Hardware Redaction via Fine-Grained eFPGA

Prashanth Mohan, Oguz Atli, and Ken Mai (Carnegie Mellon University)

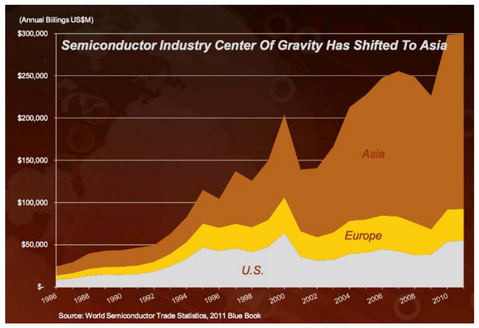
ELECTRONICS RESURGENCE INITIATIVE SUMMIT & MTO Symposium 2020 | Seattle, WA | August 18-20

Obfuscated Manufacturing for GPS (OMG)

Security and Access

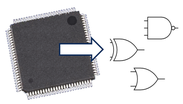
Background

Semiconductor Fab Globalization

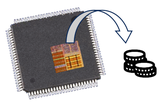


- Only 3 suppliers advancing to 10nm node and beyond
- Intel only US-owned/operated supplier committed to SOTA

Security Threats from Untrusted Fab

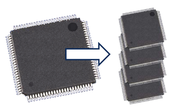


Reverse Engineering



IP Theft

Trojan Insertion



Counterfeiting

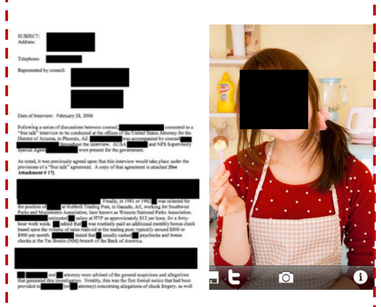
Locking/Obfuscation vs Redaction

Conventional

Locking

Obfuscation

Our Approach



Redaction

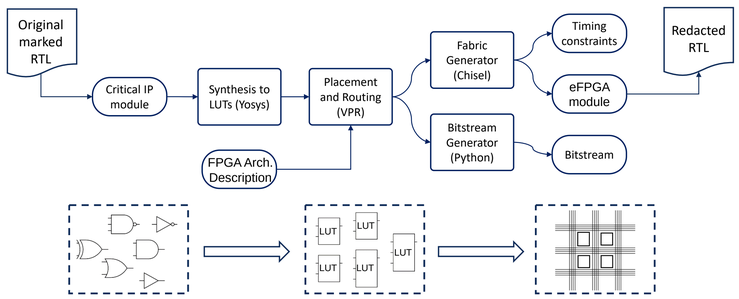
- Redaction enables designer-directed **total removal of critical IP**
- Replace critical IP blocks w/ fine-grained embedded FPGA (eFPGA)

Approach

eFPGA Redaction Insertion Flow

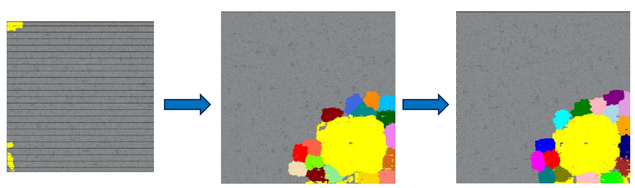
- Open-source soft IP eFPGA design and tool flow
- **Fully standard-cell synthesized eFPGA**, no custom layout
- Most of design unchanged for high performance at power (PaP)

eFPGA Fabric Generation Flow



- eFPGA RTL spawned from Chisel scripts
- Use Yosys, VPR/VTR (Univ. Toronto), and Chisel (UC Berkeley) tools

Redaction of CEP GPS P-Code Generator



Original core ($0.096mm^2$)

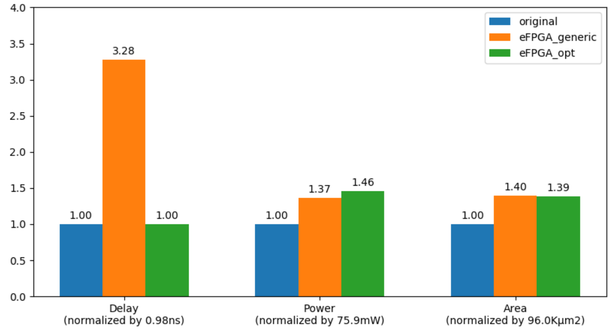
eFPGA_generic ($0.134mm^2$)

eFPGA_opt ($0.133mm^2$)

- Redact length of code, position of LFSR taps, and LFSR init value
- 4x4 tile eFPGA inserted into design
- Yellow = interconnect, Other colors = LUTs
- eFPGA_opt design has design-specific optimized interconnect

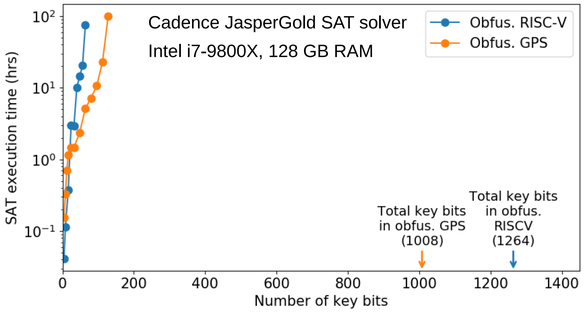
Results and Impact

Redaction VLSI Overheads (P-Code)



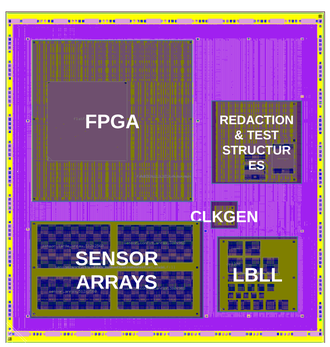
- Interconnect optimized design (green) has negligible delay overhead
- Area and power overhead ~40% versus unsecure design

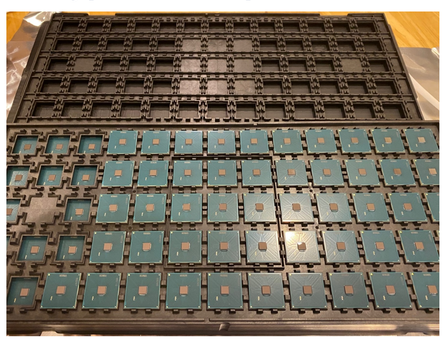
Security Evaluation



- High resistance to SAT and brute-force attack
- Essentially requires attacker to generate eFPGA configuration bitstream without any information about needed functionality

Intel 22FFL Prototype Testchips





- **Implemented redacted P-code and RISC-V on Intel 22FFL process**
- 4mm x 4mm total die size, 120 I/O bumps, 759 power bumps
- **Prototype chips currently undergoing testing**
- In collaboration with Sandia/AFNWC ARCHER project

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.
Distribution Statement A – Approved for Public Release, Distribution Unlimited