Analysis and Inner-Round Pipelined Implementation of Selected Parallelizable CAESAR Competition Candidates

Sanjay Deshpande & Kris Gaj

George Mason University
U.S.A.

This work has been partially supported by NSF Grant #1314540

Cryptographic Engineering Research Group (CERG)

CERG : http://cryptography.gmu.edu

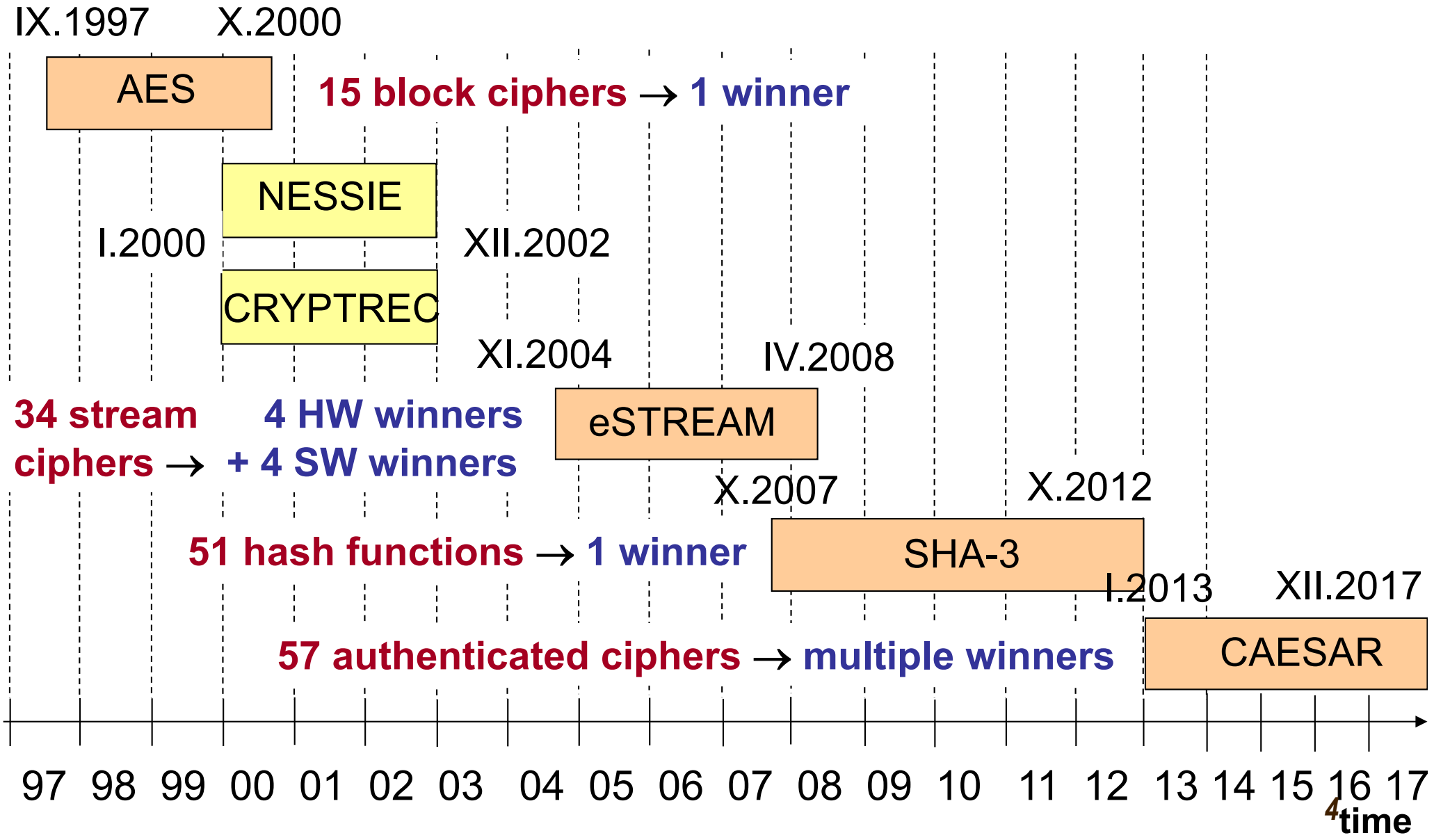
ATHENa: http://cryptography.gmu.edu/athena

CERG
Cryptographic Engineering Research Group

Outline

- CAESAR Contest
- Inner-Round Pipelining
- Selection of Suitable Candidates
- General Methodology for Pipelining
- Implementation
- Analysis of Results
- Conclusions & Future Work

Cryptographic Standard Contests



CAESAR Competition

Goal: Portfolio of new-generation authenticated ciphers

First-round submissions: March 15, 2014

Announcement of final portfolio: 2018

Organizer: A committee of leading cryptographic experts

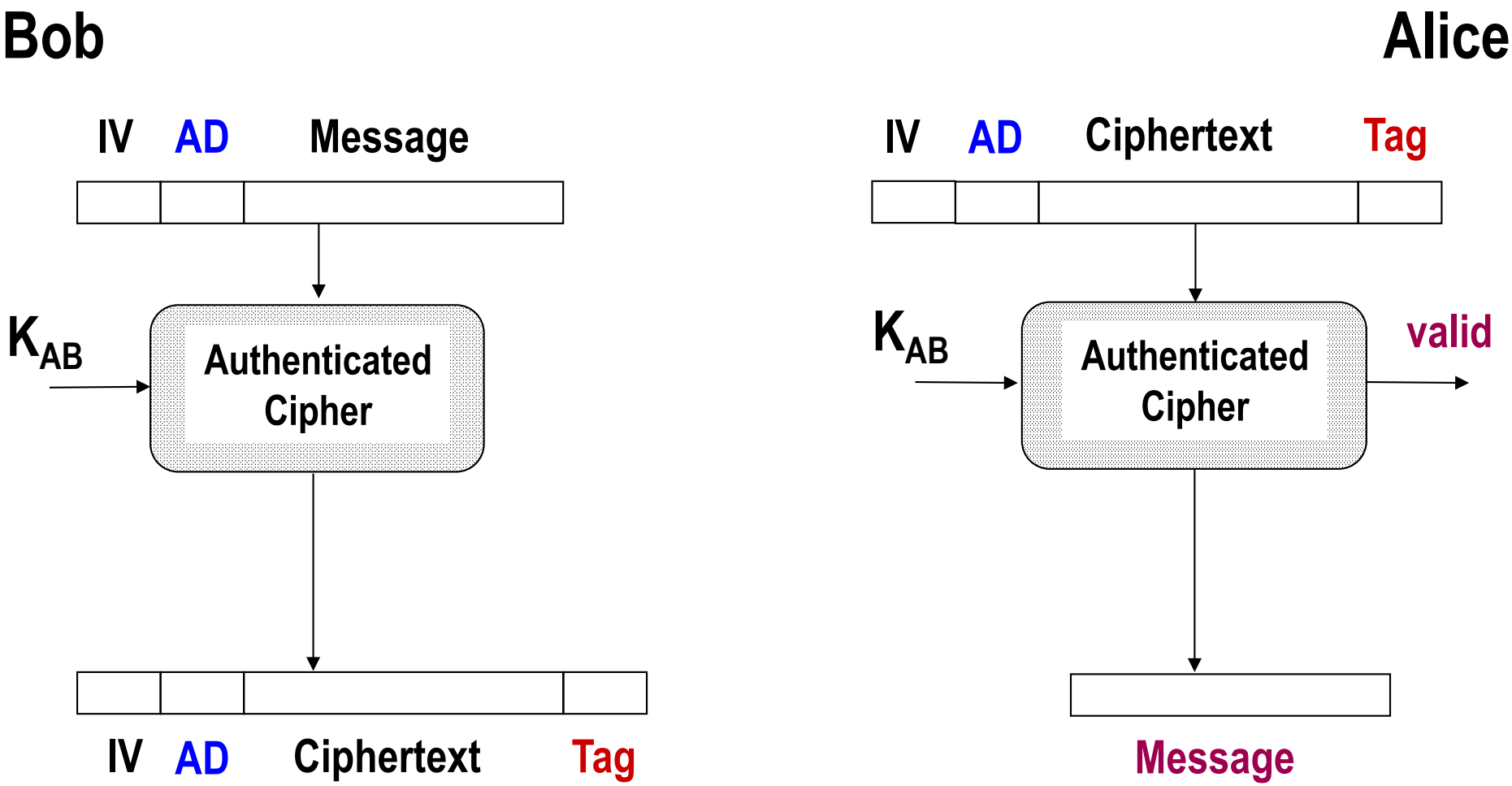
Number of candidate families:

