

Benchmarking of Cryptographic Algorithms in Hardware



**Ekawat Homsirikamol & Kris Gaj
George Mason University
USA**

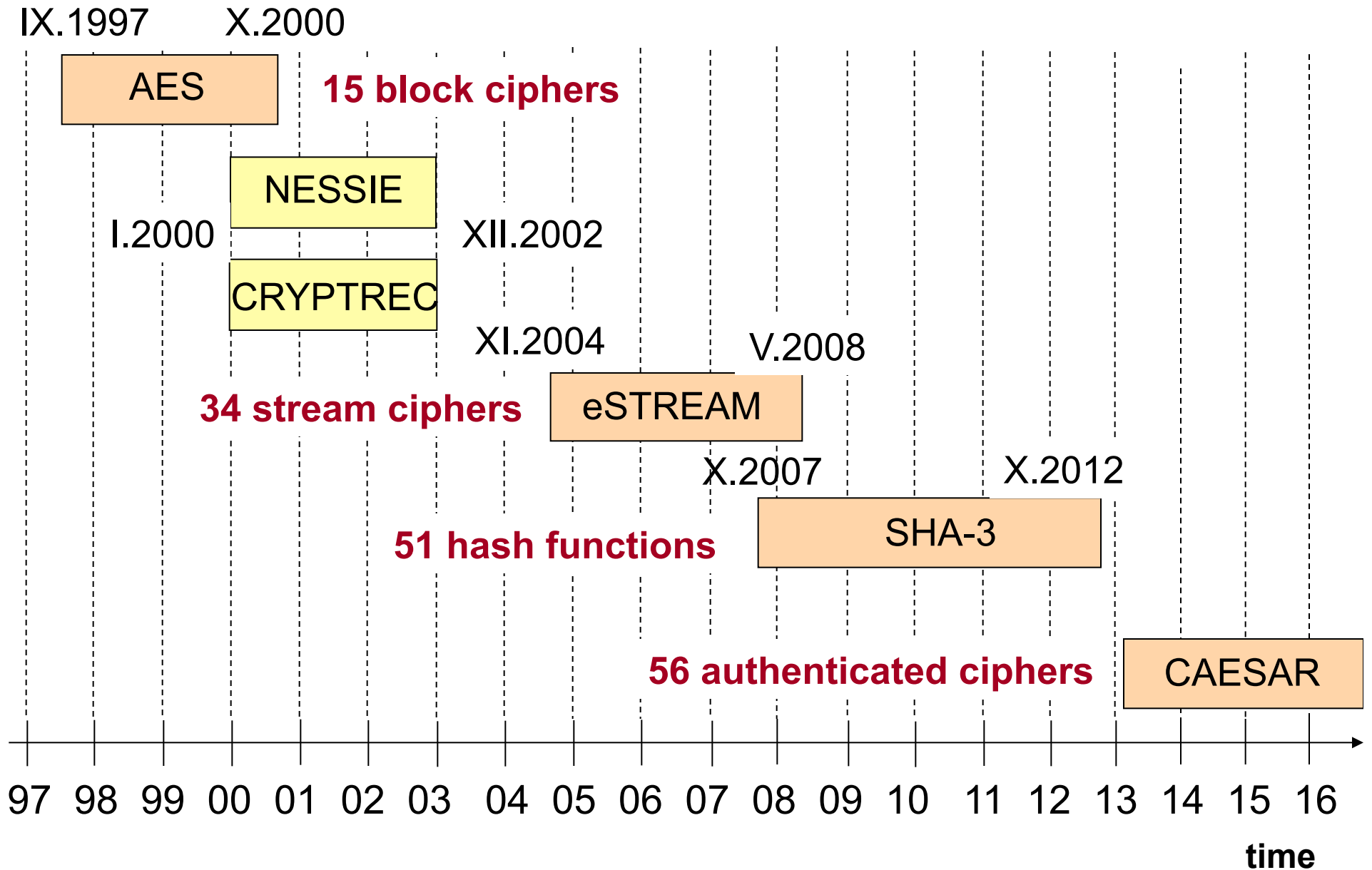
Co-Author



Ekawat Homsirikamol
a.k.a “Ice”

Working on the PhD Thesis
entitled
“A New Approach to the Development
of Cryptographic Standards Based
on the Use of
High-Level Synthesis Tools”

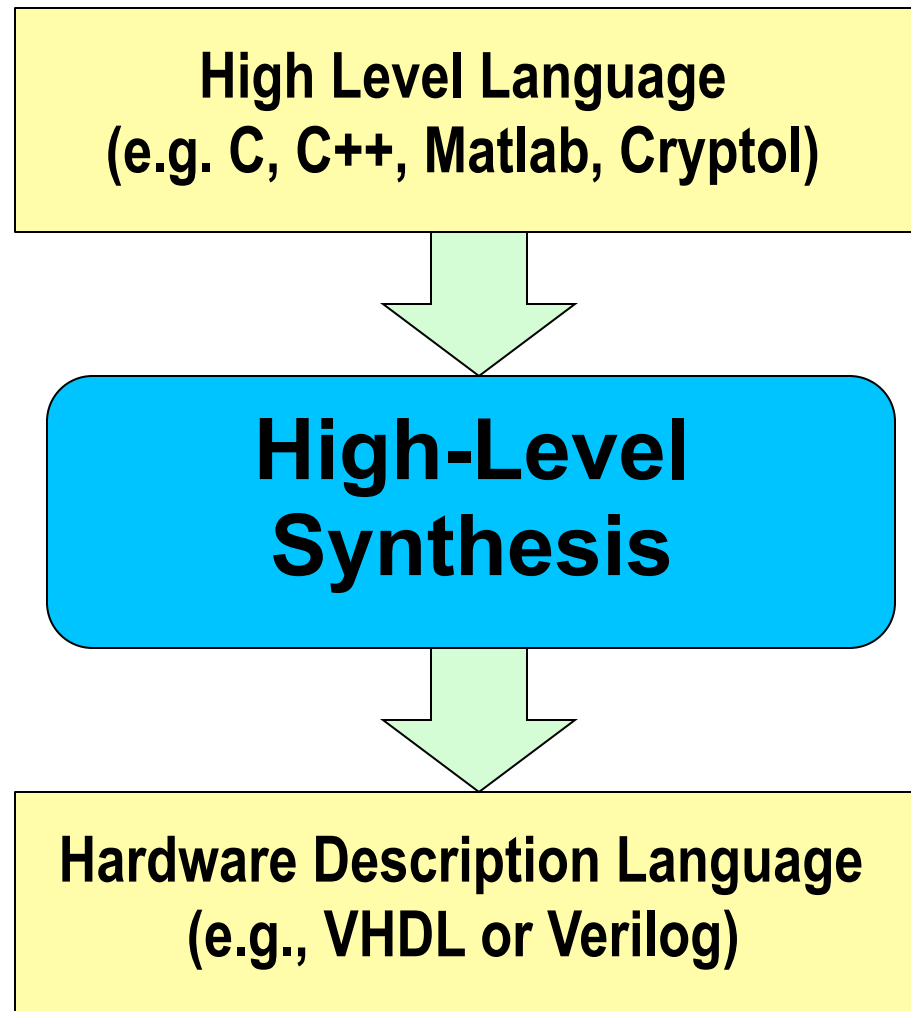
Cryptographic Standard Contests



Difficulties of Hardware Benchmarking

- **Growing number of candidates**
- **Long time necessary to develop and verify RTL (Register Transfer Level) VHDL or Verilog code**
- **Multiple variants of algorithms**
(e.g., 3 different key sizes in the AES Contest,
4 different output sizes in the SHA-3 Contest)
- **Multiple hardware architectures**
(based on folding, unrolling, pipelining, etc.)
- **Dependence on skills of the designers**

Potential Solution: High-Level Synthesis (HLS)



Short History of High-Level Synthesis

Generation 1 (1980s-early 1990s): research period

Generation 2 (mid 1990s-early 2000s):

- Commercial tools from Synopsys, Cadence, Mentor Graphics, etc.
- Input languages: behavioral HDLs Target: ASIC

Outcome: Commercial failure

Generation 3 (from early 2000s):

- Domain oriented commercial tools: in particular for DSP
- Input languages: C, C++, C-like languages (Impulse C, Handel C, etc.), Matlab + Simulink, Bluespec
- Target: FPGA, ASIC, or both

Outcome: First success stories

Cinderella Story

AutoESL Design Technologies, Inc. (25 employees)

Flagship product:

AutoPilot, translating **C/C++/System C** to **VHDL or Verilog**

- **Acquired by the biggest FPGA company, Xilinx Inc., in 2011**
- **AutoPilot integrated into the primary Xilinx toolset, Vivado, as Vivado HLS, released in 2012**

“High-Level Synthesis for the Masses”

