FPGA PERFORMANCE OPTIMIZATION, FOR CAESAR AUTHENTICATION CIPHERS

Maria Katsaiti, Nicolas Sklavos, Apostolos Fournaris

SCYTALE Research Group,
Computer Engineering & Informatics Department,
University of Patras, Hellas, (Greece)
E-mail : katsaiti@ceid.upatras.gr

Thank you to…


IN·DEI·NOMINE·FELICITER
Radboud Universiteit Nijmegen


CRYPTACUS

Affiliated with…

UNIVERSITY OF PATRAS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

SCYTALE group

Scytale Research Group

- Faculty Members,
- Researchers & Associate Researchers,
- Students (Ph.D., M.Sc., B.Sc.),
- Visitors from other Universities & Institutes.

For more information,
please visit:
www.skytale.ceid.upatras.gr

Outline

- ✓ Cryptography and Competitions
- ✓ Introduction to CAESAR and CAESAR Hardware API
- ✓ Acquaintance with selected CAESAR ciphers
- ✓ Implementation of inner-round pipelining on ciphers
- ✓ Results and conclusions

Cryptography and competitions

History of cryptographic competitions :

- AES, 2000 organized by NIST,
- eSTREAM, 2008 run by EU CRYPT,
- SHA-3, 2012 held by NIST,
- CAESAR, final portfolio will be announced in mid December, 2017

CAESAR is held by the International Cryptologic Research Community and partially funded by NIST.

CAESAR

CAESAR → Competition for Authenticated Encryption: Security, Applicability and Robustness

Purpose → Improvisation of innovative, authenticated ciphers that :

- will offer advantages over AES-GCM, and
- will be suitable for widespread adoption.

Start date : January 2013, 57 candidates

End date : December 2017, 15 finalists in Round 3

Cipher Virtues

Apart from the requirements of the Committee, authenticated ciphers should always assure the qualities of :

- confidentiality,
- integrity and
- authenticity.

These virtues are also defined as **security goals**.

Procedural CAESAR details

- ✓ Competition organized in knock-out rounds.
- ✓ Hardware implementation and any applicable tweaks are added along during the procedure.
- ✓ Committee decides whether a cipher meets expectations or not and whether is developed according to preset, universal specifications.