Round 1: 57

Round 2: 29

Round 3: 15

Authenticated Ciphers



K_{AB} - Secret key of Alice and Bob

IV – Initialization Vector, AD – Associated Data

Evaluation Criteria in Cryptographic Contests

Security

Software Efficiency

µProcessors µControllers

Hardware Efficiency

FPGAs ASICs

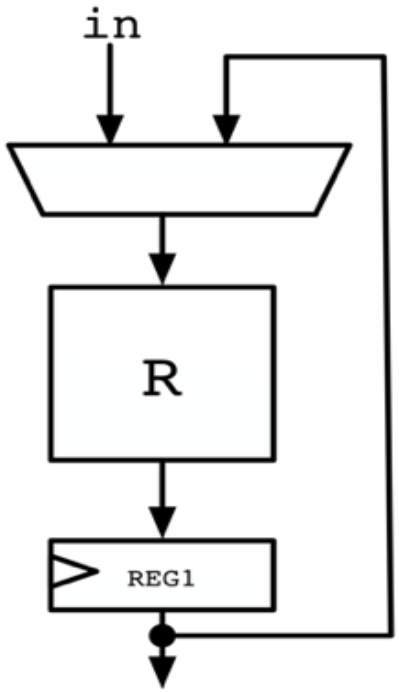
Flexibility

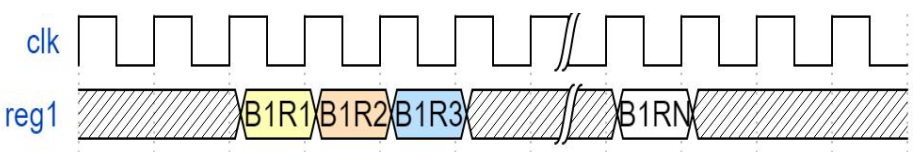
Simplicity

Licensing

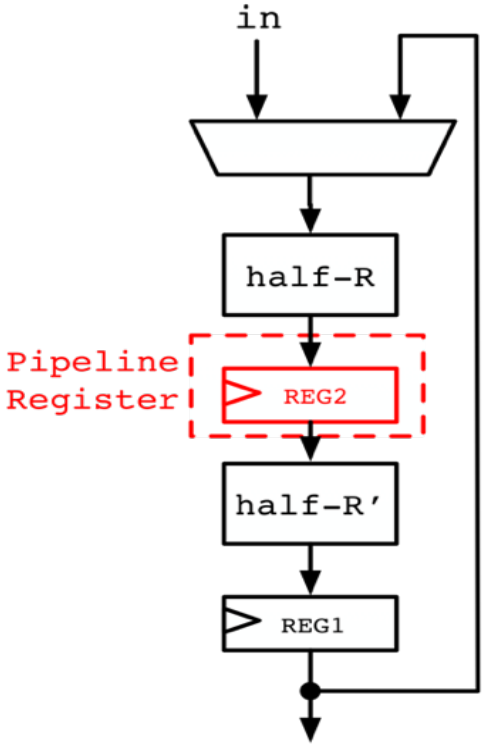
Basic Iterative Architecture vs. Pipelined Architecture

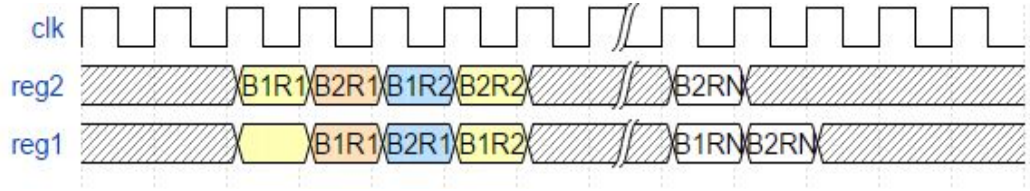
Basic Iterative Architecture





Inner-Round Pipelined Architecture



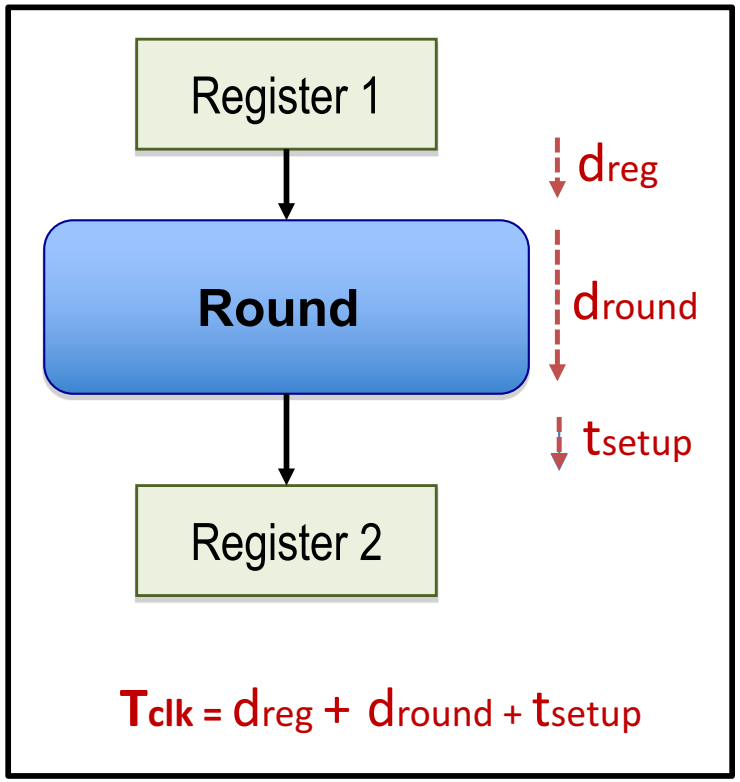


Timing Diagram showing contents of registers at each clock cycle

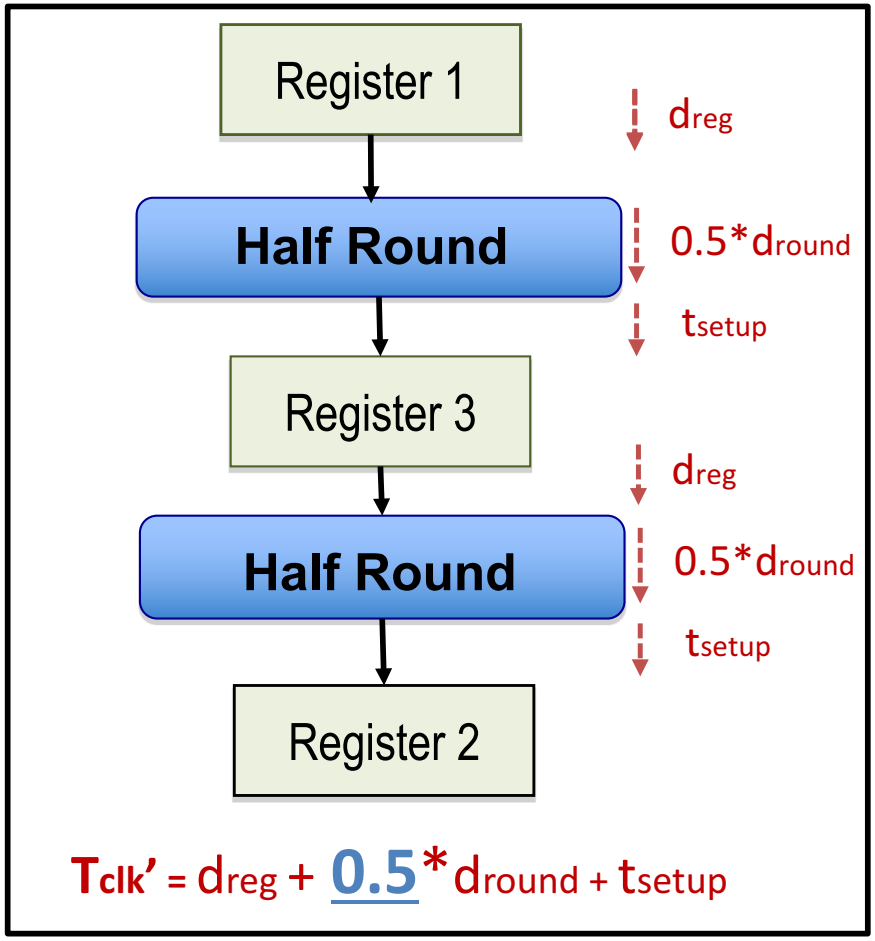
B1R1-Block1 Round1, B1R2-Block1 Round2, etc.

How Does Pipelining Help?

Basic Architecture



Ideal Pipeline Architecture



How Does Pipelining Help?

$$\text{Throughput}_{\text{Basic}} = \frac{\text{Block\_size}}{\text{N*Tclk}}$$

$$\text{Throughput}_{\text{Pipelined}} = \frac{\text{2*Block\_size}}{\text{2*N*Tclk'}}$$

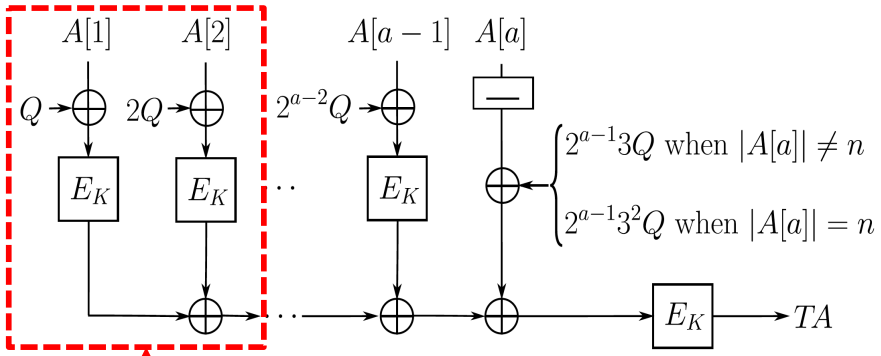
Ideal Condition:

$$\frac{\text{Throughput}_{\text{Pipelined}}}{\text{Throughput}_{\text{Basic}}} = \frac{\text{Tclk}}{\text{Tclk'}} = \frac{\text{dreg + dround + tsetup}}{\text{dreg + 0.5*dround + tsetup}} < 2$$

$$= \frac{\text{fclk'}}{\text{fclk}}$$

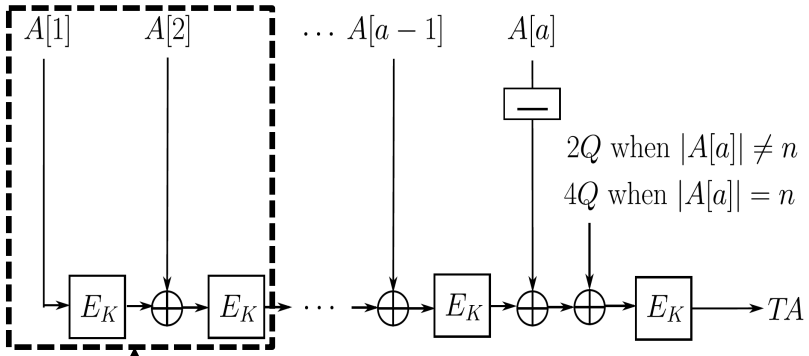
Parallelizable Authenticated Cipher Modes