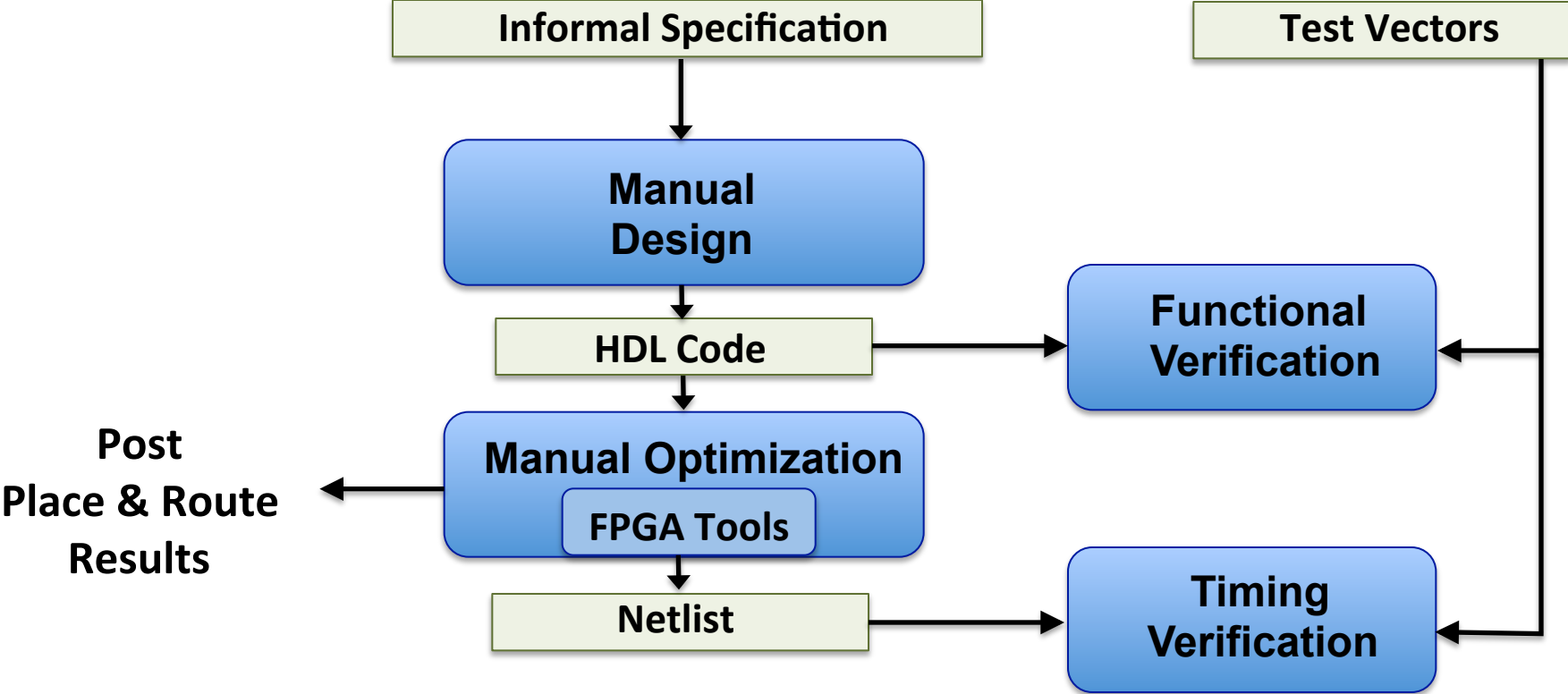
Our Hypothesis

- **Ranking** of candidate algorithms in cryptographic contests in terms of their performance in modern FPGAs will remain **the same** independently whether the HDL implementations are *developed manually* or *generated automatically* using High-Level Synthesis tools
- **The development time will be reduced by at least an order of magnitude**

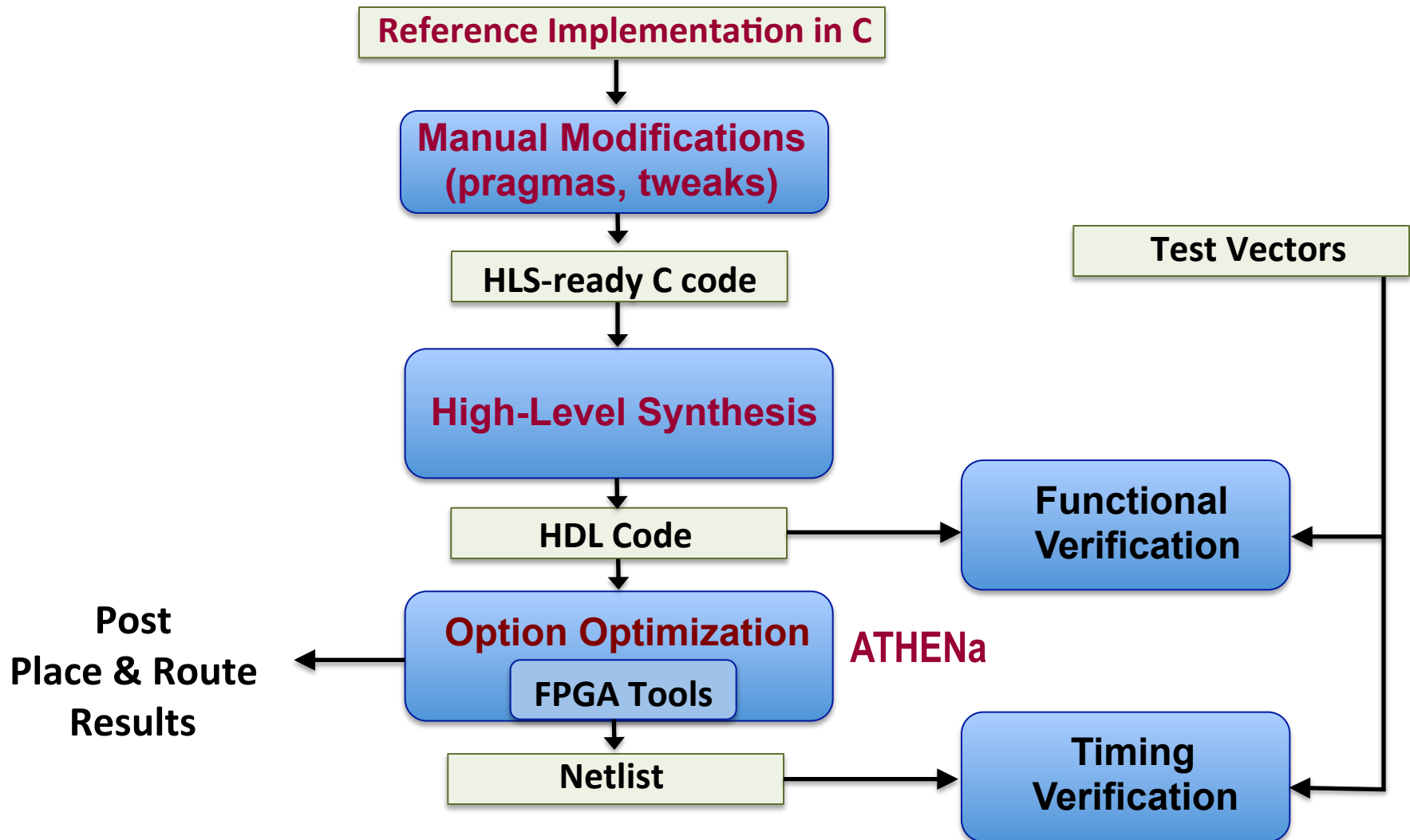
Potential Additional Benefits

- **Early feedback for designers of cryptographic algorithms**
 - **Typical design process based only on security analysis and software benchmarking**
 - **Lack of immediate feedback on hardware performance**
 - **Common unpleasant surprises,**
e.g., Mars in the AES Contest;
BMW, ECHO, and SIMD in the SHA-3 Contest

Traditional Development and Benchmarking Flow



HLS-Based Development and Benchmarking Flow



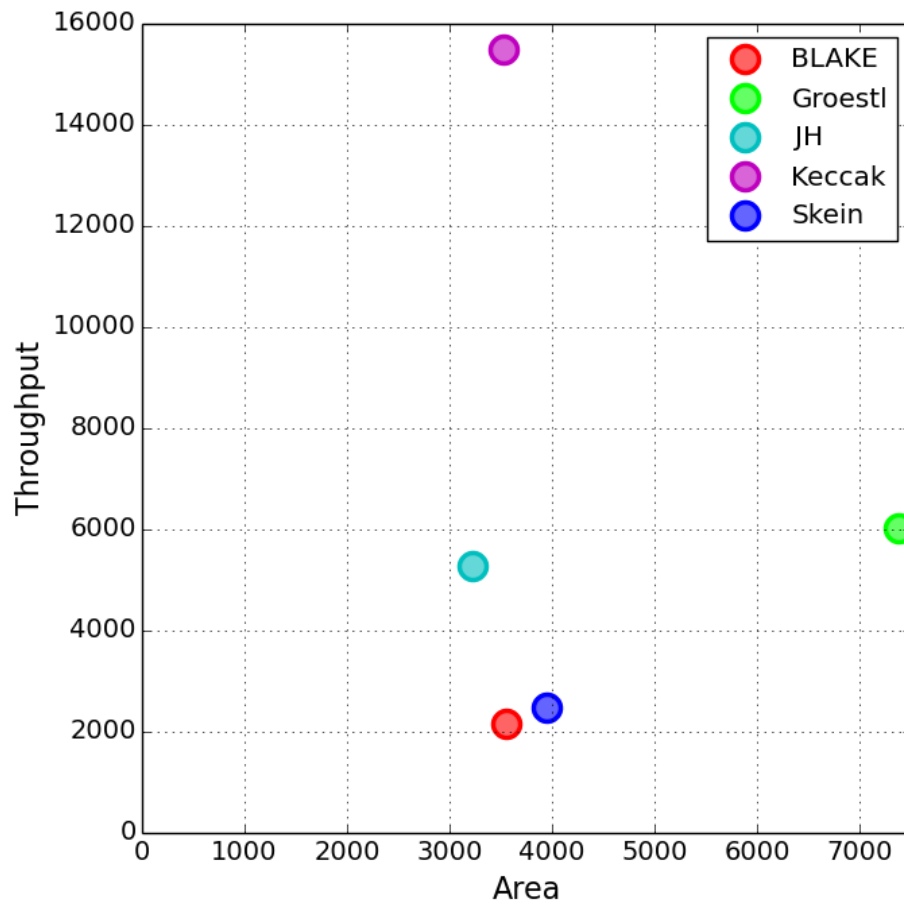
Our Test Case

- **5 final SHA-3 candidates**
- **Most efficient sequential architectures**
(/2h for BLAKE, x4 for Skein, x1 for others)
- **GMU RTL VHDL codes developed during SHA-3 contest**
- **Reference software implementations in C included in the submission packages**