Specifications of CAESAR competition

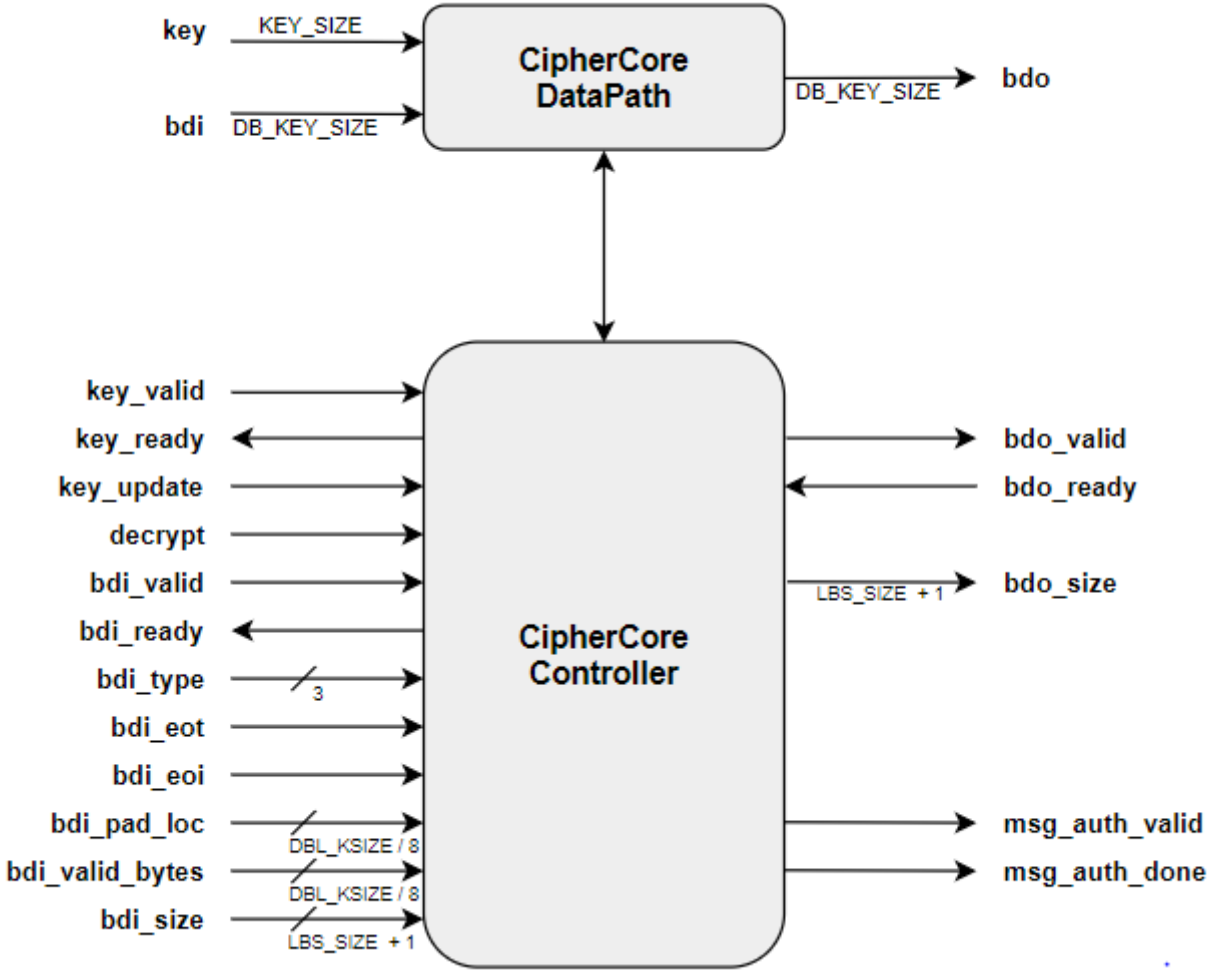
- ✓ Cipher description in any HDL language.
- ✓ Hardware implementation on CAESAR API.
- ✓ Universality allows a fair ground for comparisons.

CAESAR hardware API

CAESAR Hardware API is basically an I/O interface, allowing flexible :

- reception,
- segmentation and
- formatting of the data processing.

CAESAR hardware API



Target of this work..

- ✓ Optimization of performance on CAESAR ciphers
- ✓ The procedure of selection was based on their ability for parallelism.
- ✓ A very promising technique for acceleration of speed is pipelining.
- ✓ Results and measurements will prove pipelining to be beneficial or of no use.

Selected Ciphers : AES - OTR

- Designed by : K. Minematsu

- Input : key, nonce, AD and plaintext
- Output : Ciphertext, tag

- Instantiation of OTR based on AES blockcipher with a selection for parallel or serial AD processing.

Selected Ciphers : Deoxys

- Designers : J. Jean, I. Nikolic, Th. Peyrin , Y. Seurin
- Cipher is built upon a tweakable block cipher, Deoxys – BC, using AES round function as a basic building block.
- Deoxys is promising security, even when nonce is reused.
- Possible instantiation using a general framework, known as TWEAKEY.