Parallelizable



Clearly Parallelizable

Non Parallelizable



Dependency between data blocks

Round 3 & Round 2 Candidates Overview

Round 3 Candidates

Candidate	Associated Data	Message	Ciphertext
ACORN	X	X	X
AEGIS	X	X	X
AES-OTR (Parallel ADP)	✓	✓	✓
AES-OTR (Serial ADP)	X	✓	✓
AEZ	✓	✓	✓
Ascon	X	X	X
CLOC	X	X	✓
SILC	X	X	✓
COLM	✓	✓	✓
Deoxys	✓	✓	✓
JAMBU	X	X	X
Ketje	X	X	X
Keyak	X	X	X
MORUS	X	X	X
NORX	X	X	X
OCB	✓	✓	✓
Tiaoxin	X	X	X

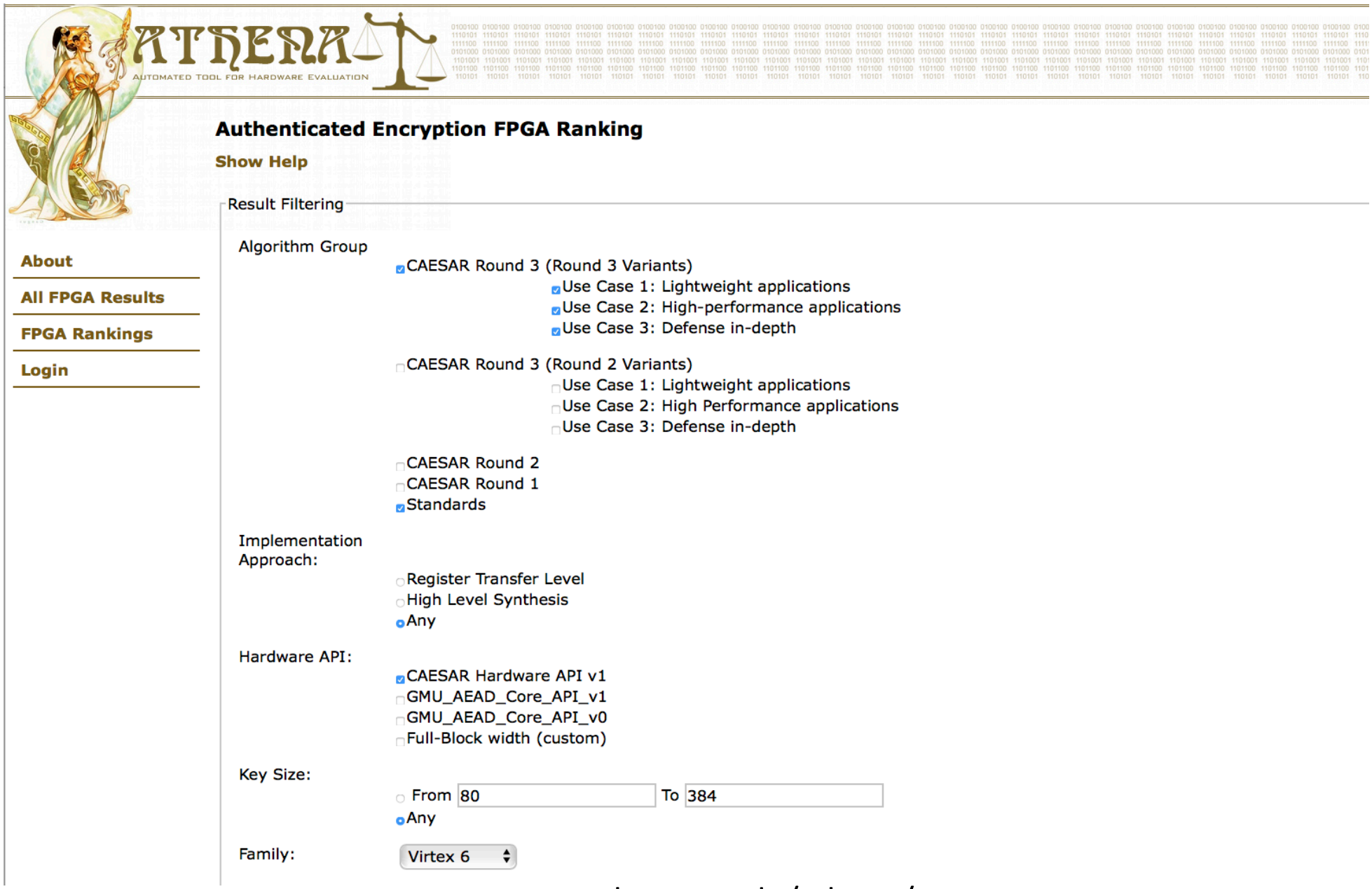
Eliminated Round 2 Candidates

Candidate	Associated Data	Message	Ciphertext
HS1-SIV	✓	✓	✓
ICEPOLE	X	X	X
Joltik	✓	✓	✓
Minalpher	✓	✓	✓
OMD	✓	X	X
PAEQ	✓	✓	✓
POET	✓	✓	✓
PRIMATEs APE	X	X	X
PRIMATEs HANUMAN	X	X	X
PRIMATEs GIBBON	X	X	X
SCREAM	✓	✓	✓
SHELL	X	✓	✓
STRIBOB	X	X	X
TriviA-ck	X	X	X

General Methodology

- Analyze the Basic Architecture implementation (already developed by other members of CERG)
- Get the initial estimates of
  - ✓ Maximum Clock Frequency
  - ✓ Area
  - ✓ Critical Path
- Based on the information from the Basic Architecture implementation insert the Pipeline Register
- Choose the optimal location for the Pipeline Register using the trial & error method
- Datapath is modified to support processing of two blocks
- Controller is modified for parallel processing of two blocks

ATHENa Database of Results (1)



cryptography.gmu.edu/athena/

ATHENa Database of Results (2)

Family: Virtex 6

Portability Resources:
- [x] Without Embedded Resources (Block Memories, DSP Units, etc.)
- [x] Without Primitives or Megafunctions

Unit of Area:
- (•) LUTs
- ( ) Slices

Throughput for:
- (•) Authenticated Encryption
- ( ) Authenticated Decryption
- ( ) Authentication Only

Min Area: 0
Max Area: 1000000
Min Throughput: 0
Max Throughput: 1000000

Ranking:
- (•) Throughput/Area
- ( ) Throughput
- ( ) Area

Update

Compare Selected

Show 50 entries

Copy

Result ID	Algorithm (Disable Unique)	Key Size [bits]	Impl Approach	Hardware API	Arch Type	Primary Opt Target	(Enc/Auth TP)/LUT [(Mbits/s)/LUT]	Auth-Only TP [Mbits/s]	Enc/Auth TP [Mbits/s]	Dec/Auth TP [Mbits/s]	In
838	morus1280128v2	128	RTL	CAESAR Hardware API v1	Basic Iterative	Throughput/Area	14.510	49,421	49,421	49,421	
706	aegis128l	128	RTL	CAESAR Hardware API v1	Basic Iterative	Throughput/Area	9.342	70,927	70,927	70,927	
834	acorn128v3	128	RTL	CAESAR Hardware API v1	32-bit	Throughput/Area	9.086	11,303	11,303	11,303	
708	tiaoxinv2	128	RTL	CAESAR Hardware API v1	Basic Iterative	Throughput/Area	7.418	52,838	52,838	52,838	
814	ketjeminorv2	128	RTL	CAESAR Hardware API v1	Basic Iterative	Throughput/Area	5.591	20,082	20,082	20,082	
771	norx3241v3	128	RTL	CAESAR Hardware API v1	Basic Iterative	Throughput/Area	5.203	15,182	15,182	15,182	
770	norx6441v3	256	RTL	CAESAR Hardware API v1	Basic Iterative	Throughput/Area	4.463	24,524	24,524	24,524	