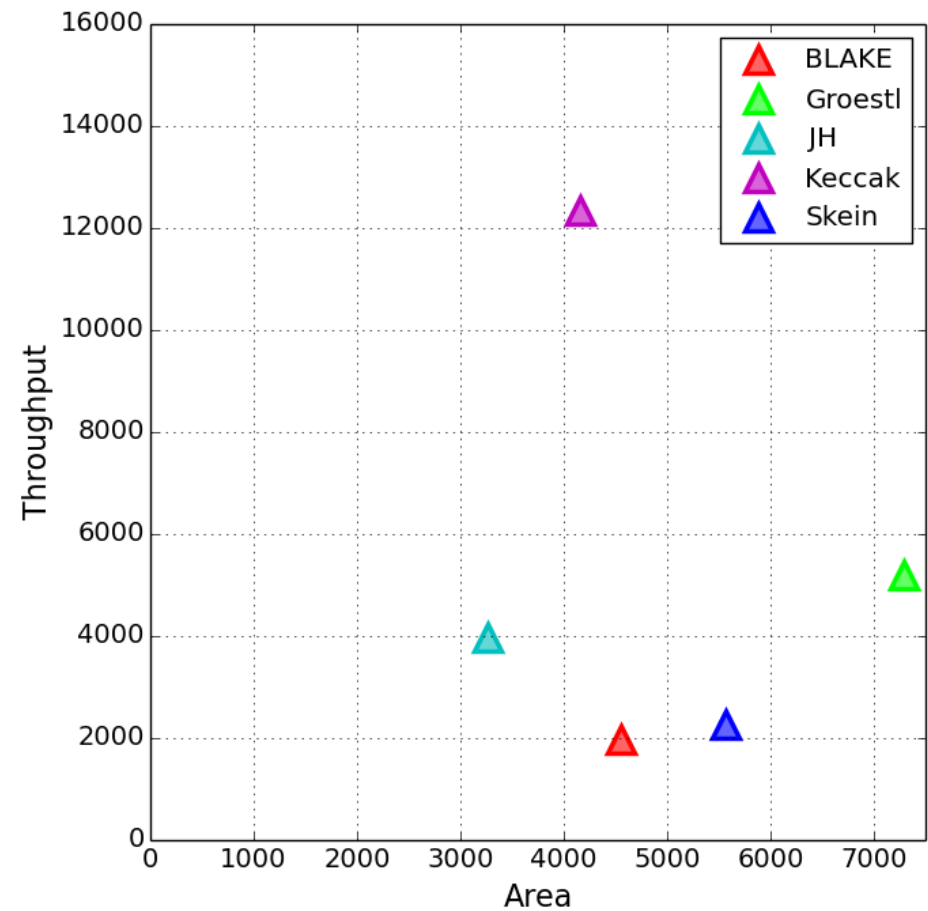
Hypotheses:

- **Ranking of candidates will remain the same**
- **Performance ratios RTL/HLS similar across candidates**

