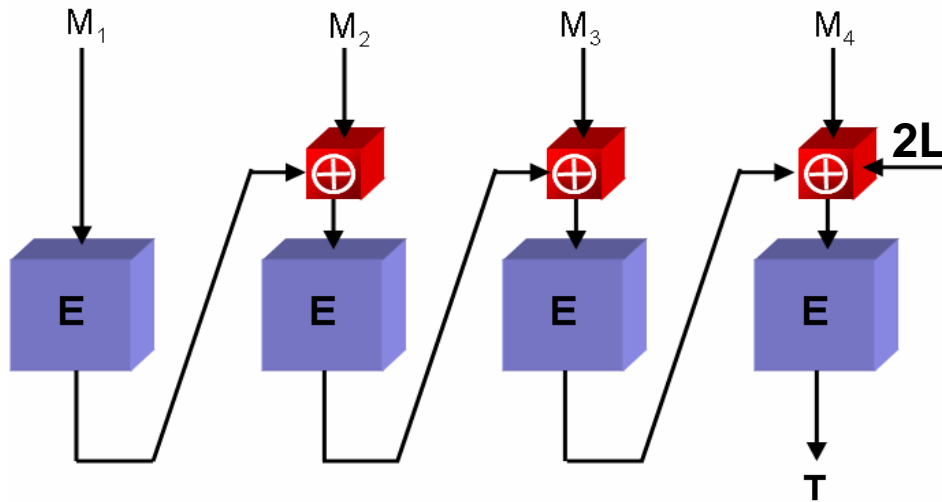
- Implemented EAX Mode of Operation using RTL VHDL
- Synthesized the circuit for both FPGA and ASIC environment
- Implemented the circuit targeting Xilinx Virtex II FPGAs
- Modified an already existing AES Implementation for ASIC synthesis

# EAX Encryption and Signature Generation



# “Tweaked” OMAC Algorithm

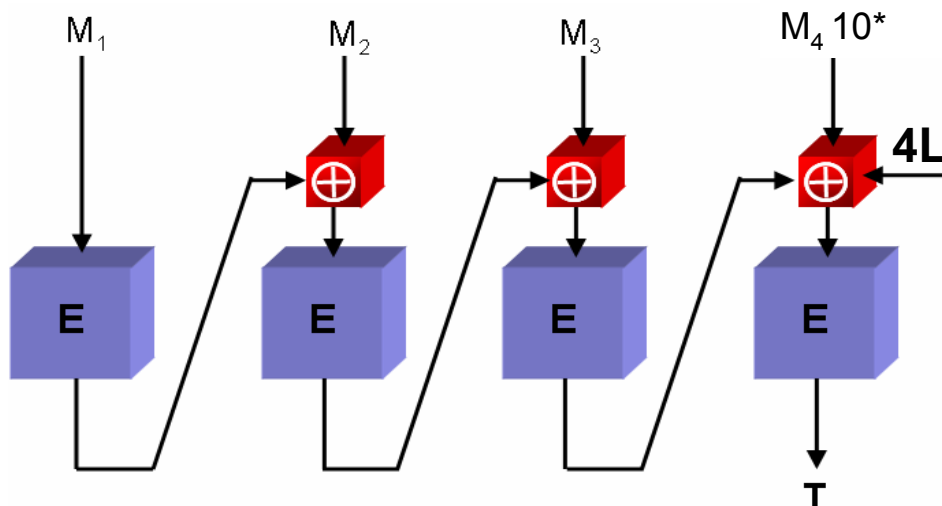
## *OMAC – One Keyed CBC-MAC*



If last block **FULL**

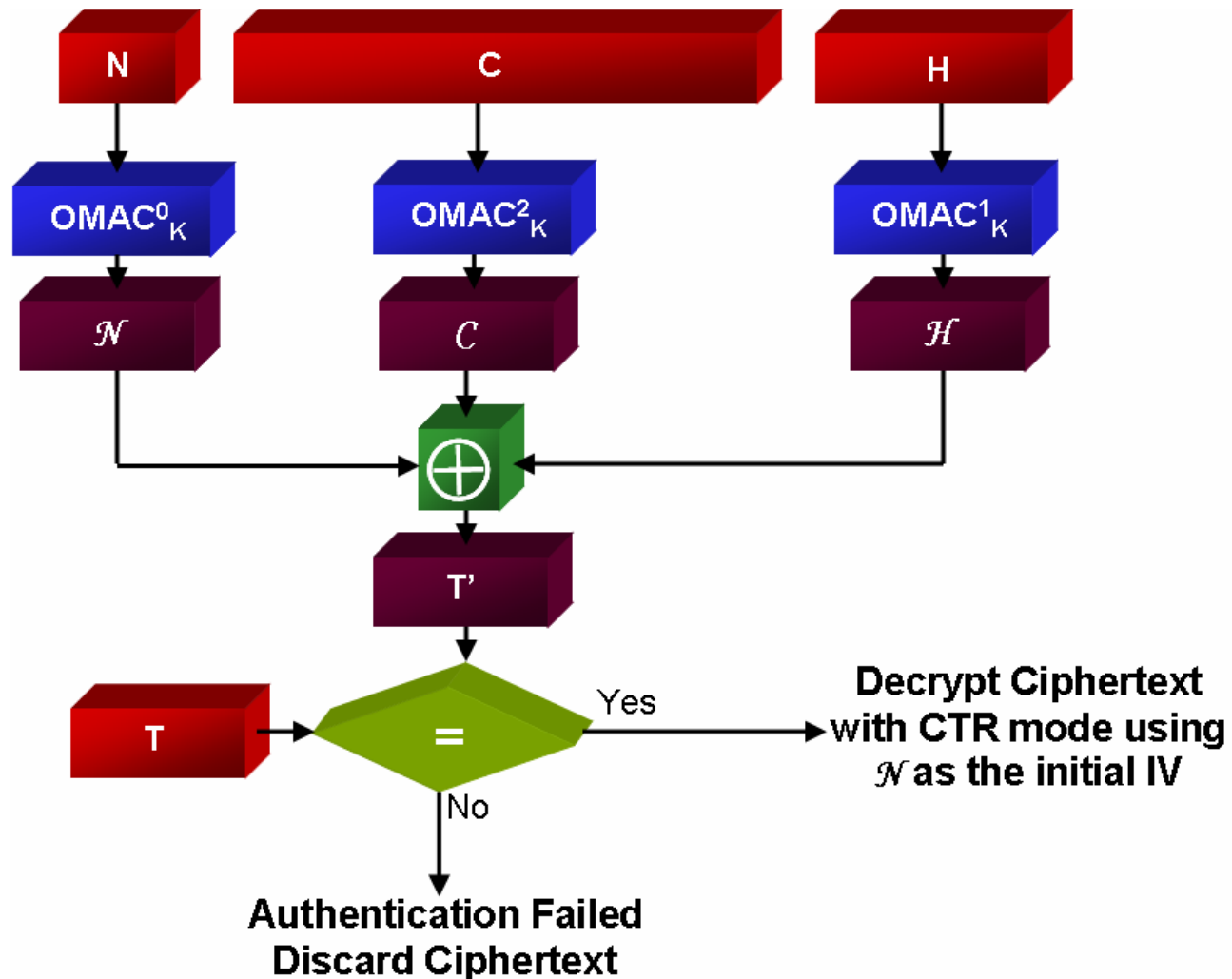
$$\mathbf{L} = \mathbf{E}_K(\mathbf{0}^n)$$