cryptography.gmu.edu/athena/

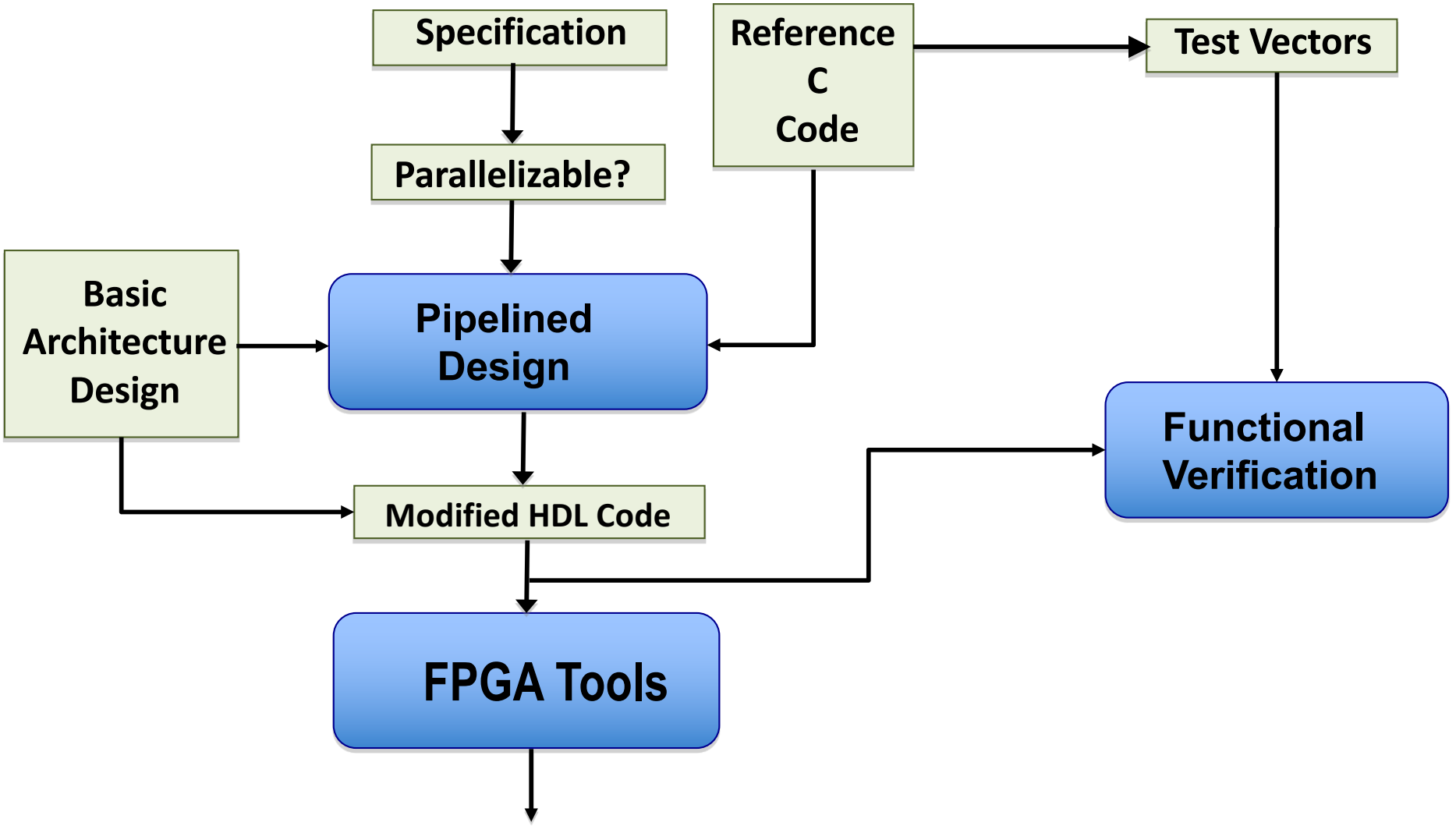
Parallelizable Round 2 and Round 3 Candidates

Candidate	Maximum Clock Frequency (MHz)
AES-COPA	**120**
AES-OTR	**150**
AEZ	335
COLM	**112**
Deoxys ≠ -128 - 128	**194**
ELmD	258
Joltik≠ -128 – 64	394
Minalpher	**168**
OCB	**172**
PAEQ128	258
POET-AES10-AES4	231
SCREAM	**92**

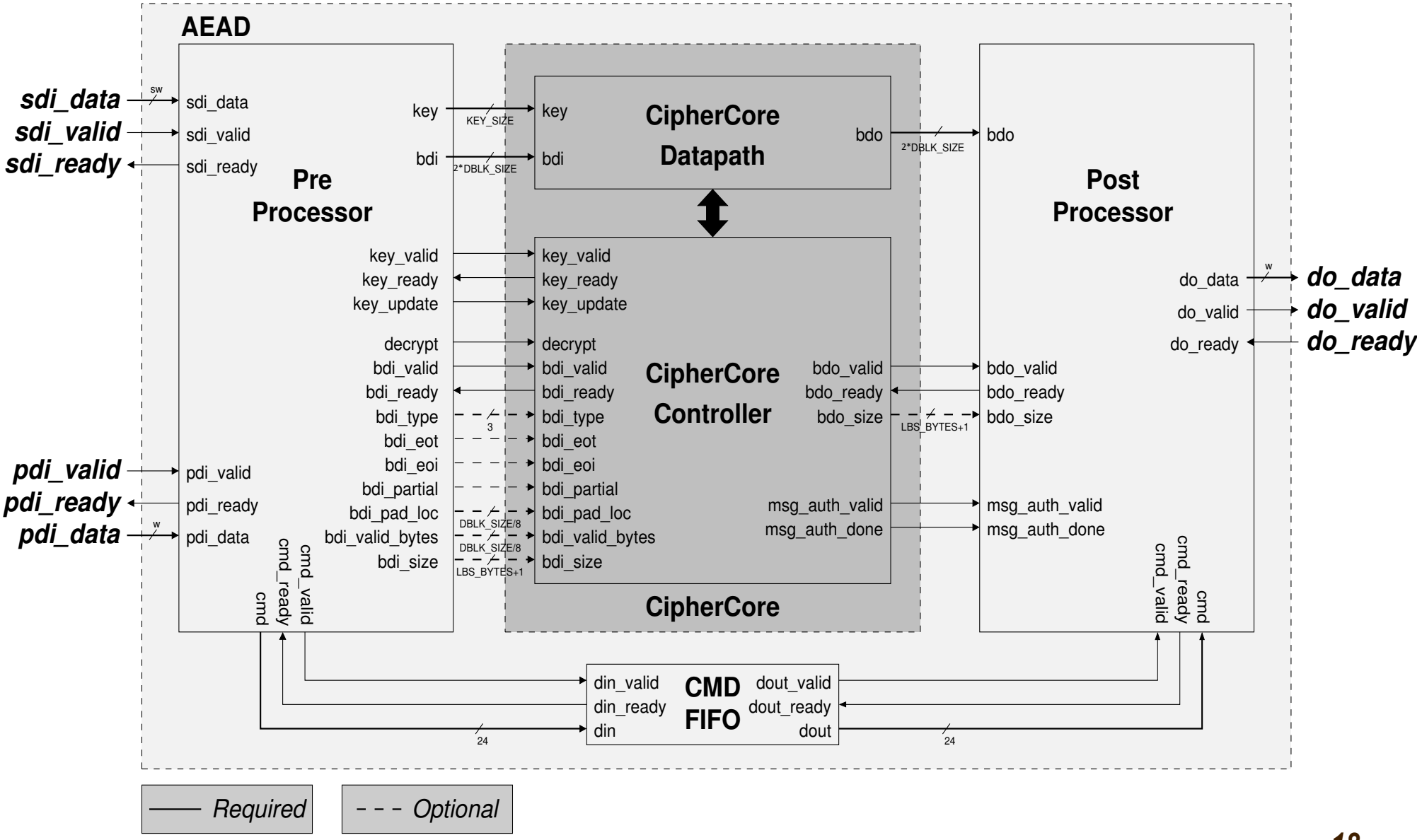
Note: Candidates in **Bold** and Red are selected as their Maximum Clock Frequency is low

Source: cryptography.gmu.edu/athena/

Development Method



Implementation Strategy



Devices & Tools

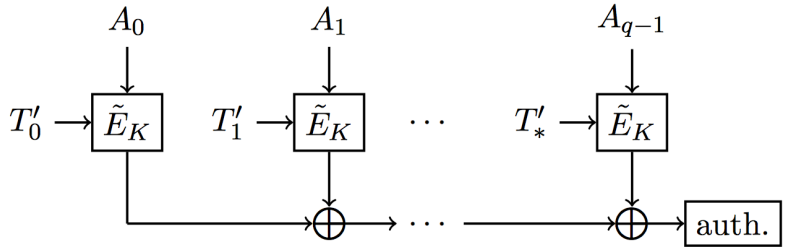
Family:	**Virtex-6**
Device :	XC6VLX75T-3FF784
Synthesis Tool:	**Xilinx** XST **14.7**
Implementation Tool:	**Xilinx** ISE **14.7**

Implementations

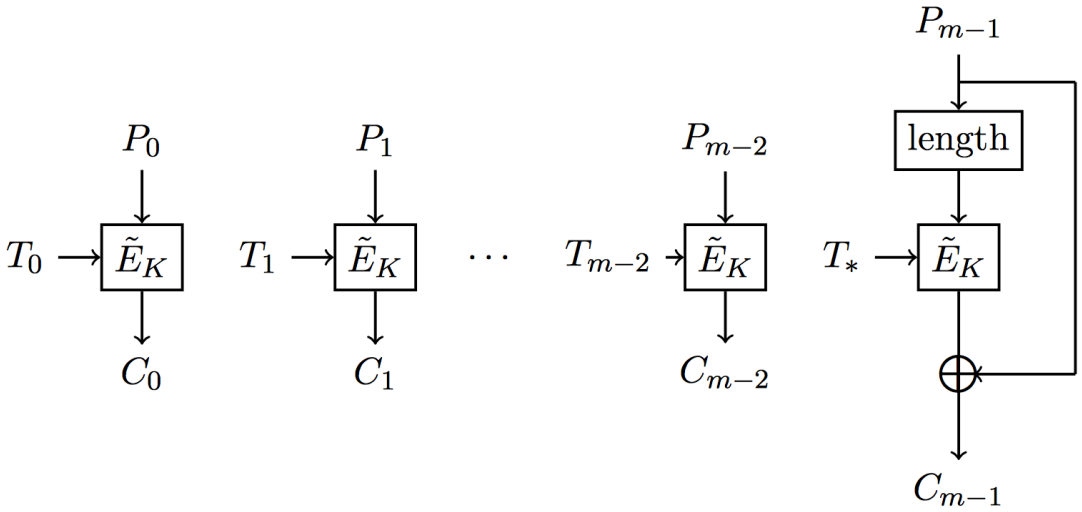
SCREAM - Side Channel REsistant Authenticated Encryption with Masking