Manual RTL vs. HLS-based Results: Altera Stratix III

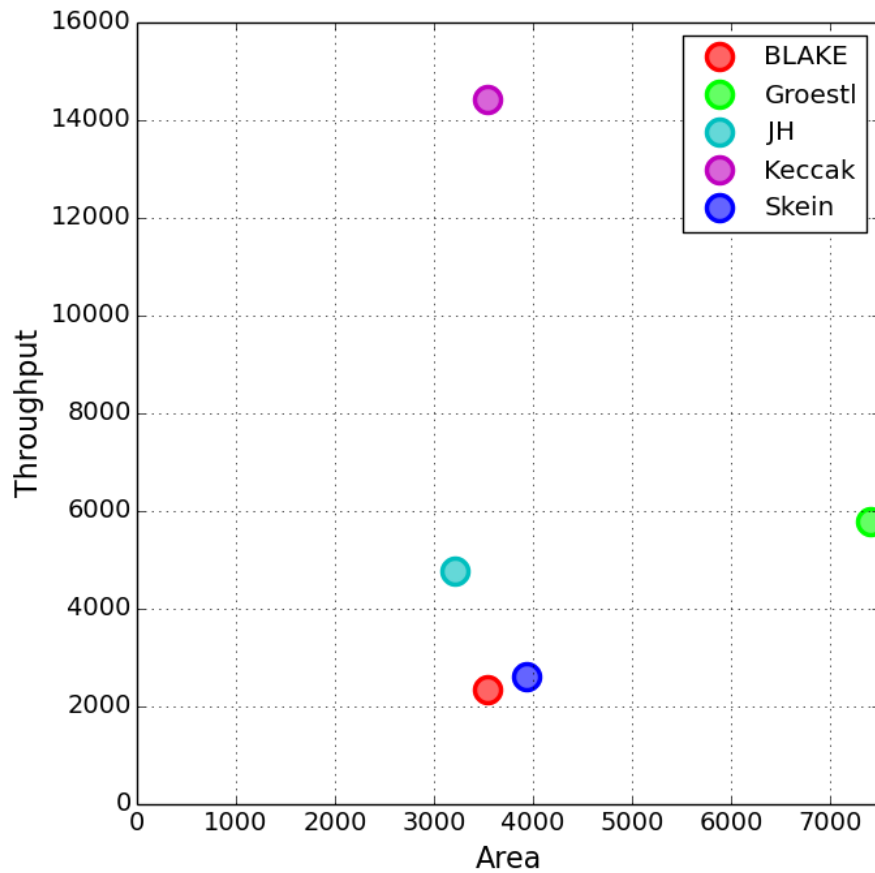


RTL

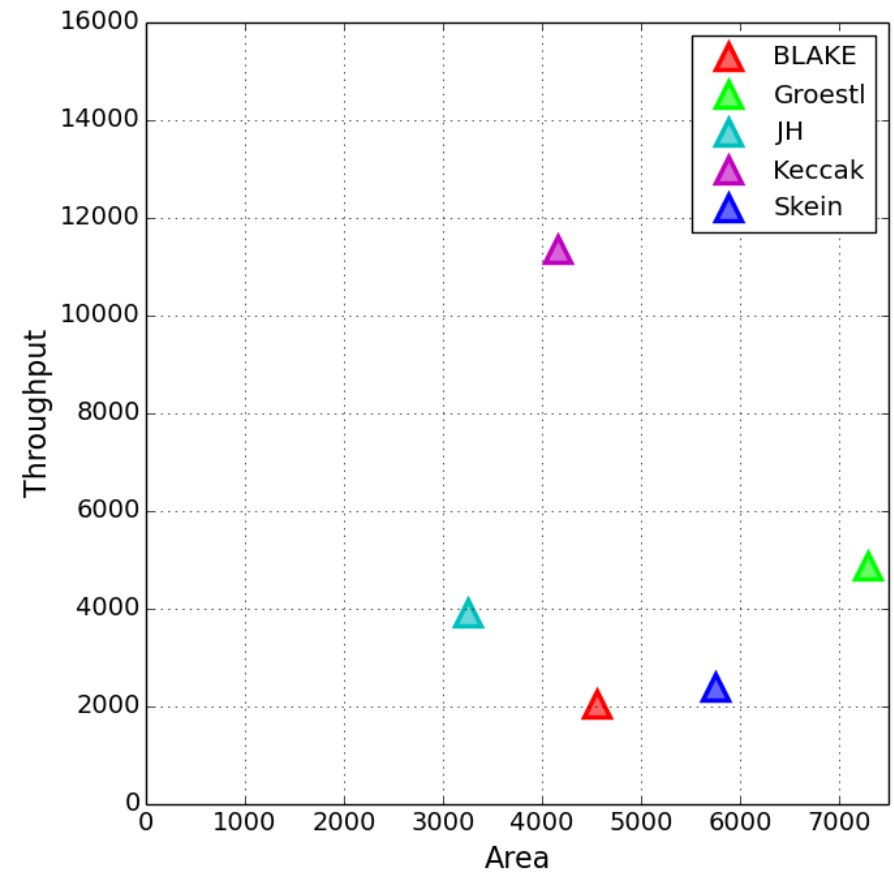


HLS

Manual RTL vs. HLS-based Results: Altera Stratix IV

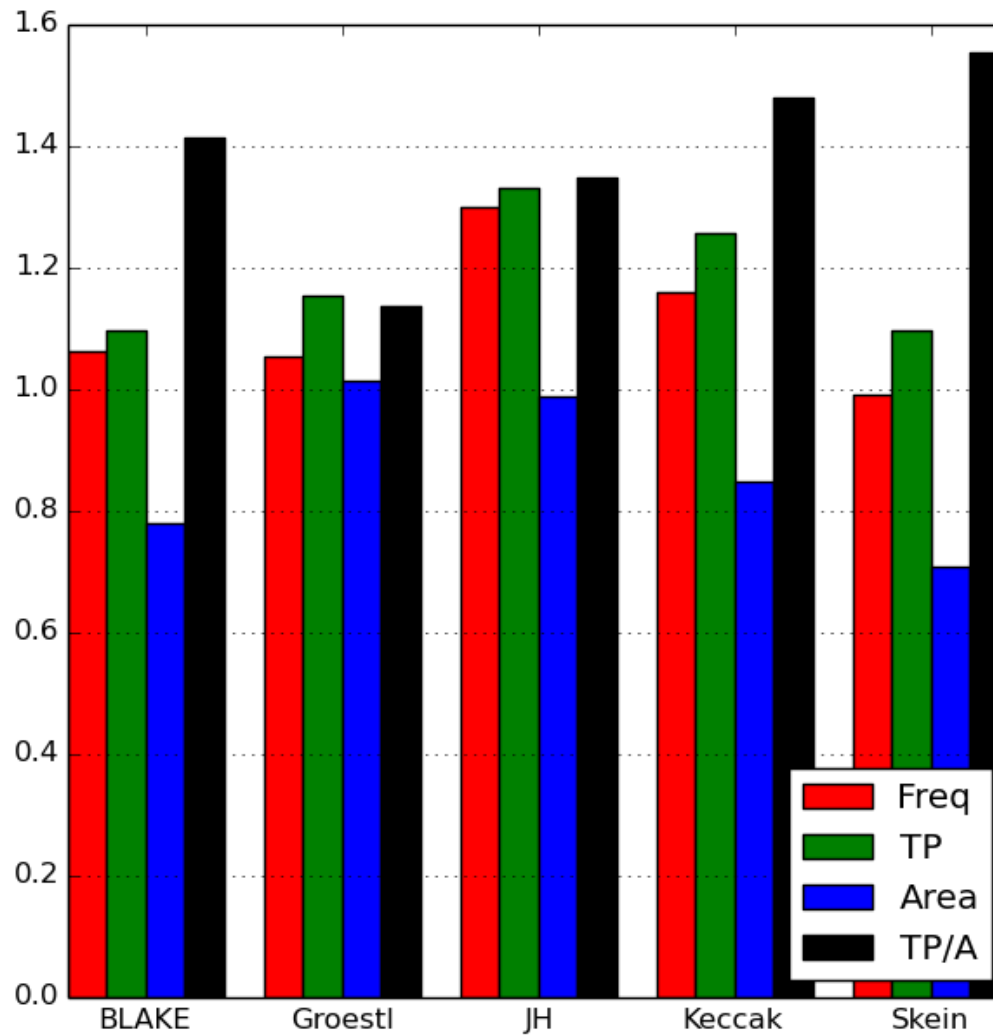


RTL

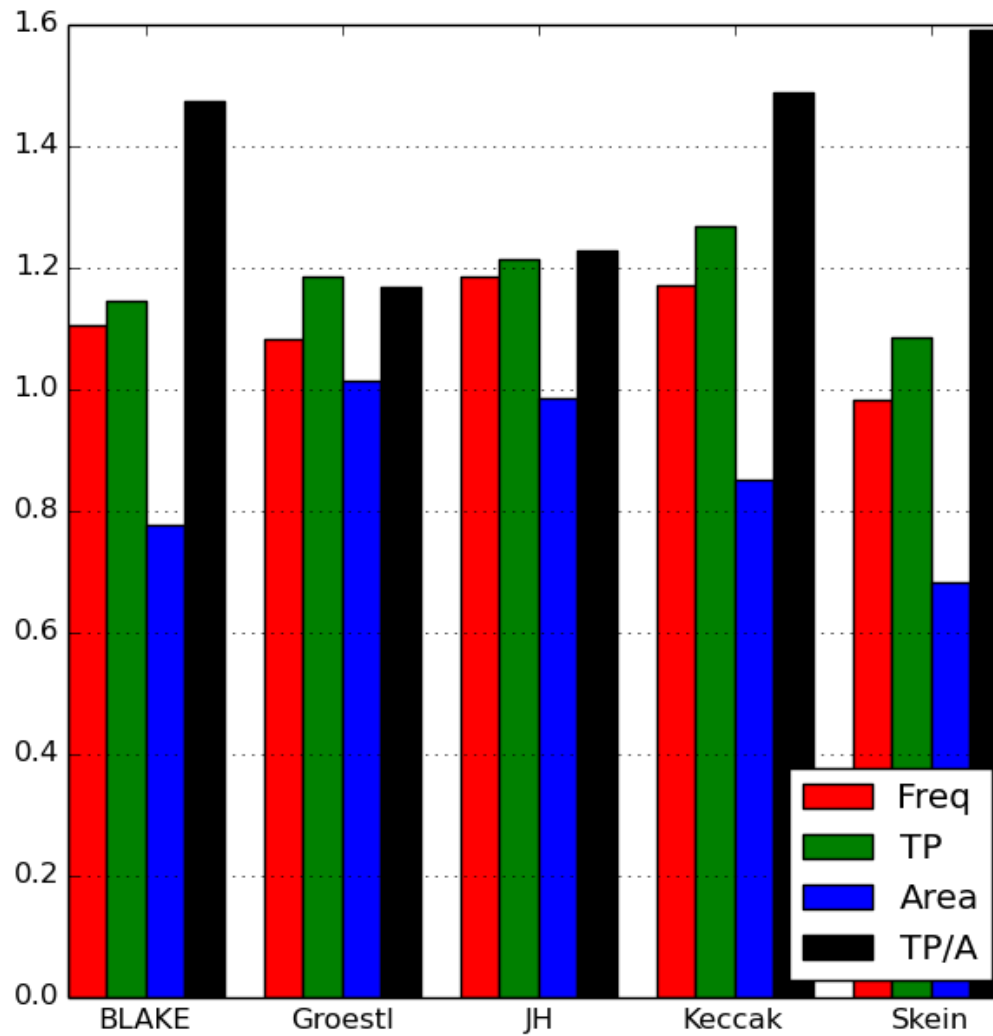


HLS

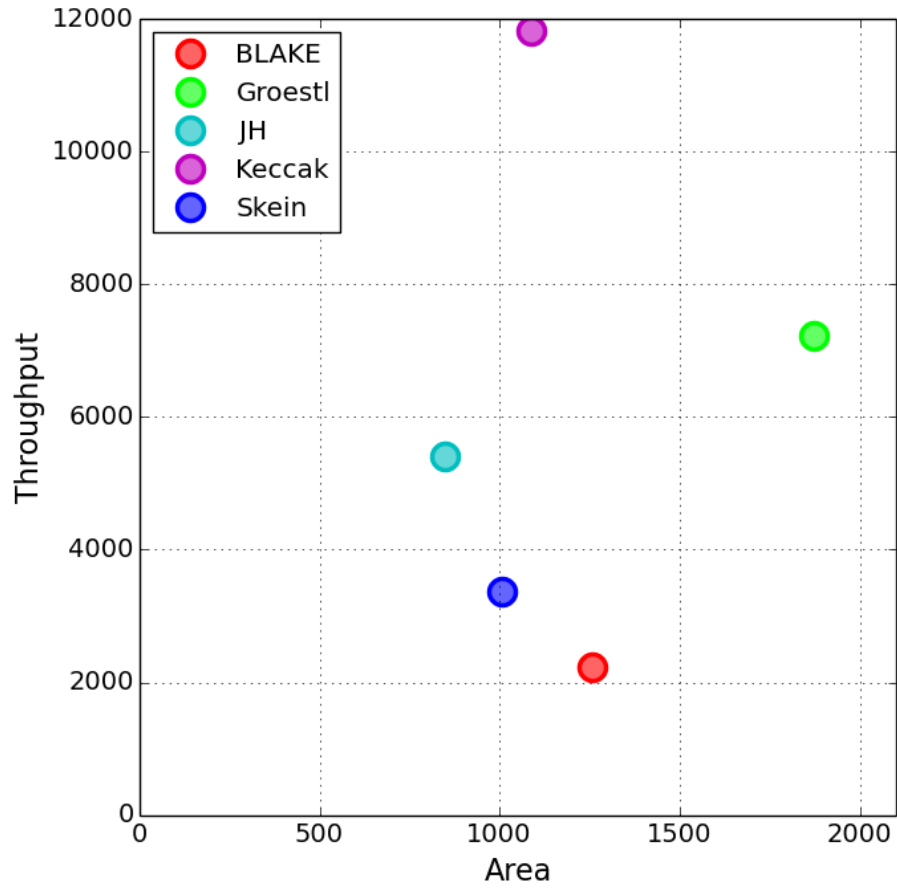
Ratios of Major Results RTL/HLS for Altera Stratix III



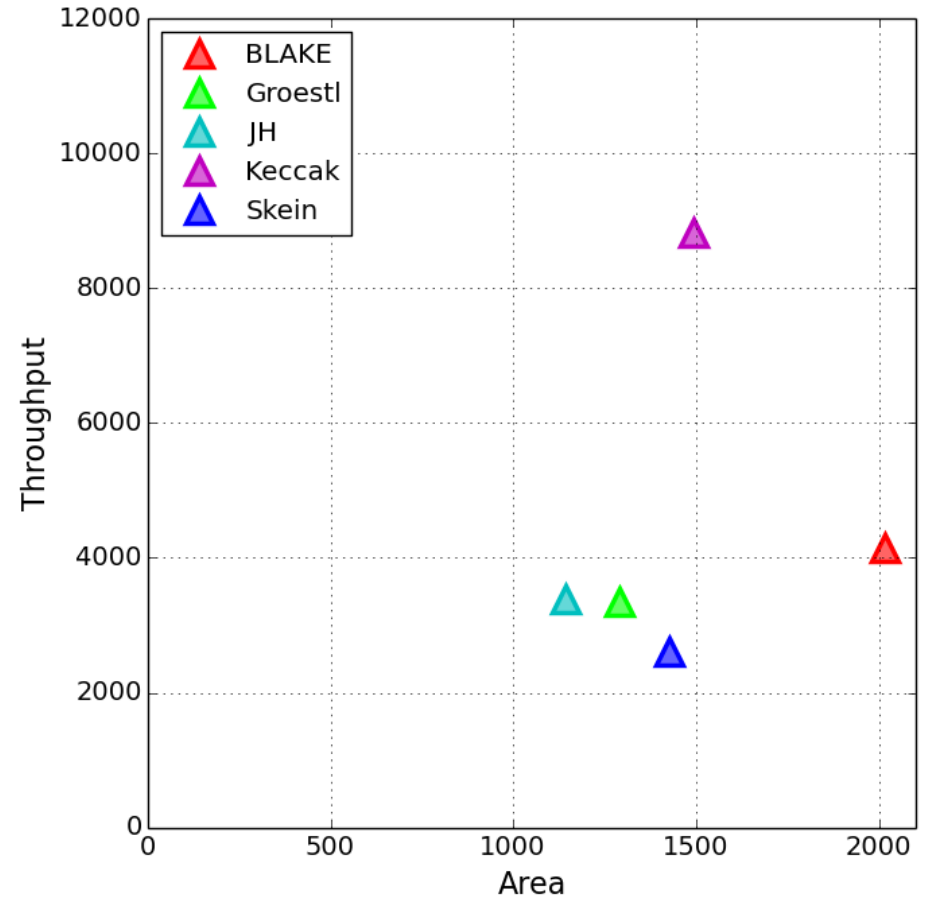
Ratios of Major Results RTL/HLS for Altera Stratix IV