*Multiplication  $2L$  and  $4L$  is performed over  $GF(2^8)$*



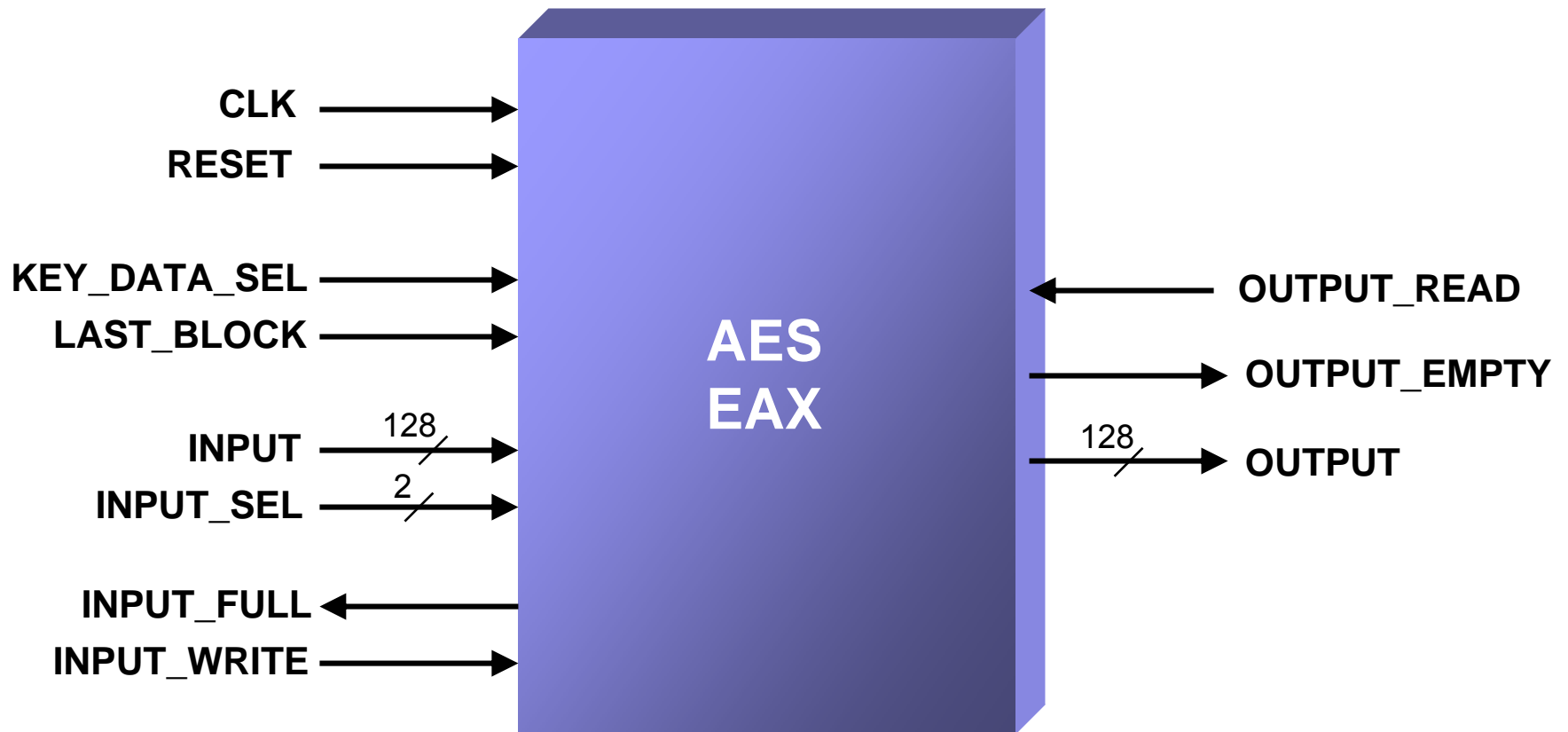
If last block **PARTIAL**

# EAX Decryption and Signature Verification

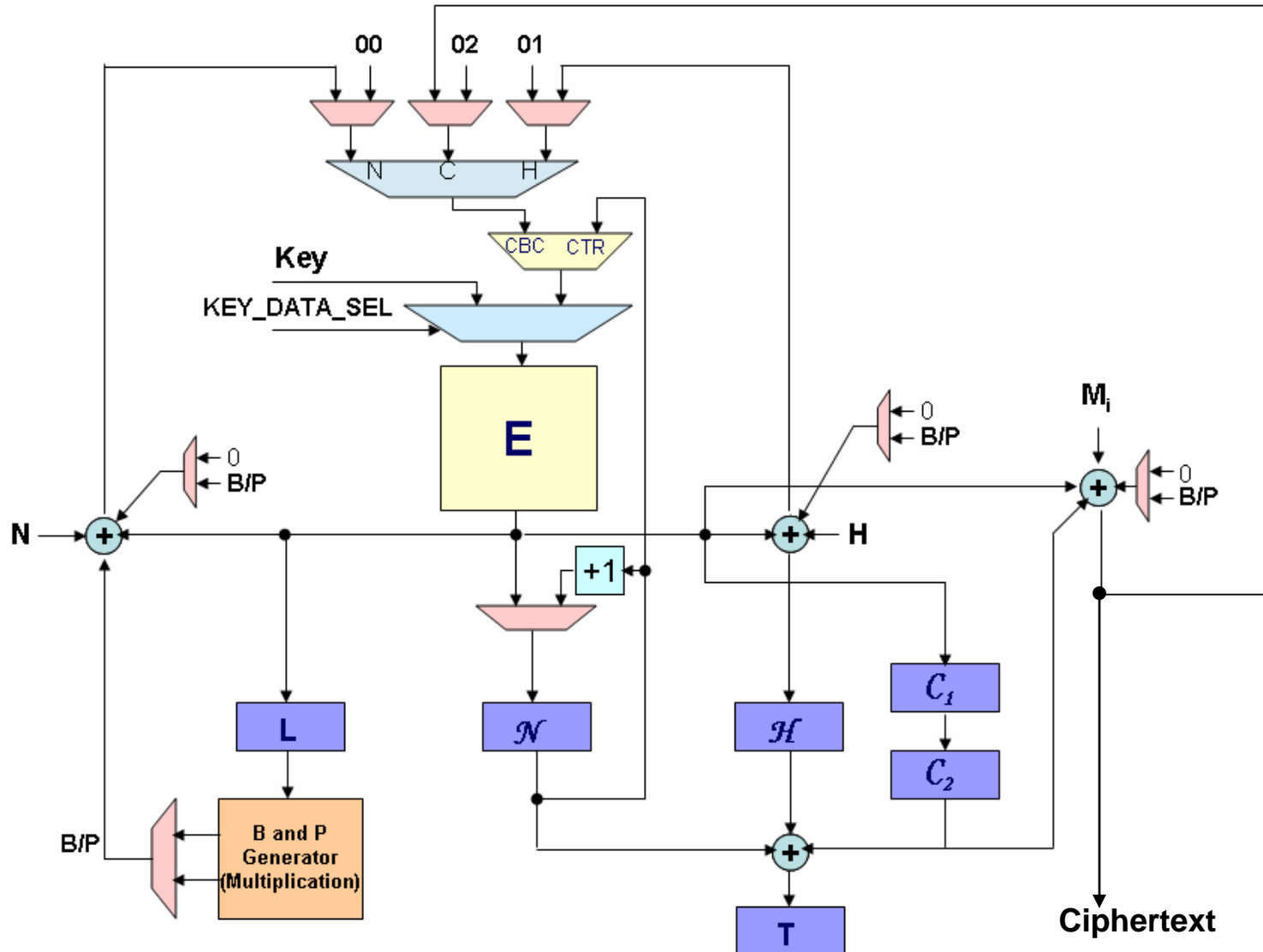




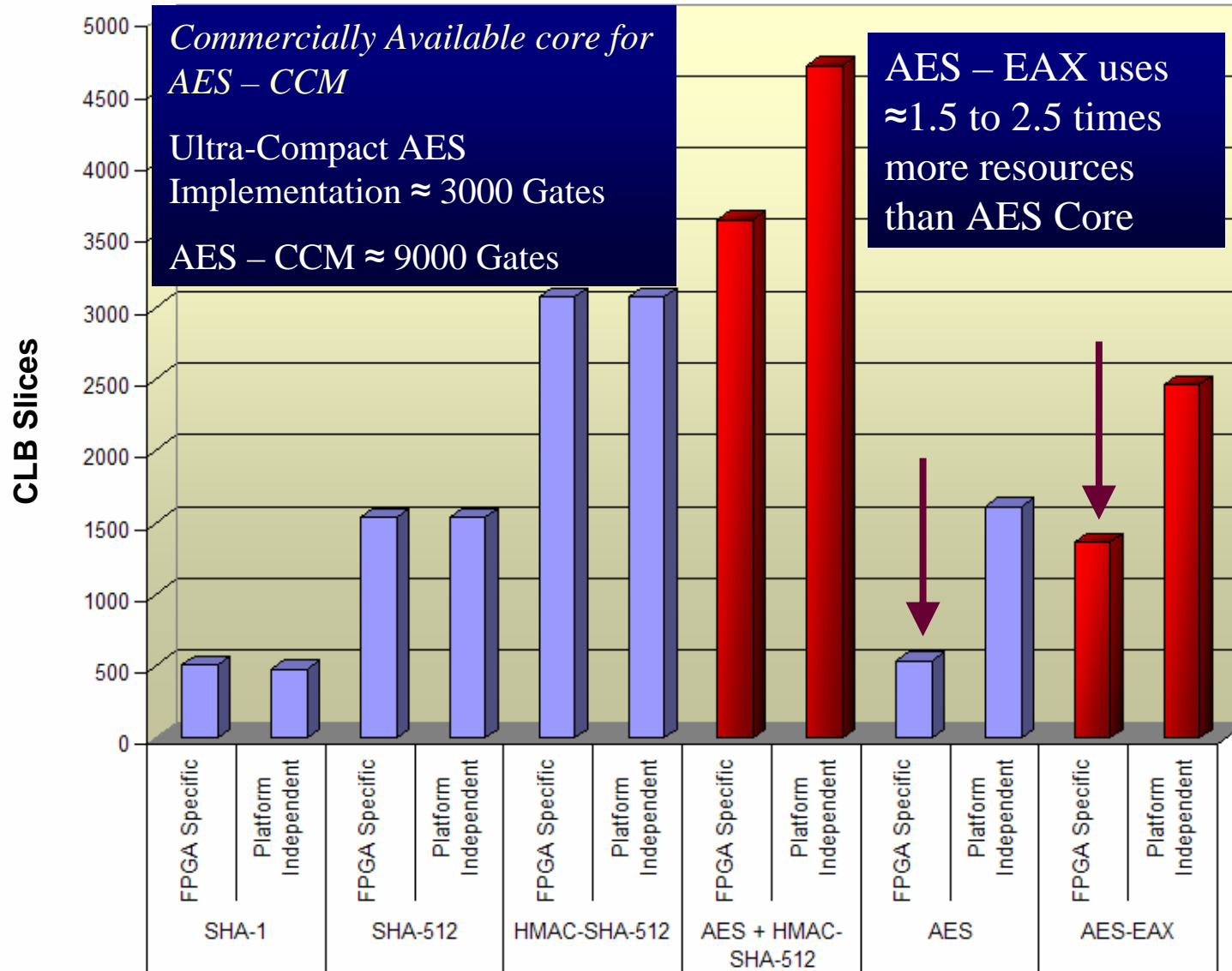
# Interface



# Block Diagram

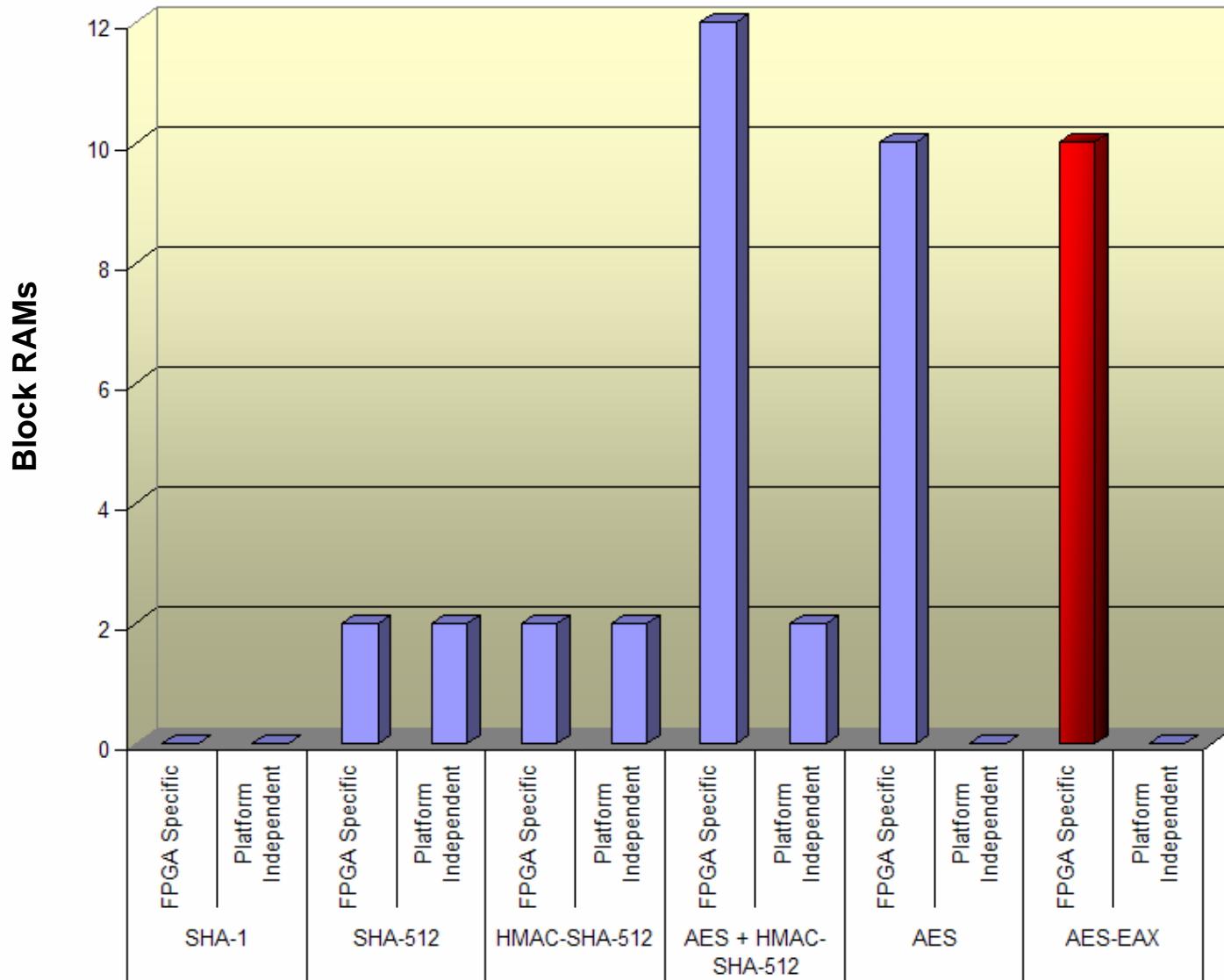