- Tweakable Block Cipher (TBC)
- LS Cipher design
- 10 steps of 2 rounds each

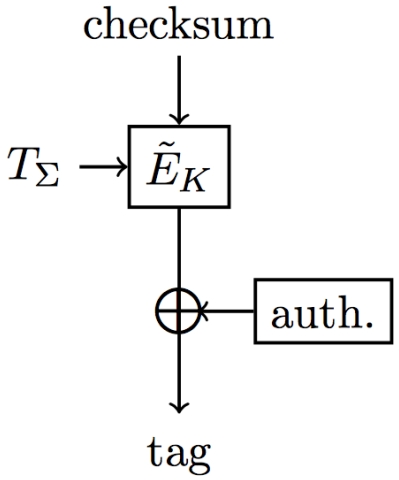
Associated Data Processing



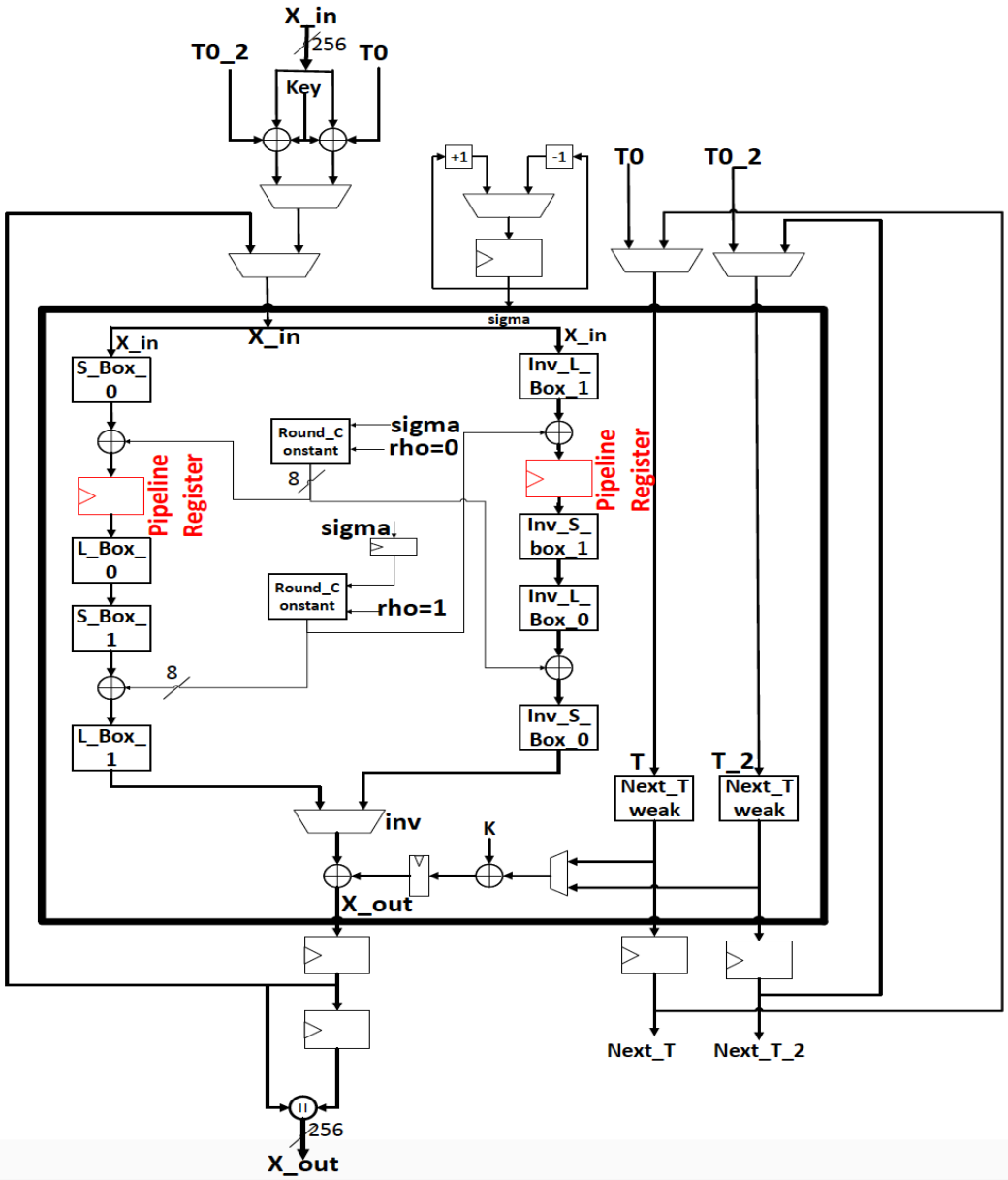
Message/ Ciphertext Processing



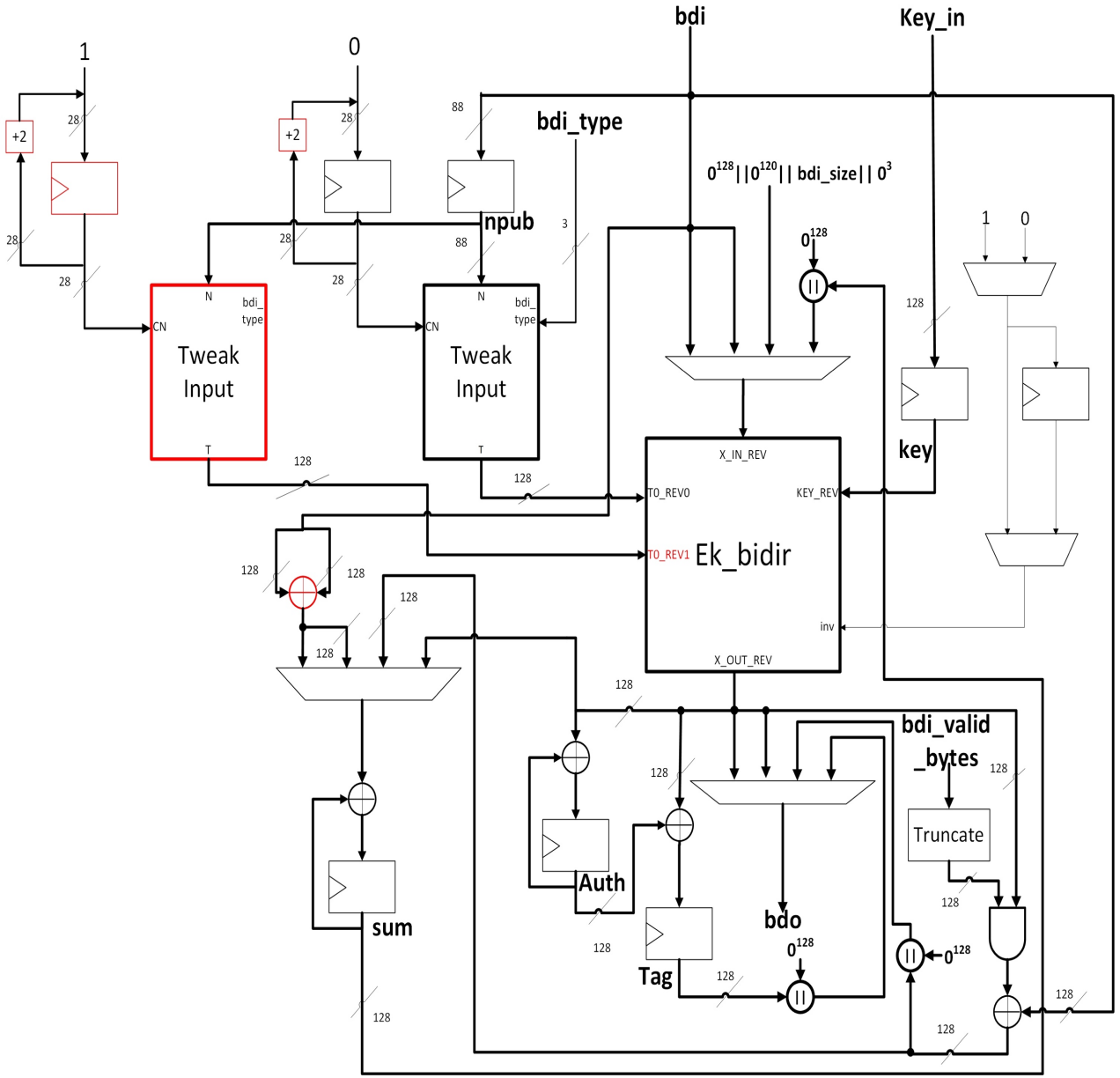
Tag Calculation



SCREAM: Round Function Pipelined



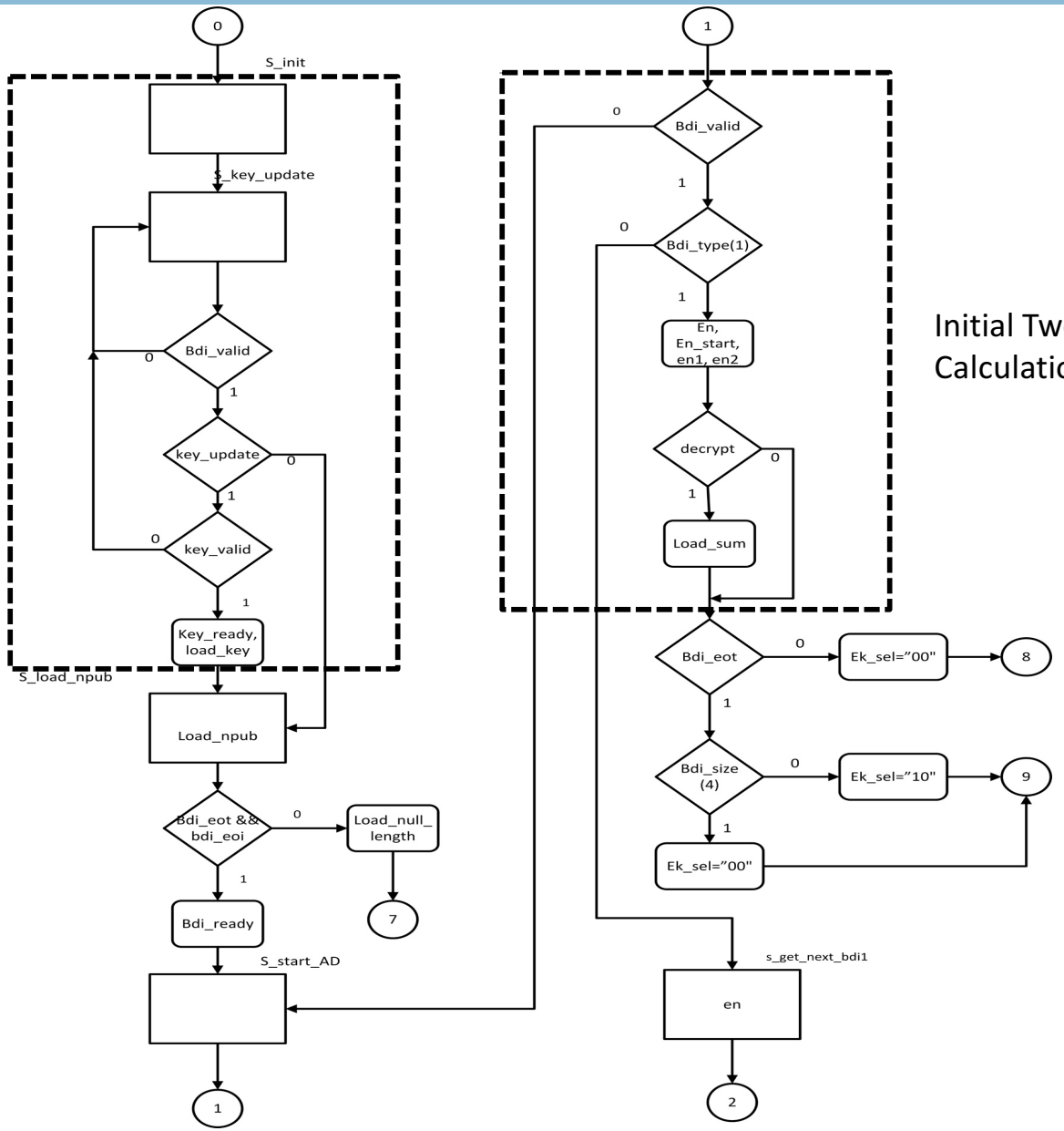
SCREAM: Pipelined Architecture -Datapath



Additional Tweak input has been added to support the processing of a second block of data

SCREAM: Controller Design (1)