Lack of Correlation for Xilinx Virtex 6

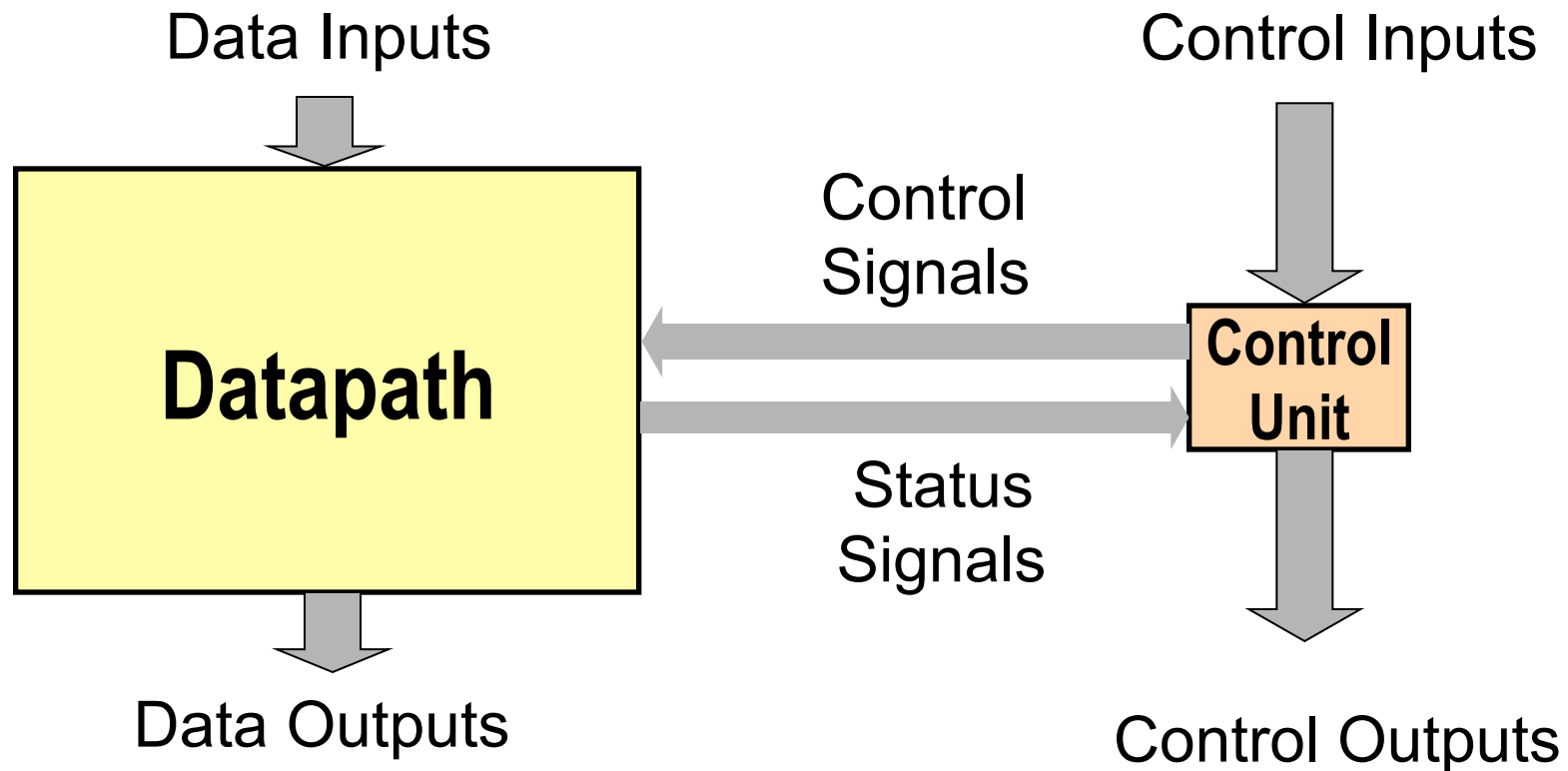


RTL



HLS

Datapath vs. Control Unit



Determines

- Area
- Clock Frequency

Determines

- Number of clock cycles

Encountered Problems

Datapath inferred correctly

- Frequency and area within 30% of manual designs

Control Unit suboptimal

- Difficulty in inferring an overlap between completing the last round and reading the next input block
- One additional clock cycle used for initialization of the state at the beginning of each round
- The formulas for throughput:

RTL: $\text{Throughput} = \text{Block_size} / (\#Rounds * T_{CLK})$

HLS: $\text{Throughput} = \text{Block_size} / ((\#Rounds+2) * T_{CLK})$

Hypothesis Check

Hypothesis I:

- Ranking of candidates in terms of **throughput, area, and throughput/area ratio** will remain the same

TRUE for Altera Stratix III and Stratix IV

FALSE for Xilinx Virtex 5 and Virtex 6

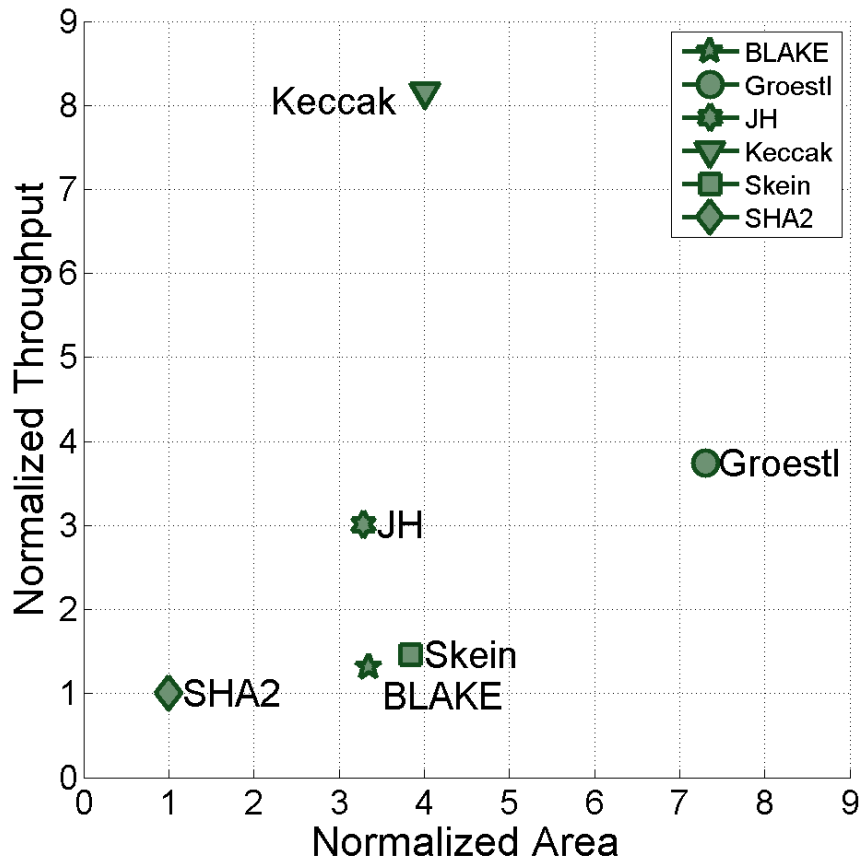
Hypothesis II:

- Performance ratios RTL/HLS similar across candidates

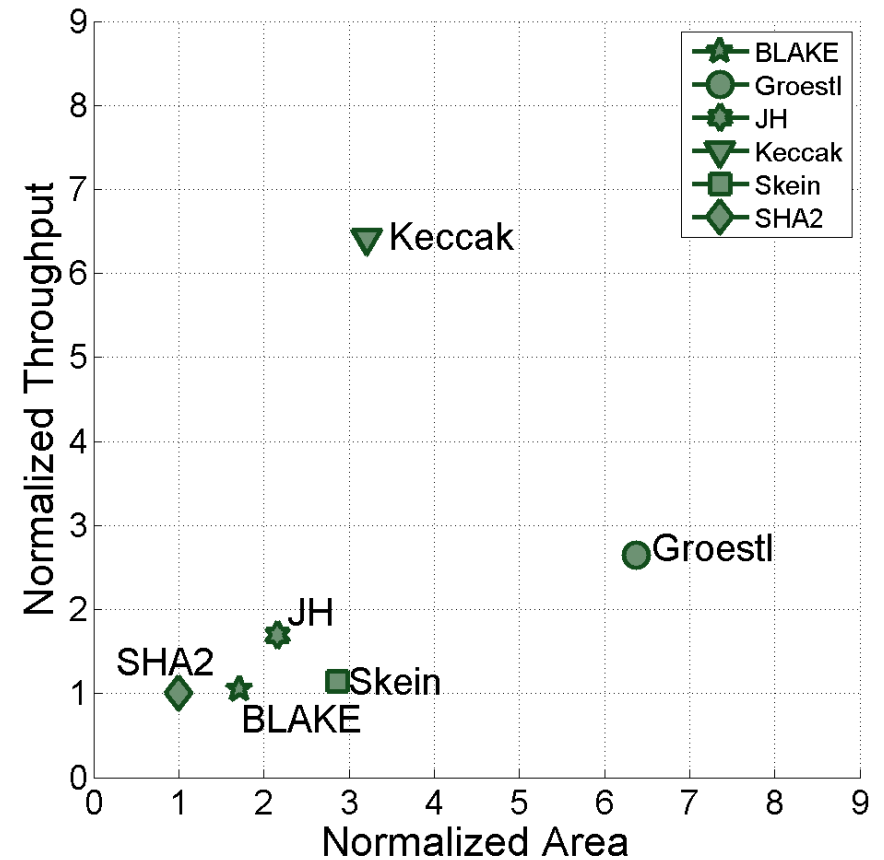
	Stratix III	Stratix IV
Frequency	0.99-1.30	0.98-1.19
Area	0.71-1.01	0.68-1.02
Throughput	1.10-1.33	1.09-1.27
Throughput/ Area	1.14-1.55	1.17-1.59