# FPGA Resource Utilization

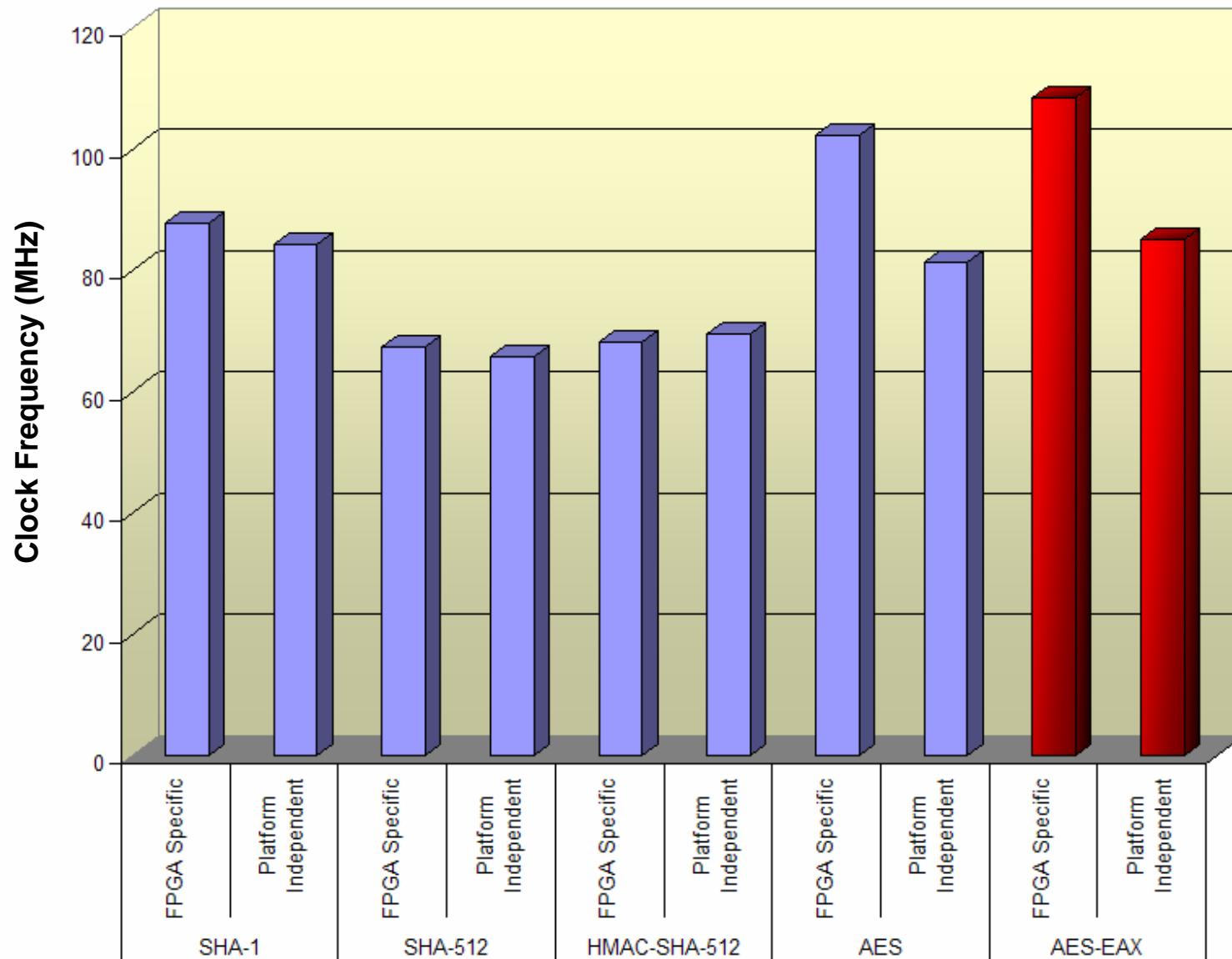


**Target FPGA:  
2v1000bg575**

# Block RAM Utilization



# FPGA Timing Comparison



# Output Throughput Computation

$$\text{Number of Block Cipher Calls} = 2 \left\lceil \frac{|M|}{n} \right\rceil + \left\lceil \frac{|H|}{n} \right\rceil + \left\lceil \frac{|N|}{n} \right\rceil$$

$$\text{Throughput} = \frac{\text{Number of bits processed}}{\text{Number of clock cycles}}$$

$$\therefore \text{Throughput} = \frac{|M| + |H| + |N|}{10 \times \left( 2 \left\lceil \frac{|M|}{n} \right\rceil + \left\lceil \frac{|H|}{n} \right\rceil + \left\lceil \frac{|N|}{n} \right\rceil \right)}$$

$$\therefore \text{Throughput} \approx \frac{|M|}{10 \times \left( 2 \left\lceil \frac{|M|}{n} \right\rceil \right)}$$

$$\therefore \text{Throughput} \approx \frac{n}{10 \times 2} \approx \frac{n}{20} \text{ [bits/cycle]}$$

$$\therefore \text{Throughput} \approx \frac{128}{20} \approx 6.4 \text{ [bits/cycle]}$$