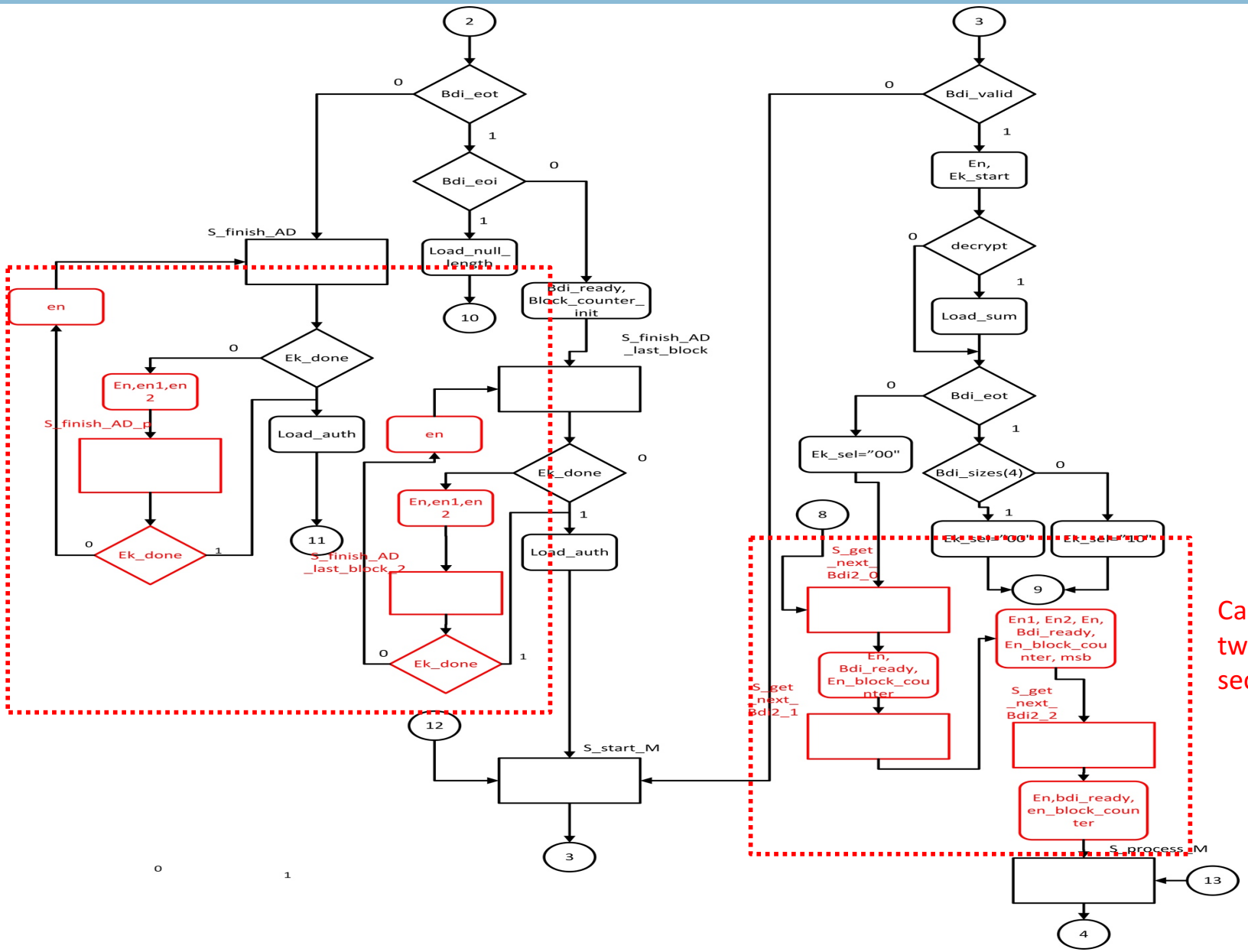
Key Setup & initialization



Initial Tweak Calculation

SCREAM: Controller Design(2)

Support added for processing two blocks of associated data



Calculating tweak for second block

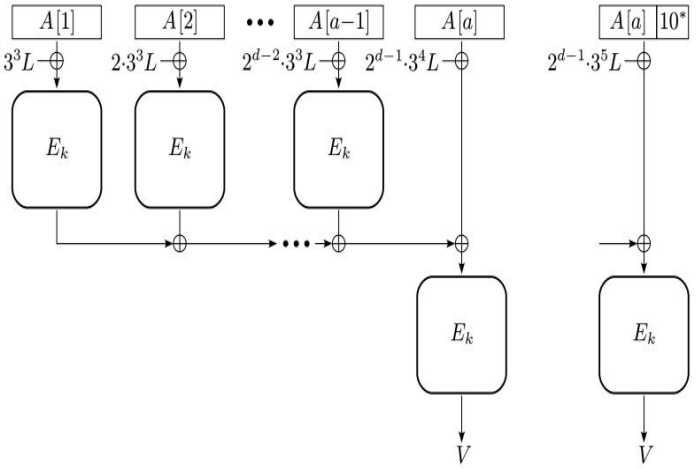
SCREAM Results

	Basic Arch.	Pipelined Arch.
Max. Clk Frequency	92 MHz	170 MHz

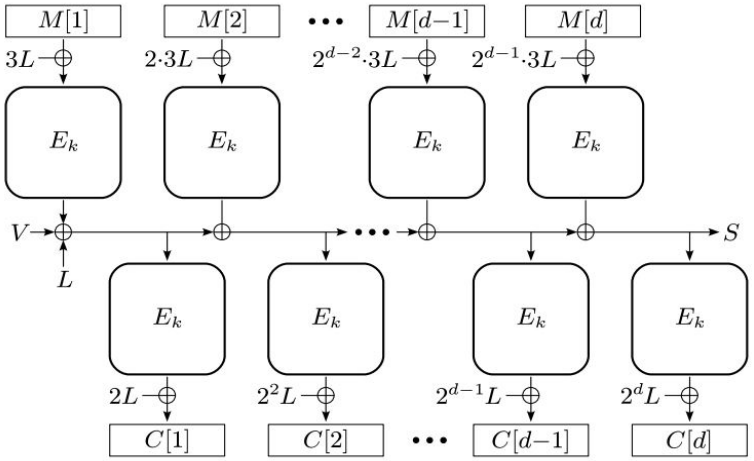
AES-COPA

- Basic Primitive used in AES-COPA is AES
- Recommended Parameters:
  - key length: 16 bytes (128 bits)
  - tag length: 16 bytes (128 bits)