Correlation Between Altera FPGA Results and ASICs

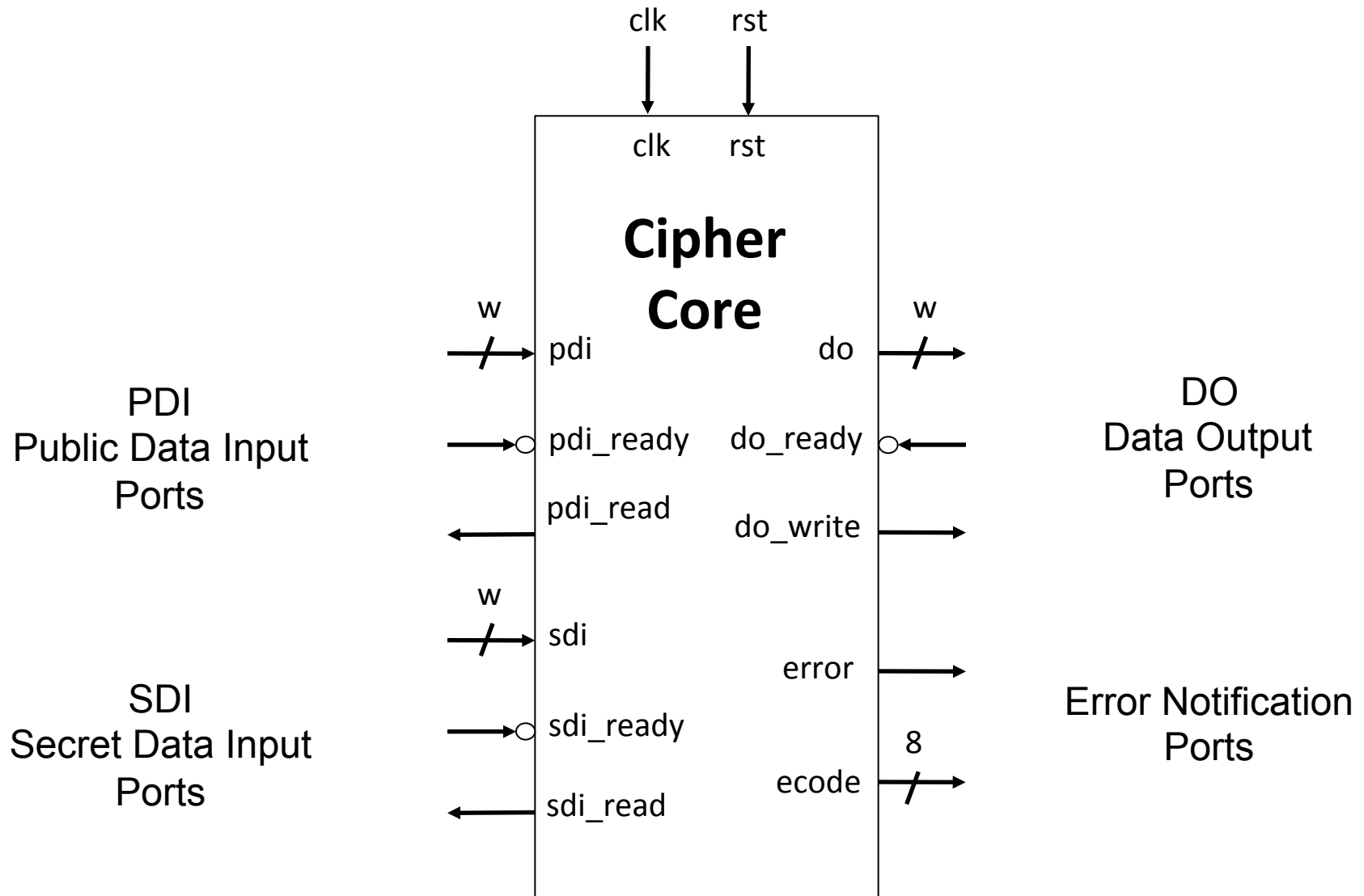
Stratix III FPGA



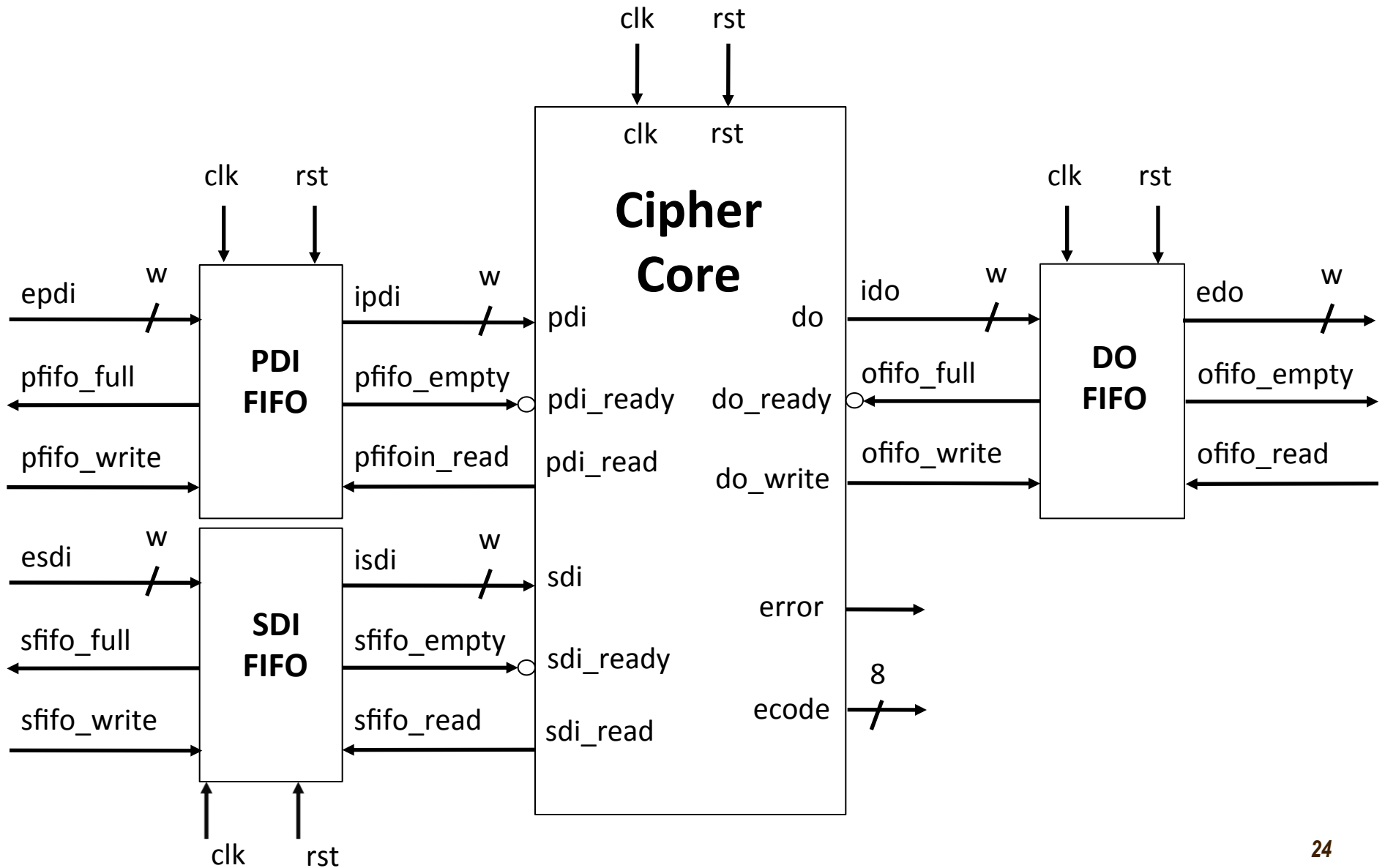
ASIC



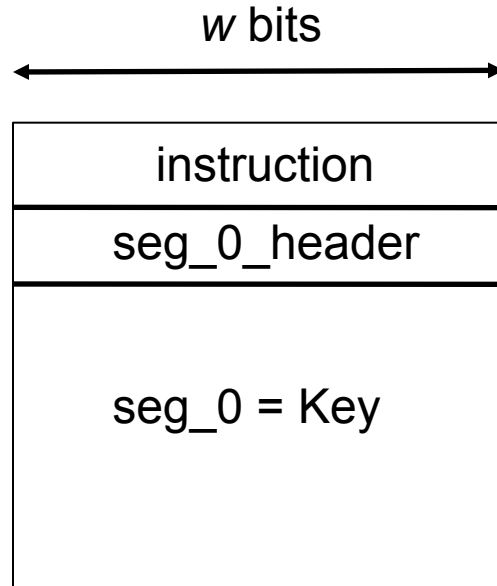
Proposed Interface for Authenticated Ciphers



