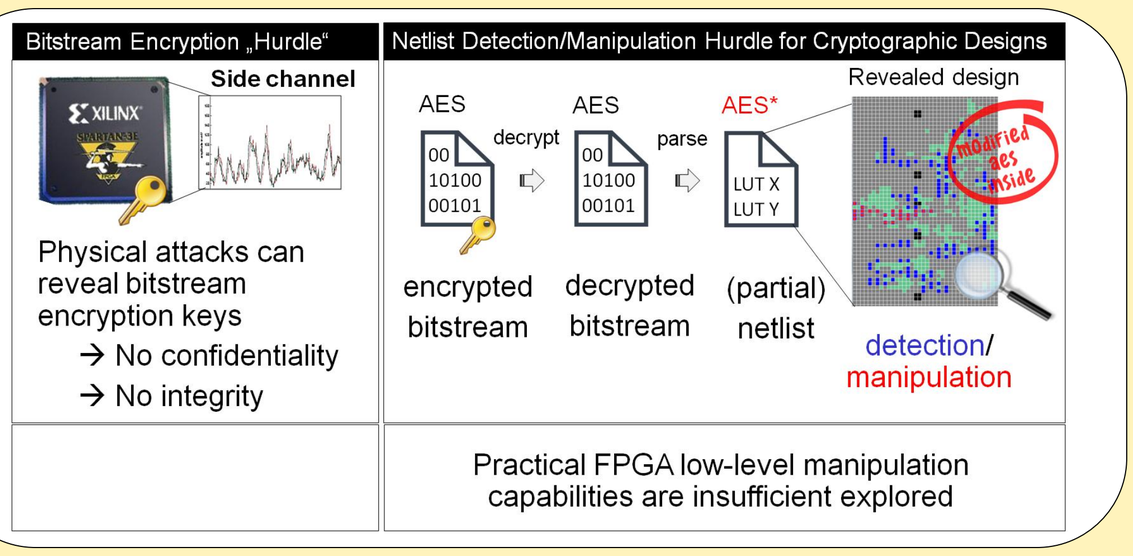
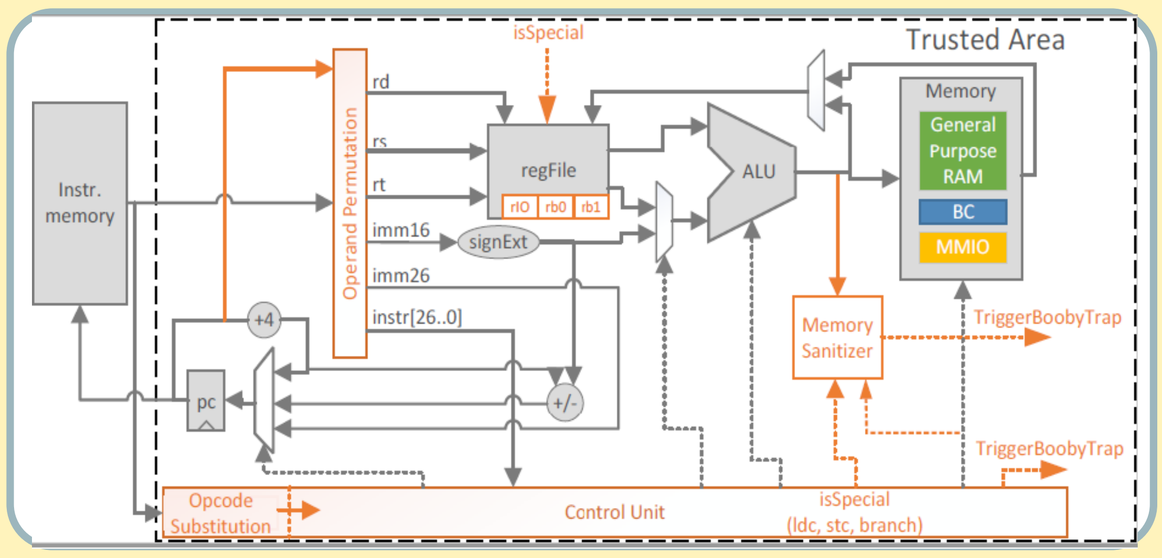
New Directions in FPGA Security

PIs: Russell Tessier and Christof Paar, University of Massachusetts, Amherst

Motivation – Exploring Attacker's FPGA Manipulation Capabilities

This project explores new techniques to protect FPGA designs from reverse engineering





Problem #1: A static attacker might obtain a third-party netlist even if bitstream encryption used

- FPGA design can become available from bitstream
- Manipulation possible in real-world applications

Problem #2: Soft processor instructions can be reverse engineered

- FPGA-based processors increasingly used
- Observation can reveal execution algorithm even if encryption used

