WRIGHT STATE UNIVERSITY

SCAN Cryptoprocessor

Raghudeep Kannavara[1], Dr. Nikolaos Bourbakis[1], Dr. Apostolos Dollas[2]

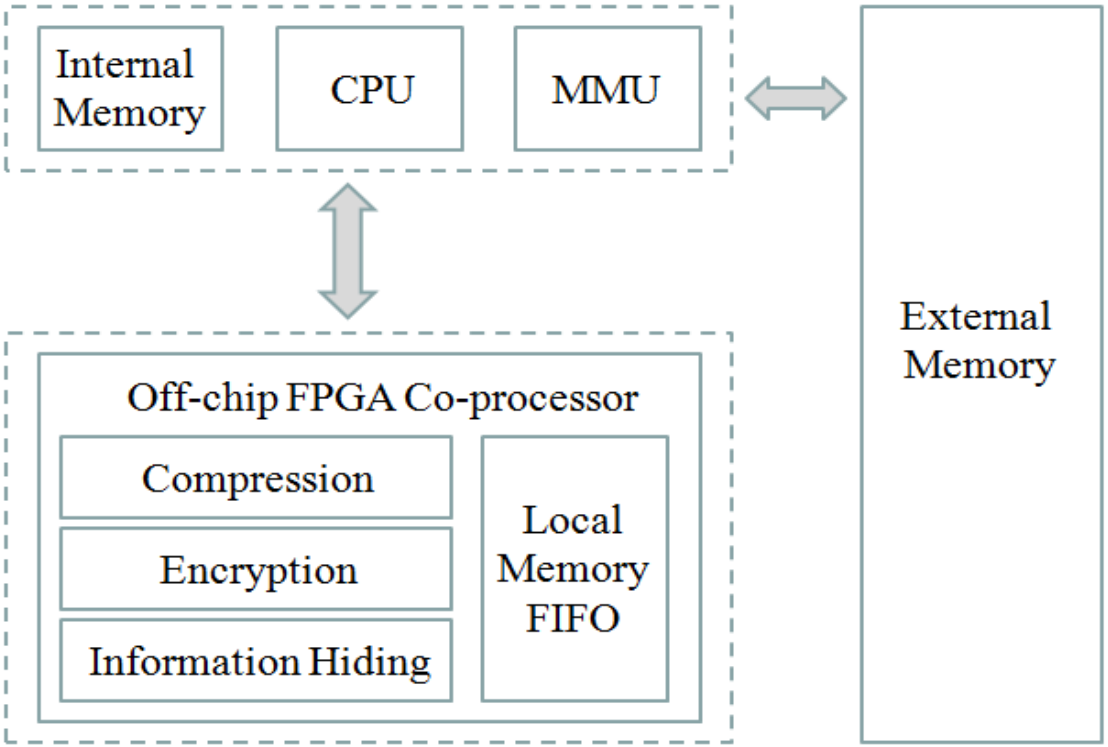
[1]ATR Center, Wright State University, Dayton, OH 45435

[2]Technical University of Crete, 73100 Chania, Crete, Greece

*This work is partially supported by ARL, CGO Inc and AIIS Inc funding.

This work presents the architecture and instruction set of the SCAN cryptoprocessor. The SCAN cryptoprocessor is a modified SparcV8 processor architecture with a new instruction set to handle image compression, encryption and information hiding based on the SCAN methodology, the modules for which are implemented in reconfigurable logic and the results of the FPGA synthesis are presented.

A tightly coupled coprocessor architecture with dedicated data-path and a local memory system, interacting with the main processor through asynchronous FIFOs which enable the coprocessor to be implemented with a clock frequency different from the processor system, is proposed.



New Instruction Set

LOADIMG
STOREIMG
LOADMSG
STOREMSG
LOADKEY1
LOADKEY2
LOADSEED
CMPRS_IMG
DCMPRS_IMG
ENCRYPT
DECRYPT
INFOHIDE
INFOEXTRACT
CMPRS_ENCR
DECR_DCMPRS
INFOHIDE_CMPRS
DCMPRS_INFOEXTRACT
INFOHIDE_ENCR
DECR_INFOEXTRACT
INFOHIDE_CMPRS_ENCR
DECR_DCMPRS_INFOEXTRACT

FPGA Synthesis Results

WRIGHT STATE UNIVERSITY

Module	Slices of Virtex XCV600	% occupied
Block Error Module (four blocks)	164	2.3
Context Module (four blocks)	148	2.14

Synthesis results – Logic distribution - Compression Module

Module	Number of clock cycles
Block Error Module	131072
Context Module	4096

Clock cycles for Image compression (Image size = 128x128, Block size = 64x64)

Module	Slices of Virtex XCV600	% occupied
Encrypt Module (one block)	33	0.47
Decrypt Module (one block)	33	0.47

Synthesis results – Logic distribution – Encryption, Decryption Module

Module	Number of clock cycles
Encrypt Module	4096
Decrypt Module	4096

Clock cycles for Image Encryption (Image size = 128x128, Block size = 64x64)

Module	Slices of Virtex XCV600	% occupied
Embed Module	40	0.57
Extract Module	26	0.37
Complexity Module	80	1.15

Synthesis results – Logic distribution - Message Embedding, Extraction Module

The number of clock cycles required for information hiding depends on the size of the message and the complexity matrix of the cover image.