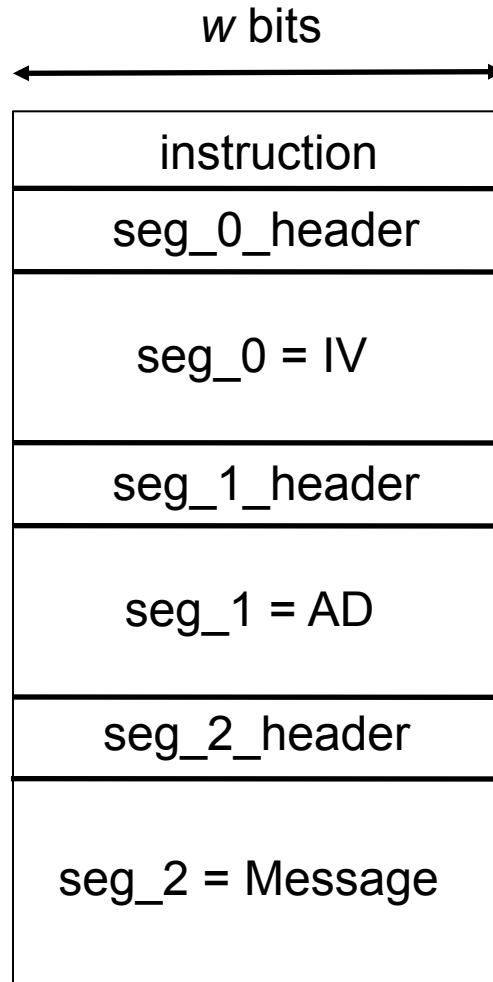
Typical External Circuit



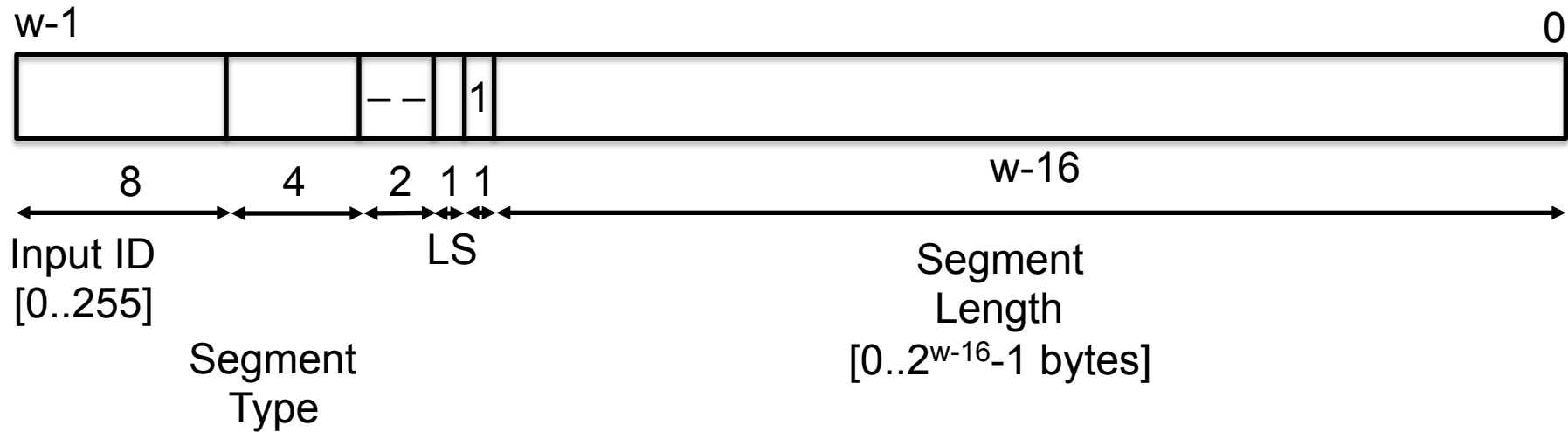
Format of Secret Data Input



Format of Public Data Input: Encryption



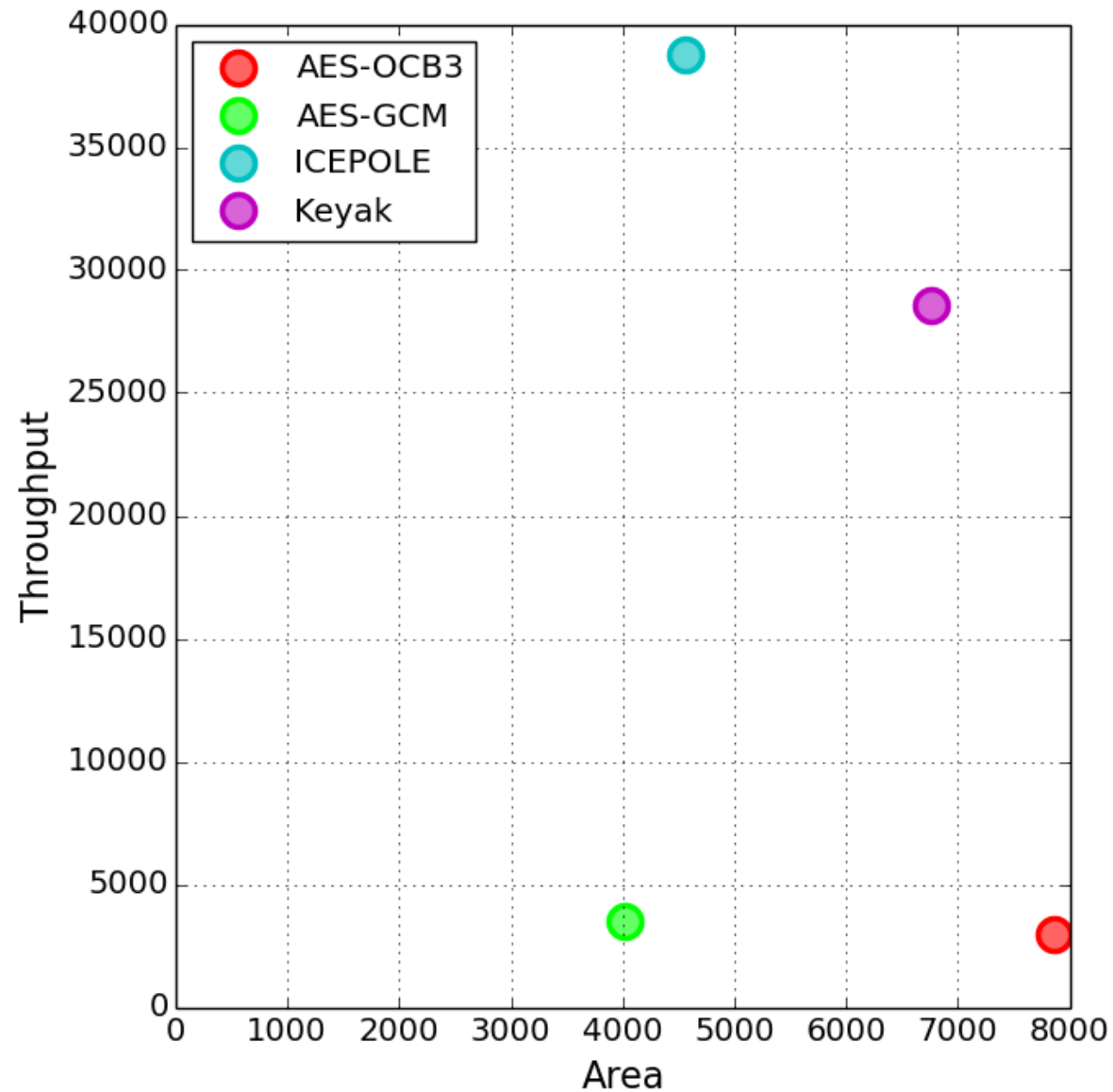
Format of Segment Header



- 0000 – Reserved
- 0001 – Initialization Vector
- 0010 – Associated Data
- 0011 – Message
- 0100 – Ciphertext
- 0101 – Tag
- 0110 – Key

LS = 1 if the last segment of input
0 otherwise


Manual RTL Designs Following Proposed Interface on Altera Stratix IV



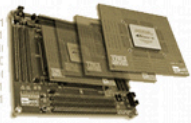
ATHENa Database of Results for Authenticated Ciphers

- **Already available at**
<http://cryptography.gmu.edu/athena>
- **Similar to the database of results for hash functions, filled with ~1600 results during the SHA-3 contest**
- **Results can be entered by designers themselves.**
If you would like to do that, please contact me regarding an account.
- **The ATHENa Option Optimization Tool supports automatic generation of results suitable for uploading to the database**

Ordered Listing with a Single-Best (Unique) Result per Each Algorithm



ATHENA
AUTOMATED TOOL FOR HARDWARE EVALUATION



Database of FPGA Results for Authenticated Ciphers

Show Help

Compare Selected

Show 25 entries

Copy CSV Excel

Result ID	Algorithm	Platform	Timing				
Result ID	Algorithm Enable Unique	Family	Enc/Auth TP [Mbits/s]	Dec/Auth TP [Mbits/s]	Auth-Only TP [Mbits/s]	Key Sched Time [ns]	Impl Freq [MHz]
14	ICEPOLE	Stratix IV GX	38,779	38,779	38,779	-	227.220
23	Keyak	Stratix IV GX	28,564	28,564	28,564	-	255.040
11	AES-GCM	Stratix IV GX	3,612	3,612	4,414	-	310.370
18	AES-OCB3	Stratix IV GX	2,911	2,911	2,911	-	250.190

Result ID Algorithm Stratix IV Enc/Auth TP [Mbits/s] Dec/Auth TP [Mbits/s] Auth-Only TP [Mbits/s] Key Sched Time [ns] Impl Freq [MHz]

First Previous 1 Next Last

Showing 1 to 4 of 4 entries (filtered from 20 total entries)

Details of Result ID 14

Algorithm

Associated Data Support:	-
IV or Nonce Size [bits]:	96
Transformation Category:	Cryptographic
Key Size [bits]:	128
Transformation:	Authenticated Cipher
Group:	CAESER Round 1
Algorithm:	ICEPOLE
Tag Size [bits]:	128
Secret Message Number:	-
Secret Message Number Size [bits]:	-
Message Block Size [bits]:	1,024
Other Parameters:	-
Specification:	icepolev1.pdf
Formula for Message Size After Padding:	-

Design

Design ID:	3
Primary Optimization Target:	Throughput/Area
Secondary Optimization Target:	-
Architecture Type:	Basic Iterative
Description Language:	VHDL
Use of Megafunctions or Primitives:	No
List of Megafunctions or Primitives:	-
Maximum Number of Streams Processed in Parallel:	1
Number of Clock Cycles per Message Block in a Long Message:	-
Datapath Width [bits]:	-
Padding:	Yes
Minimum Message Unit:	-
Input Bus Width [bits]:	256

Details of Result ID 14

Timing

Encryption/Authentication Throughput [Mbits/s]:	38,779
Decryption/Authentication Throughput [Mbits/s]:	38,779
Authentication-Only Throughput [Mbits/s]:	38,779
Synthesis Clock Frequency [MHz]:	-
Key Scheduling Time [ns]:	-
Requested Synthesis Clock Frequency [MHz]:	-
Requested Implementation Clock Frequency [MHz]:	-
Implementation Clock Frequency [MHz]:	227.220
(Encryption/Authentication Throughput)/ALUT [(Mbits/s)/ALUT]:	8.497
(Decryption/Authentication Throughput)/ALUT [(Mbits/s)/ALUT]:	8.497
(Auth-Only Throughput)/ALUT [(Mbits/s)/ALUT]:	8.497

Resource Utilization

ALUTs:	4,564
Flip Flops:	4,434
DSPs:	0
Memory Bits:	0

Power and Energy Consumption

Estimated Power [mW]:	-
Estimated Dynamic Power [mW]:	-
Estimated Static Power [mW]:	-
Estimated Energy/Bit [mJ/Gbit]:	-
Operating Conditions used for Estimation (V, Temp, Etc):	-
Measured Power [mW]:	-
Measured Dynamic Power [mW]:	-
Measured Static Power [mW]:	-

Comparison of Result #s 14 and 23

Algorithm

Associated Data Support:	on	on
IV or Nonce Size [bits]:	96	128
Transformation Category:	Cryptographic	Cryptographic
Key Size [bits]:	128	128
Transformation:	Authenticated Cipher	Authenticated Cipher
Group:	CAESER Round 1	CAESER Round 1
Algorithm:	ICEPOLE	Keyak
Tag Size [bits]:	128	128
Secret Message Number:	-	-
Secret Message Number Size [bits]:	-	-
Message Block Size [bits]:	1024	1344
Other Parameters:		
Specification:	icepolev1.pdf	keyakv1.pdf
Formula for Message Size After Padding:		

Design

Design ID:	3	6
Primary Optimization Target:	Throughput/Area	Throughput/Area
Secondary Optimization Target:		
Architecture Type:	Basic Iterative	Basic Iterative
Description Language:	VHDL	VHDL
Use of Megafunctions or Primitives:	No	No
List of Megafunctions or Primitives:		
Maximum Number of Streams Processed in Parallel:	1	1
Number of Clock Cycles per Message Block in a Long Message:	-	12
Datapath Width [bits]:	-	1600
Padding:	Yes	Yes
Minimum Message Unit:		
Input Bus Width [bits]:	256	128
Output Bus Width [bits]:	256	128
Implementation URL:		
Shared I/O Bus:	No	No
Encryption/Auth Throughput Formula:	$1024/(6*T)$	$1344/(12*T)$
Decryption/Auth Throughput Formula:	$1024/(6*T)$	$1344/(12*T)$
Authentication-Only Throughput Formula:	$1024/(6*T)$	$1344/(12*T)$
Key Scheduling Time Formula:		

Implementation of CAESAR Round 1 Candidates

- **30 Round 1 CASER candidates** to be implemented manually in VHDL as a part of the graduate class taught at GMU in Fall 2014. **One cipher per student.**
- **One PhD student, Ice,** will implement the same **30 ciphers** in parallel using HLS.
- Preliminary results in **mid-December 2014**, about a month before the announcement of Round 2 candidates.
- Deadline for **second-round Verilog/VHDL**: April 15, 2014.