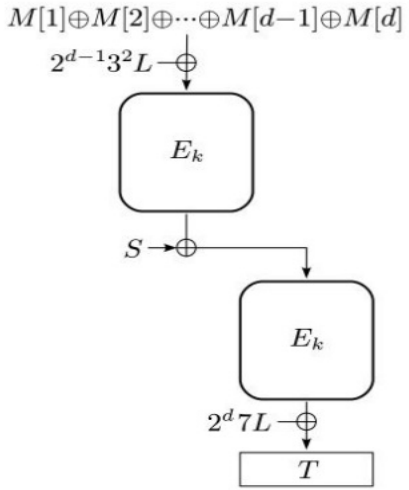
Associated Data Processing



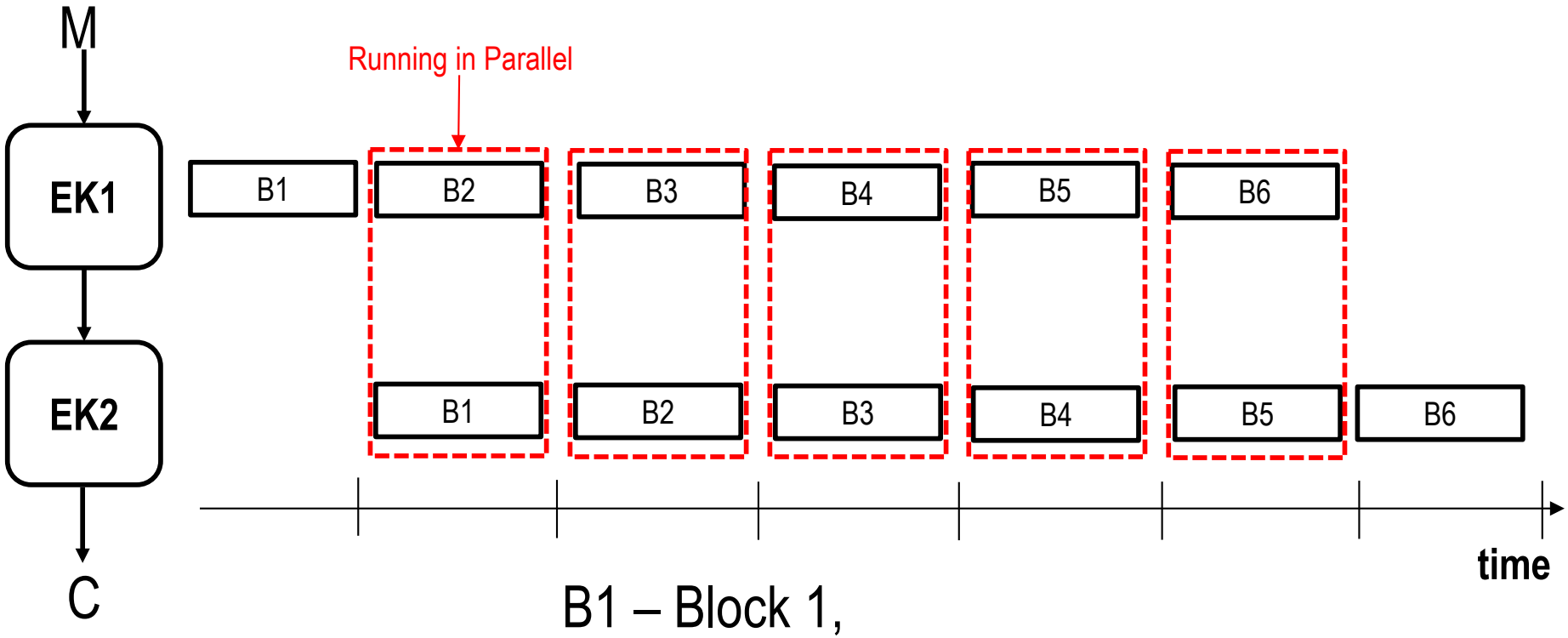
Message and Ciphertext Processing



Tag Calculation

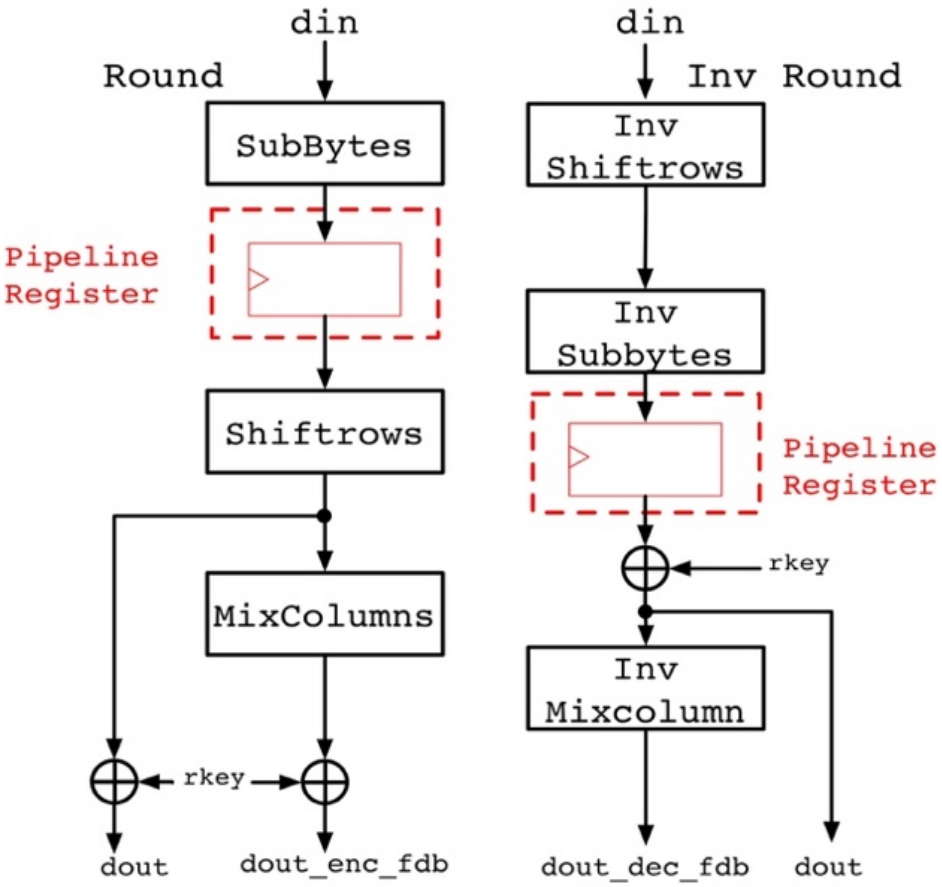


AES-COPA Encryption/ Decryption Parallelization



B1 – Block 1,
B2 – Block 2,
and so on

AES-COPA: Pipelined Round Design



	Basic Arch.	Pipelined Arch.
Max. Clk Frequency	120 MHz	210 MHz

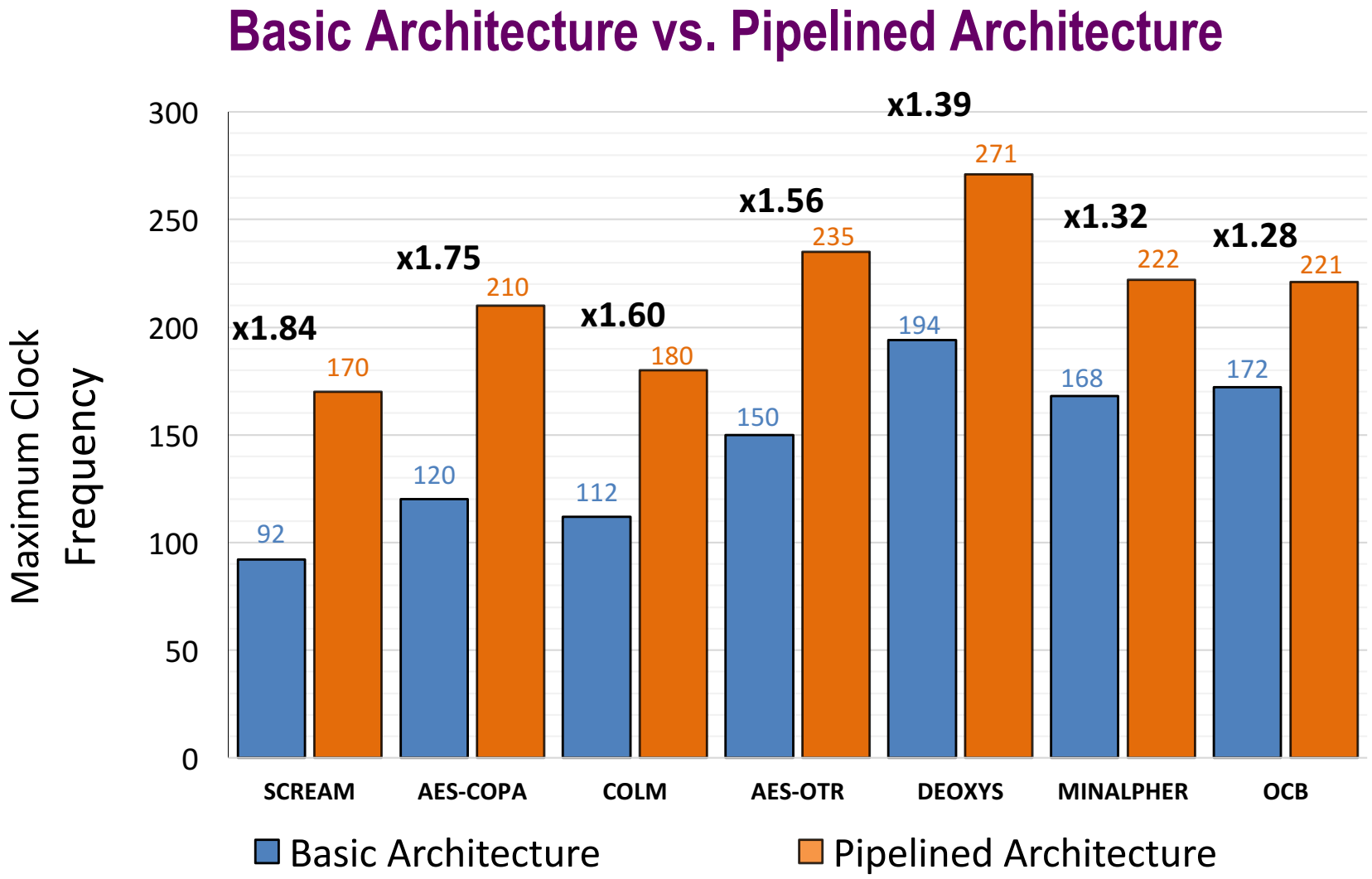
Results for All Investigated Candidates

Maximum Clock Frequency

Candidate	Basic Architecture	Pipelined Architecture	Pipelined/ Basic
SCREAM	92 MHz	170 MHz	1.84
AES-COPA	120 MHz	210 MHz	1.75
COLM	112 MHz	180 MHz	1.60
AES-OTR	150 MHz	235 MHz	1.56
Minalpher	168 MHz	222 MHz	1.39
OCB	172 MHz	221 MHz	1.32
Deoxys	194 MHz	271 MHz	1.28