Approaches

Overcoming bitstream manipulation

- Learn techniques used to find crypto cores (e.g. AES)
- Crypto cores in bitstream can be incomplete – Initialize after bitstream loaded
  - Implemented with low overhead

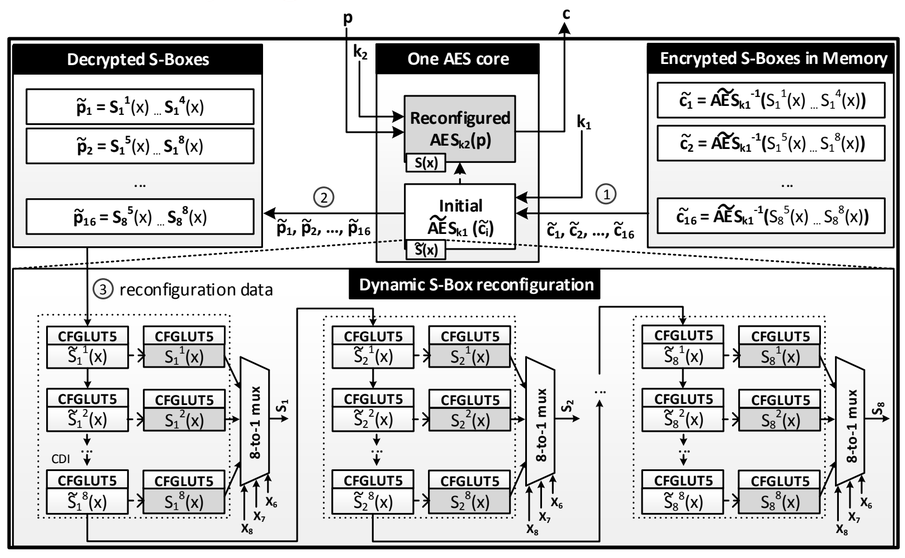
Building a diverse execution environment for soft processors

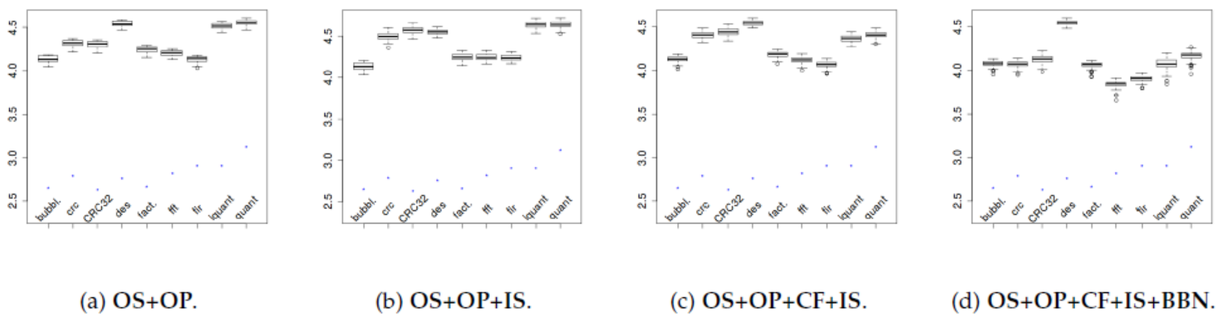
- Scramble the instruction format per implementation
- Isolate external I/O access
- Code flattening

AES detection results

Design	Synth. script	S-Box Column Detection	Sub-graphs	Overall time (s)	BM time (s)
aes	resyn	124/32	252,810	249.57	223.56
	compr	111/28	207,030	208.19	186.17
	rwsat	128/32	284,170	265.65	239.93
ch_ intrinsics (7,560)	resyn	124/32	487,530	957.48	916.33
	compr	111/28	363,760	462.95	428.04
	rwsat	128/32	459,830	567.43	526.43
mkSM-Adapter4B (9,480)	resyn	124/32	644,760	528.13	405.26
	compr	111/28	604,000	499.11	376.83
	rwsat	128/32	695,890	537.98	418.87
mkDelay-Worker32b (12,060)	resyn	124/32	1,082,370	977.62	580.95
	compr	111/28	1,018,050	1020.21	618.07
	rwsat	127/32	1,070,830	963.89	576.46
stereo-vision0 (18,510)	resyn	124/32	1,150,870	3485.93	793.83
	compr	111/28	1,104,550	3670.51	802.80
	rwsat	128/32	1,253,420	3488.30	812.37

Self-modifying AES core





(a) OS+OP. (b) OS+OP+IS. (c) OS+OP+CF+IS. (d) OS+OP+CF+IS+BBN.

OS = operand substitution

OP = opcode permutation

CF = code flattening

BBN = basic block normalization

More difficult to differentiate code with more obfuscation techniques

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

UMASS AMHERST