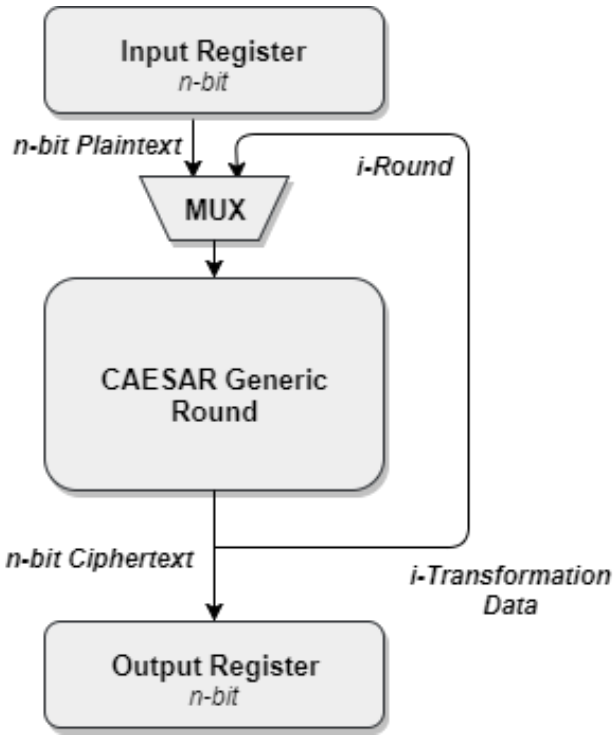
Selected Ciphers : OCB

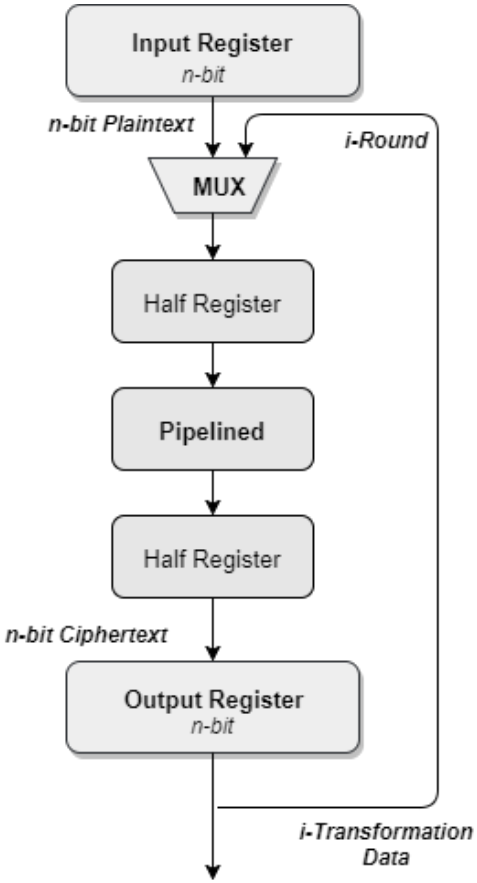
- Designers : T. Krovetz, Ph. Rogaway
- Significantly fast encryption algorithm.
- Consists of AES-GCM as basic building block.
- Nonce in OCB is not allowed to be reused, as confidentiality is endangered.

Pipelining technique

- Long logic paths augment delays in a circuit.
- Pipelining is a design trick, according to which, placement of registers in circuits can help lessen the delays.
- Inner-round pipelining, especially, refers to the placement of these registers inside the round function of the cipher.

Generic Vs pipelining architecture





How we did it..

In this work we..

- described selected ciphers in VHDL,
- simulated our designs with Modelsim and
- implemented in Virtex-6 FPGA device, using Xilinx Vivado Design Suite.

Our metrics focused on their **efficiency**, **throughput**, **area** and **throughput-to-area** ratio (T/A).

Implementation synthesis results

	AES-OTR	Deoxys	OCB
Key Size	128 bits	128 bits	128 bits
Rounds	10	14	10
Throughput improvement	55%	37%	27%
Area increase	49%	41%	13%
Throughput to Area (T/A) ratio	5%	-9%	15%

In a nutshell..

- ✓ Introduction to CAESAR competition.
- ✓ Acquaintance with selected CAESAR ciphers.
- ✓ Implementation of inner-round pipelining on ciphers.
- ✓ Results and performance of the pipelining technique.

Future work focusing on..

- ✓ Improving performance of pipelining on all ciphers.
- ✓ Implementing inner-round pipelining on the final portfolio.
- ✓ New approaches for speed acceleration and performance boost.

Thank you for your attention!

For more information contact:

katsaiti@ceid.upatras.gr