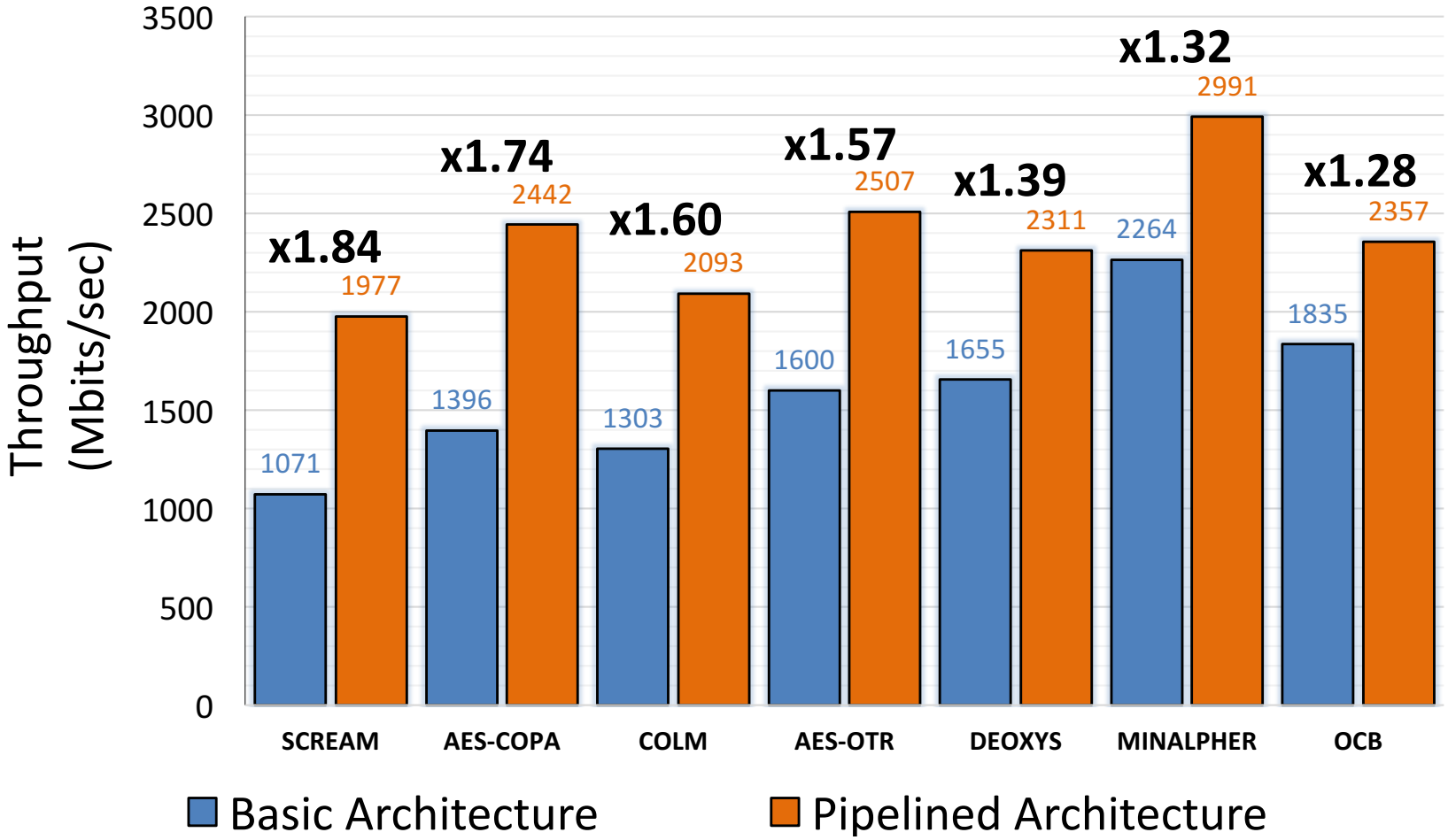
Analysis of Results

Maximum Clock Frequency



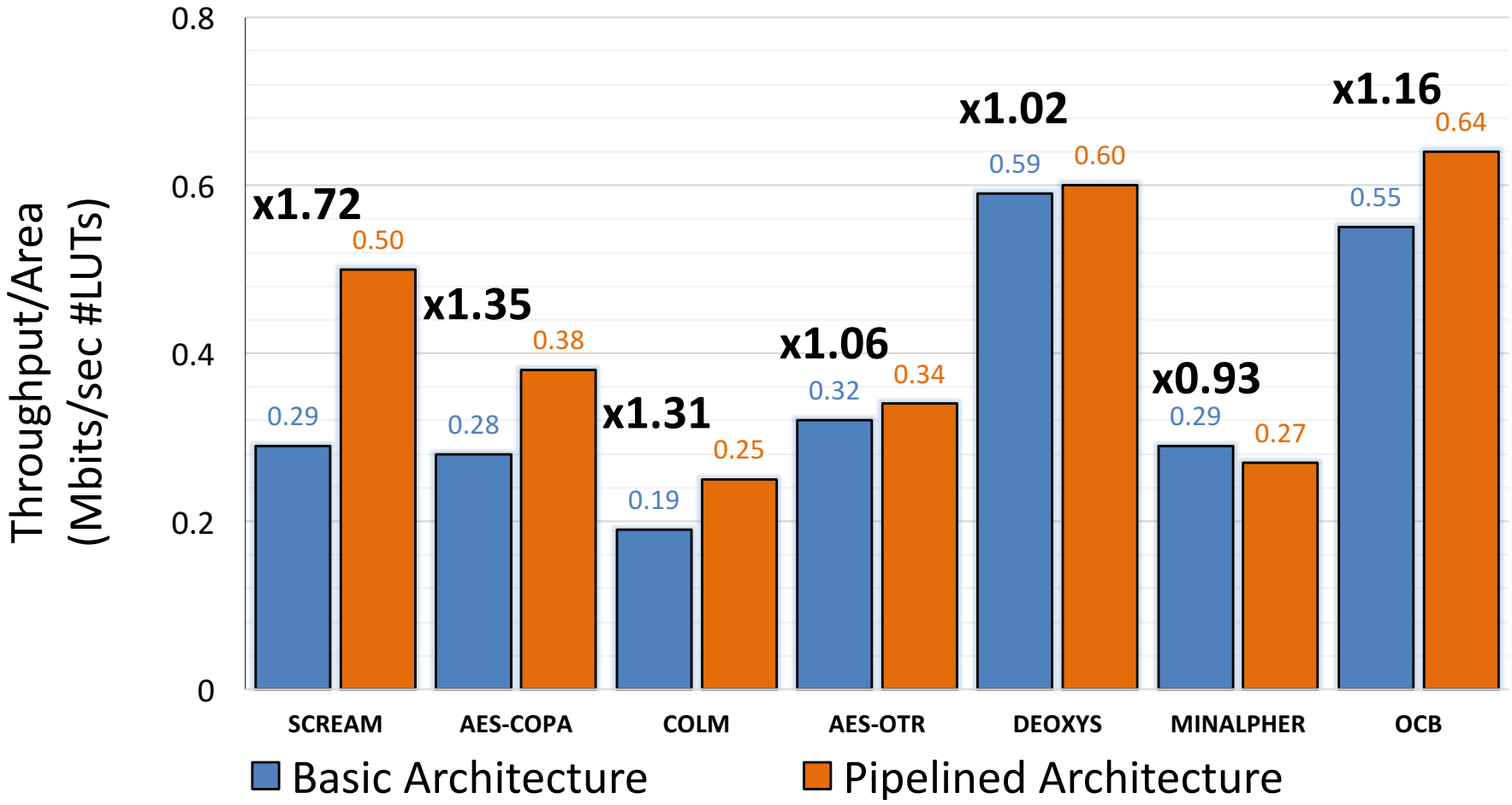
Throughput

Basic Architecture vs. Pipelined Architecture



Throughput to Area Ratio

Basic Architecture vs. Pipelined Architecture



Conclusions

- The **improvement** in Maximum Clock Frequency and Throughput **depends on the algorithm and its critical path**
- Candidate with the **lowest Maximum Clock Frequency and Throughput** in the Basic Architecture (SCREAM) has achieved the **highest amount of gain** in the Pipelined Architecture
- **Improvement in Throughput/#LUTs** was observed **in six out of seven candidates** (all except Minalpher)
- For **four out of seven candidates** (SCREAM, AES-COPA, COLM and AES-OTR), the **frequency and throughput gains exceeded 50%**

Future Work

- Further improving the **placement of pipeline registers**
- Increasing the **number of pipeline stages**
- Identifying the **optimal number of pipeline stages** with the best Throughput/Area ratio
- Pipelining of **remaining parallelizable Round 3 and Round 2 CAESAR candidates**

Thank you!

Questions?

Comments?

Suggestions?

ATHENa: http://cryptography.gmu.edu/athena

CERG: http://cryptography.gmu.edu