*|M| - Message Size*

*|H| - Header Size*

*|N| - Nonce Size*

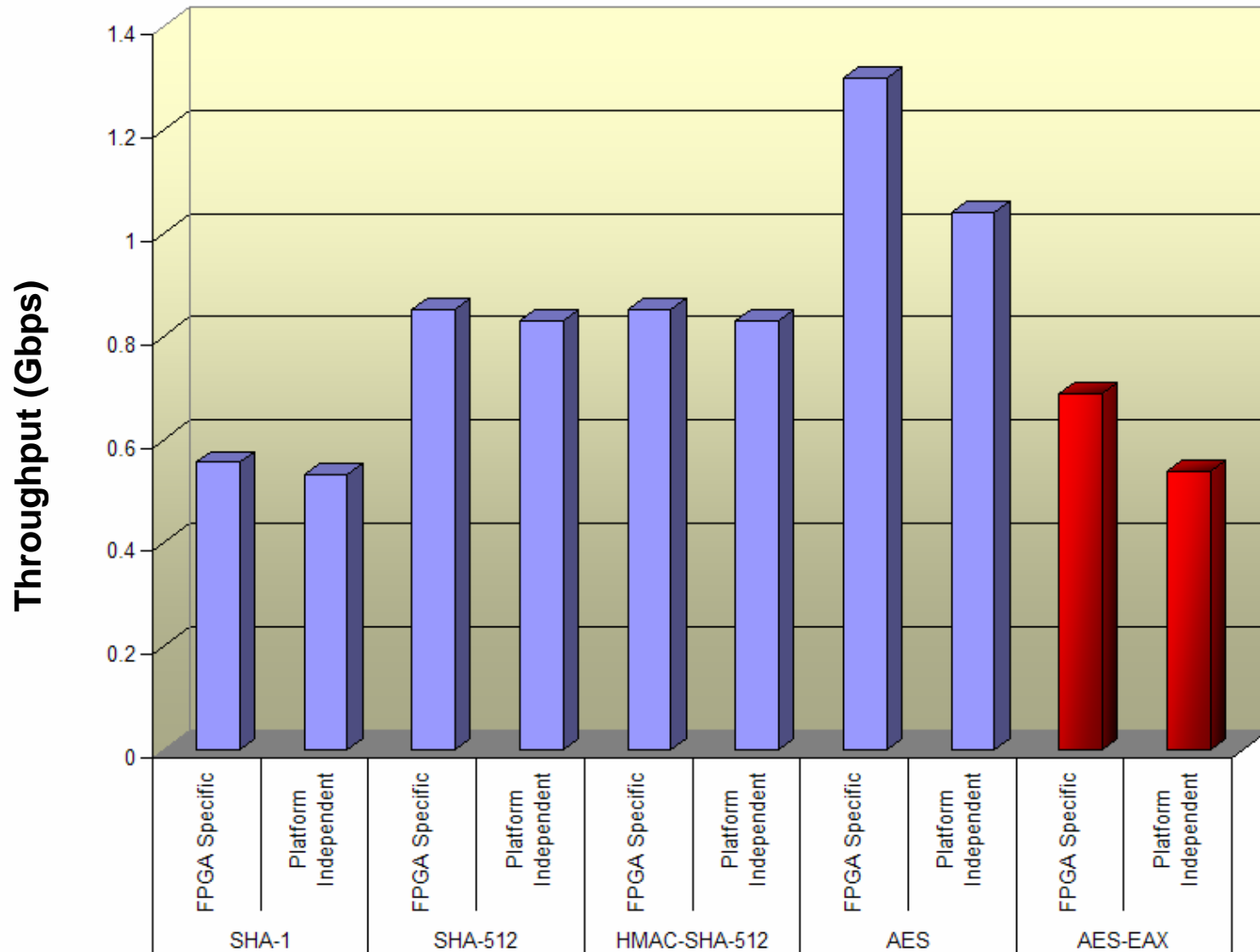
*n - Block Size of the Cipher*

Please note that Key Setup times are not considered while computing throughput

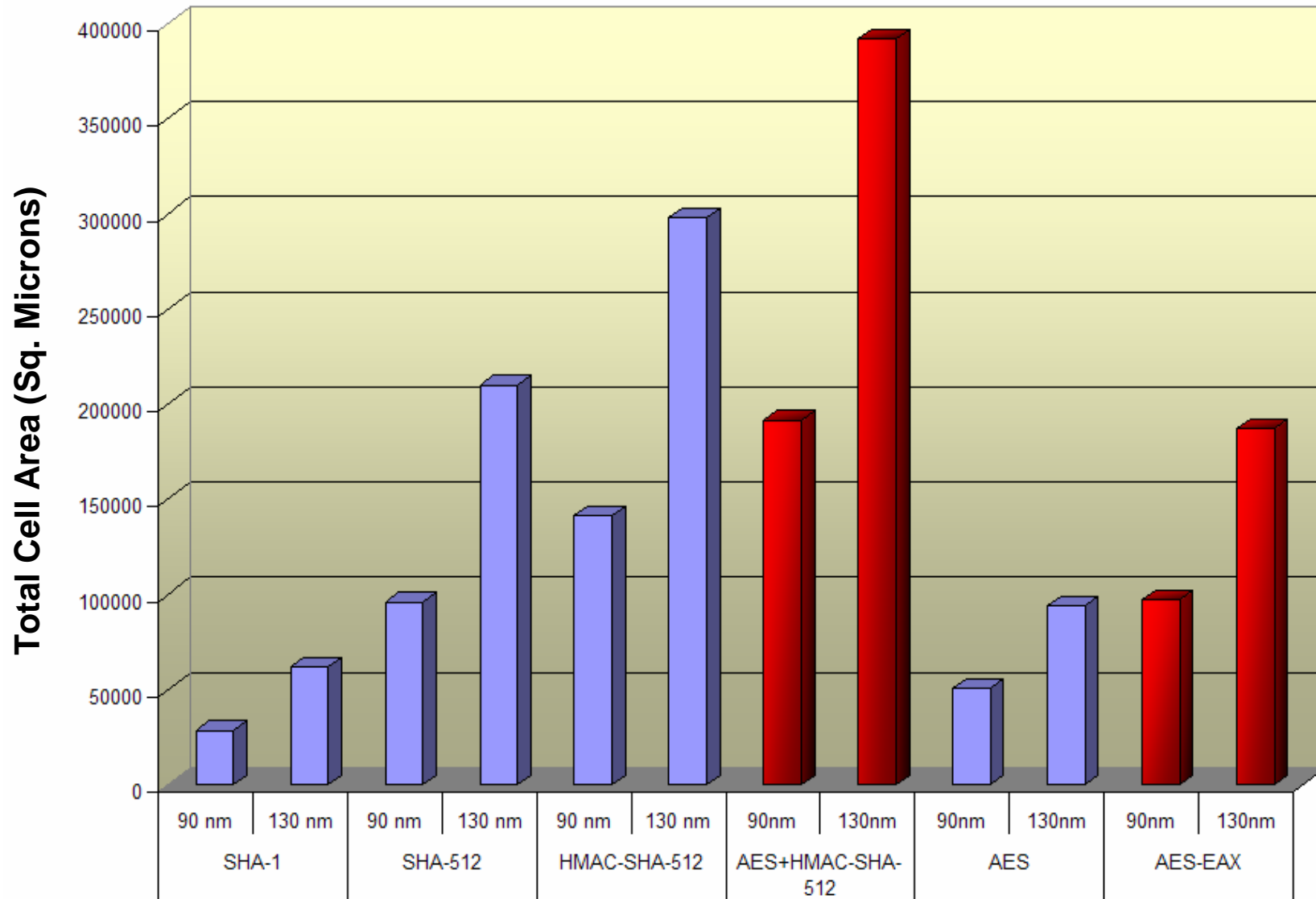
# Output Throughput Computation

	AES		AES-EAX	
	FPGA Specific	Platform Independent	FPGA Specific	Platform Independent
Minimum Clock Period	9.786 ns	12.285 ns	9.219 ns	11.758 ns
Maximum Clock Frequency	102.19 MHz	81.40 MHz	108.47 MHz	85.05 MHz
Throughput	1.3 Gbps	1.04 Gbps	0.69 Gbps	0.54 Gbps

