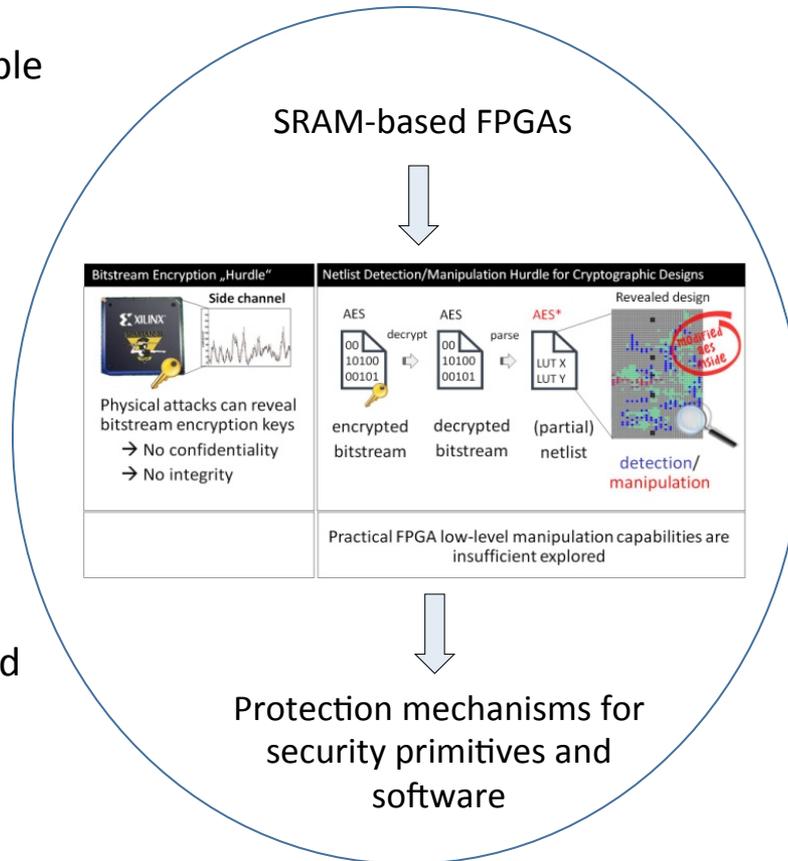# TWC: Small: New Directions in Field Programmable Gate Array (FPGA) Security

Challenge:

- SRAM FPGAs are vulnerable due to bitstream configuration
- Soft microprocessors and crypto functions implemented in FPGAs
- Growing use of FPGAs in embedded systems

Solution:

- Configure crypto cores after FPGA bitstream load
- Use diversification to obscure soft processor instructions

PI: Russell Tessier, Co-I: Christof Paar
Department of Electrical and Computer Engineering
University of Massachusetts Amherst
tessier@umass.edu

SRAM-based FPGAs

Bitstream Encryption „Hurdle"
Side channel
XILINX
Physical attacks can reveal bitstream encryption keys
→ No confidentiality
→ No integrity

Netlist Detection/Manipulation Hurdle for Cryptographic Designs
Revealed design
AES   AES   AES*
00   00
10100   10100
00101   00101
decrypt   parse
LUT X
LUT Y
Modified es inside
encrypted bitstream   decrypted bitstream   (partial) netlist   detection/ manipulation

Practical FPGA low-level manipulation capabilities are insufficient explored

Protection mechanisms for security primitives and software

Scientific Impact:

- Efficient protection of FPGA crypto functions
- Quantifiable soft processor security
- Better protection against FPGA reverse engineering

Broader Impact:

- FPGA designs are more secure
- FPGAs can be used for secure embedded systems
- Students are trained to understand system security