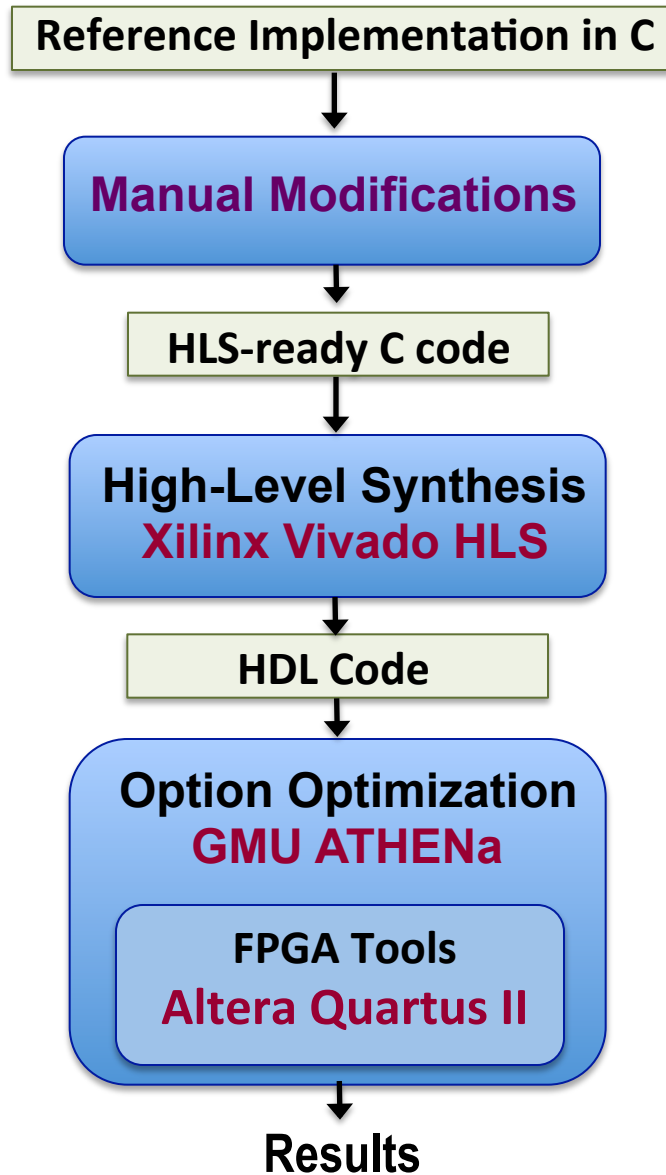
Support for CAESAR Teams

- **Our Team would be happy to work closely with the designer teams**
- **About 50 candidates remaining vs. 30 students working on VHDL designs this Fall**
- **If you would like your candidate cipher to be implemented in VHDL, please do not hesitate to contact me ASAP.**

Conclusions

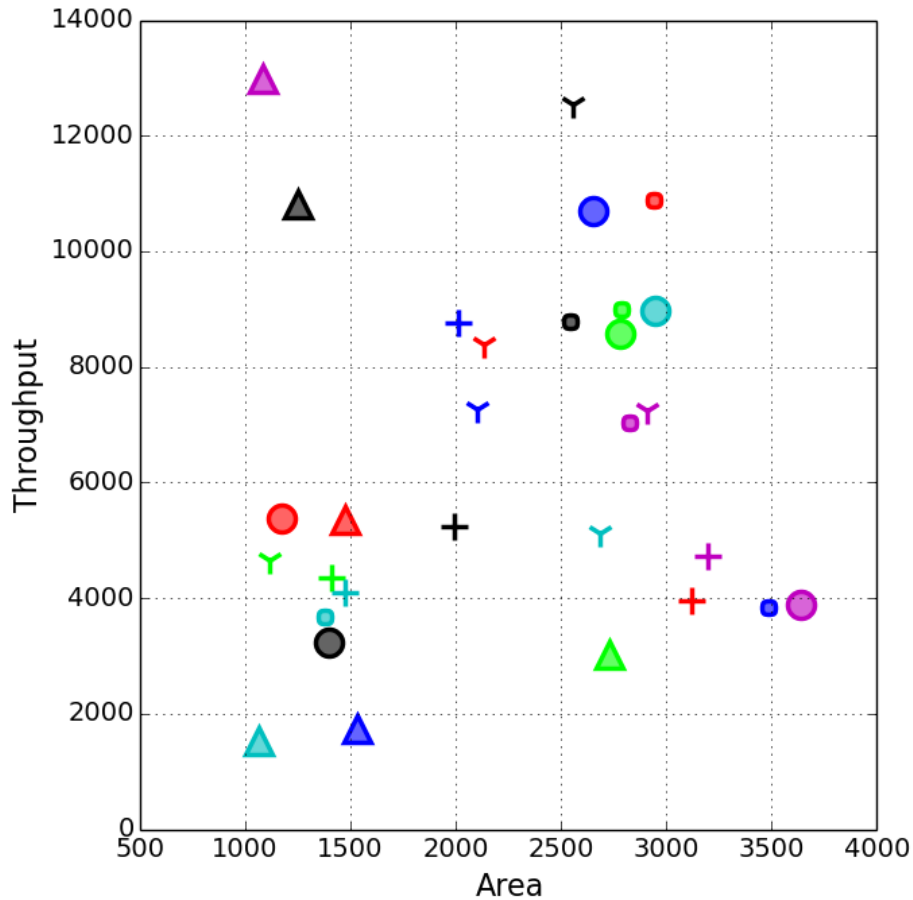
- **High-level synthesis offers a potential to allow hardware benchmarking during the design of cryptographic algorithms and in early stages of cryptographic contests**
- **Case study based on 5 final SHA-3 candidates demonstrated correct ranking for Altera FPGAs for all major performance measures**
- **More research needed to overcome remaining difficulties, such as**
 - **Limited correlation with manual RTL designs for Xilinx FPGAs**
 - **Suboptimal control unit.**

Most Promising Methodology & Toolset

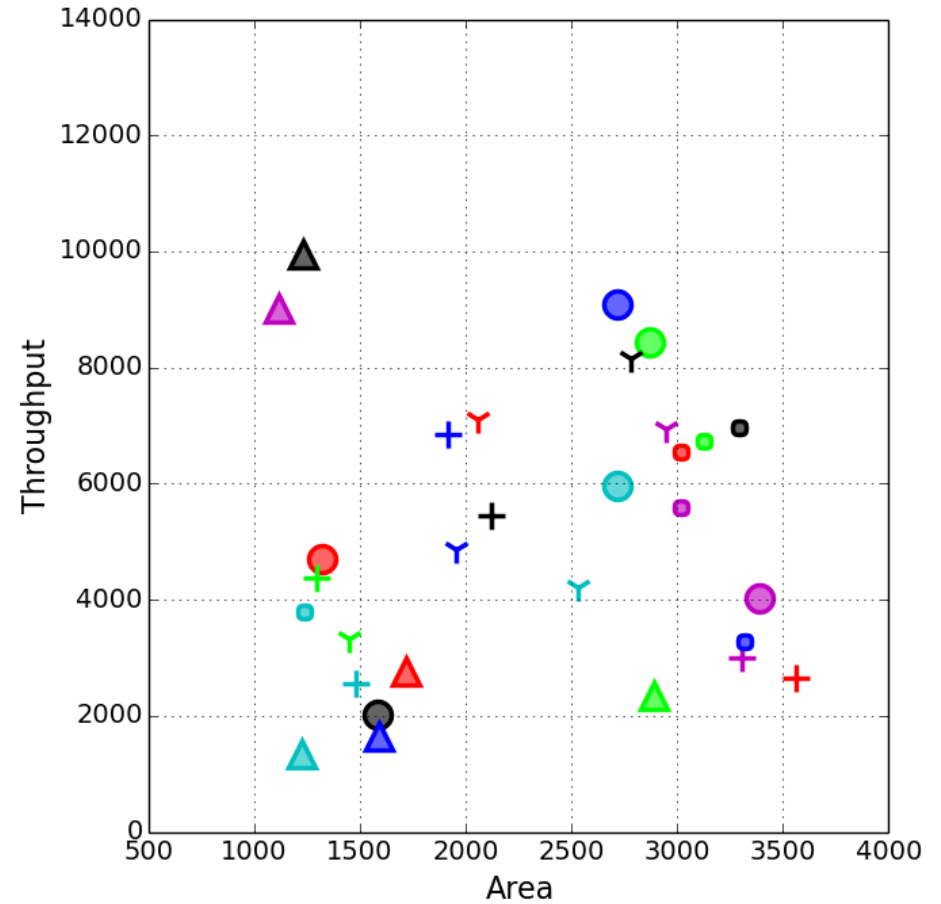


Frequency & Throughput decrease
Area increases
by no more than 30%
compared to manual RTL

Expected by the end of 2014



20-30 RTL results
generated by **20-30 GMU students**



30 HLS results
generated by **"Ice" alone**

Thank you!

Questions?



Suggestions?

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

CERG: <http://cryptography.gmu.edu>