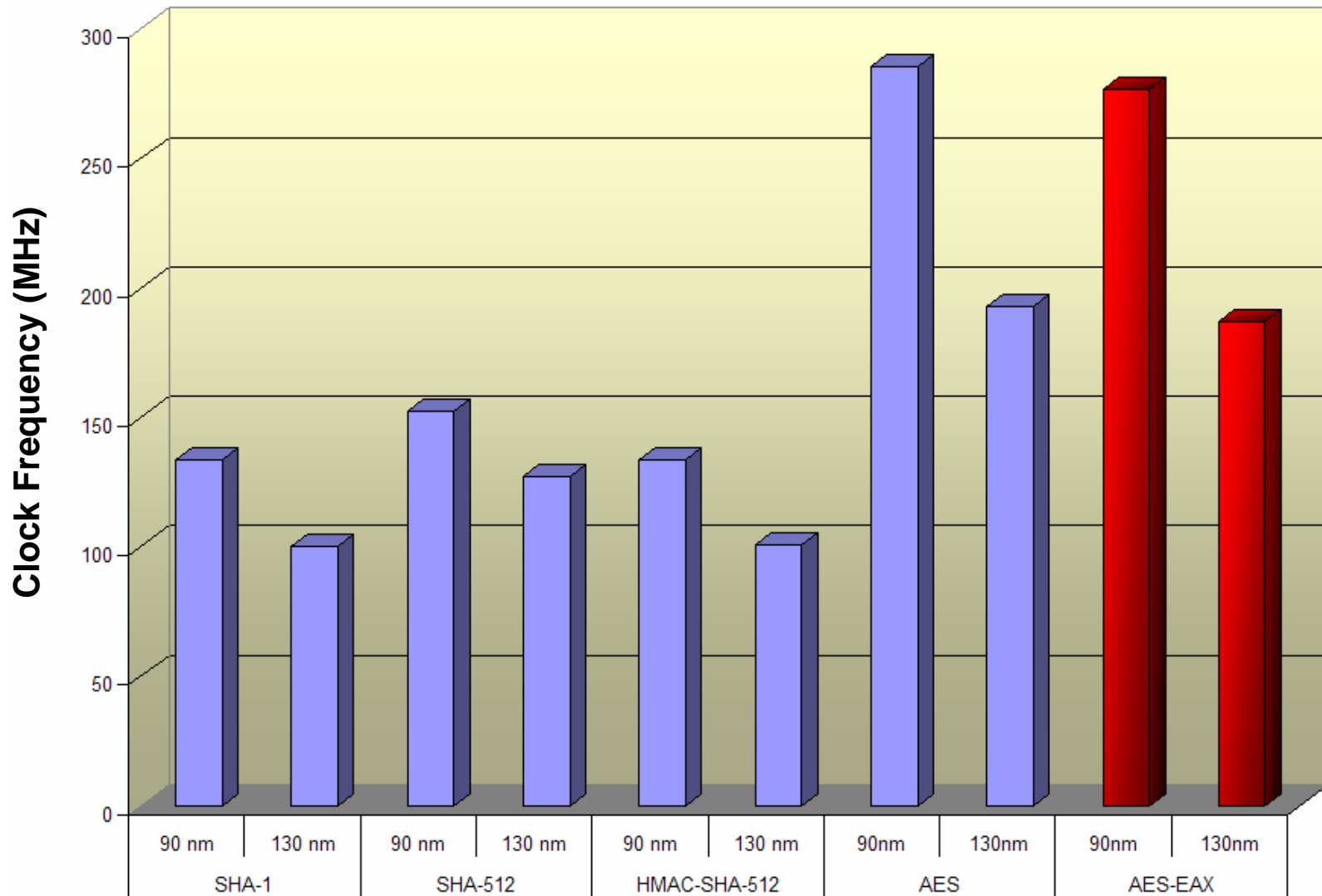
# FPGA Throughput Comparison



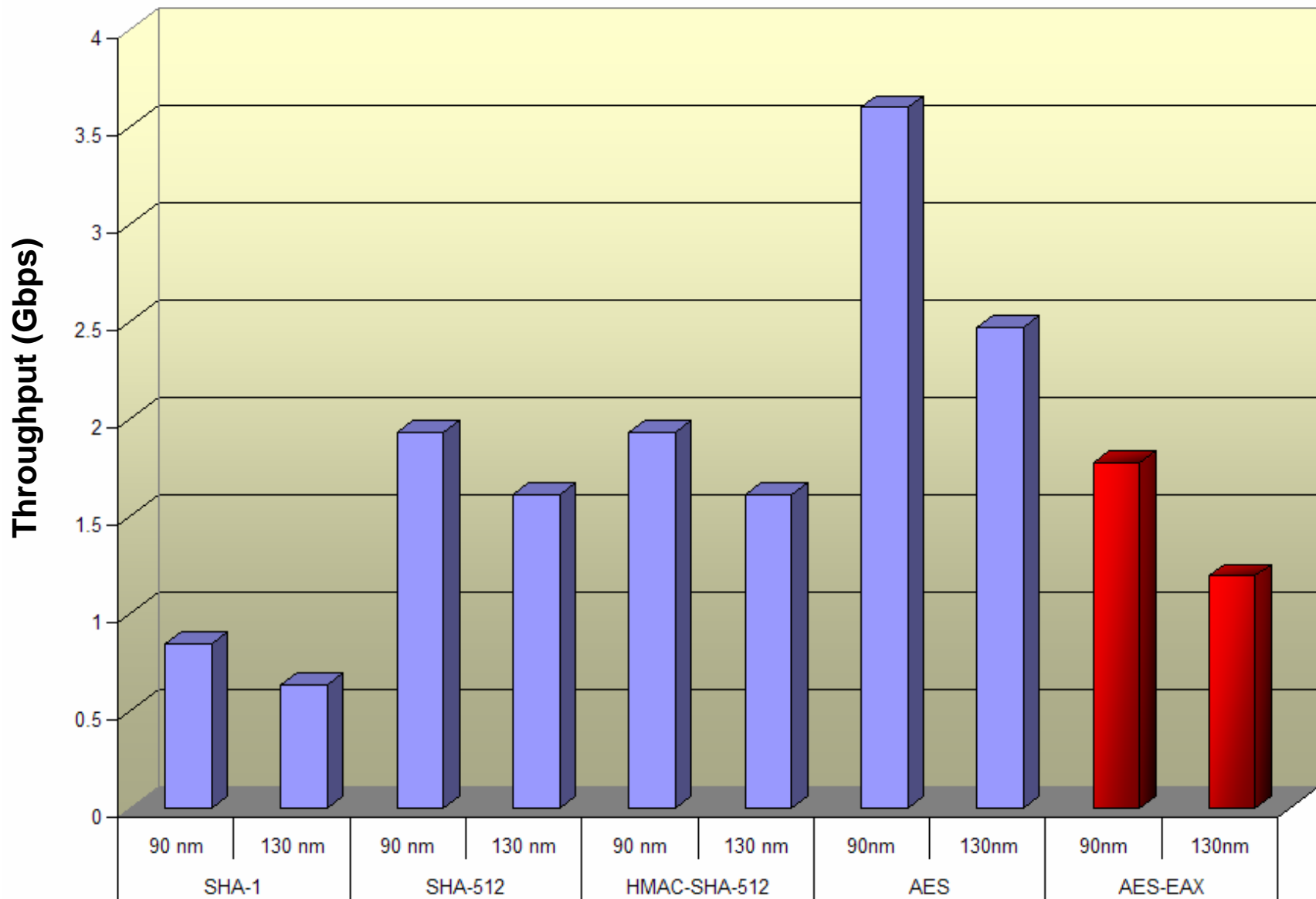
# ASIC Resource Utilization



# ASIC Timing Comparison



# ASIC Throughput Comparison



# Conclusions

- Authenticated Encryption Modes are more efficient than Generic Composition Schemes in terms of Resource Utilization
- Throughput for EAX mode is approximately  $\frac{1}{2}$  the throughput of the underlying block cipher
- One-Pass Schemes are more efficient in terms of Throughput

