Hardware Redaction via Designer-Directed Fine-Grained eFPGA Insertion – Fall 2020

Ken Mai

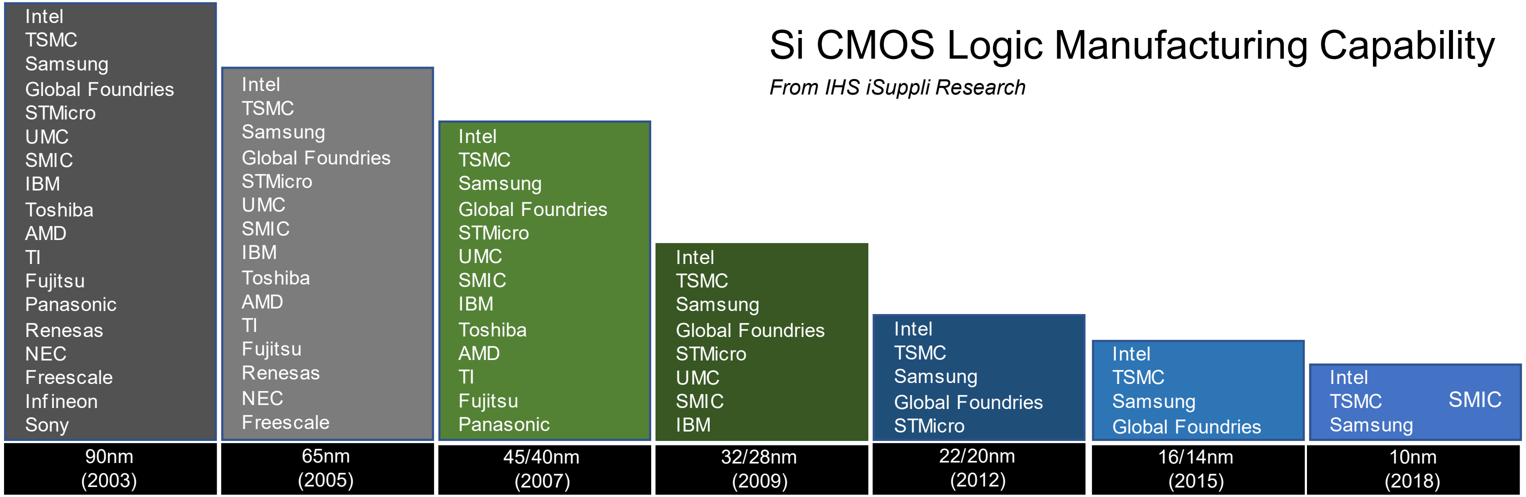
Electrical and Computer Engineering

CyLab Carnegie Mellon University Security and Privacy Institute

Shrinking Number of Leading-Edge IC Fabs

Si CMOS Logic Manufacturing Capability

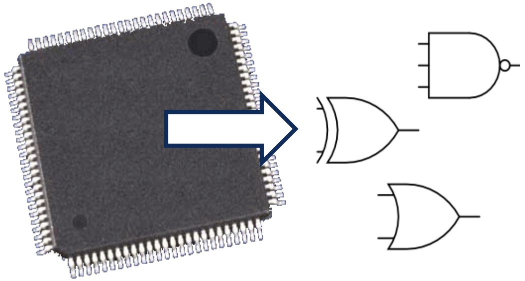
From IHS iSuppli Research



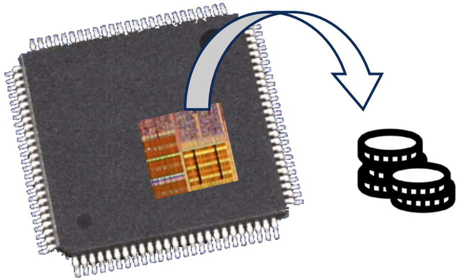
90nm (2003)	65nm (2005)	45/40nm (2007)	32/28nm (2009)	22/20nm (2012)	16/14nm (2015)	10nm (2018)
Intel	Intel	Intel	Intel	Intel	Intel	Intel
TSMC	TSMC	TSMC	TSMC	TSMC	TSMC	TSMC
Samsung	Samsung	Samsung	Samsung	Samsung	Samsung	Samsung
Global Foundries	Global Foundries	Global Foundries	Global Foundries	Global Foundries	Global Foundries	SMIC
STMicro	STMicro	STMicro	STMicro	STMicro		
UMC	UMC	UMC	UMC			
SMIC	SMIC	SMIC	SMIC			
IBM	IBM	IBM	IBM			
Toshiba	Toshiba	Toshiba				
AMD	AMD	AMD				
TI	TI	TI				
Fujitsu	Fujitsu	Fujitsu				
Panasonic	Renesas	Panasonic				
Renesas	NEC					
NEC	Freescale					
Freescale						
Infineon						
Sony						

- Few suppliers are committed to advancing to 10nm node and beyond
- Dominance of fabless semiconductor model → 3rd parties fab

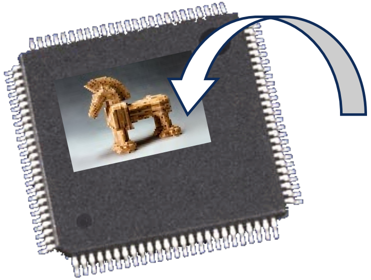
Security Threats from Untrusted Fab



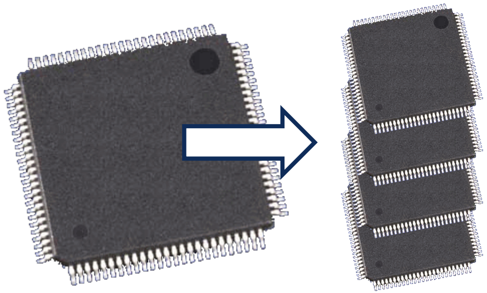
Reverse Engineering



IP Theft



Trojan Insertion



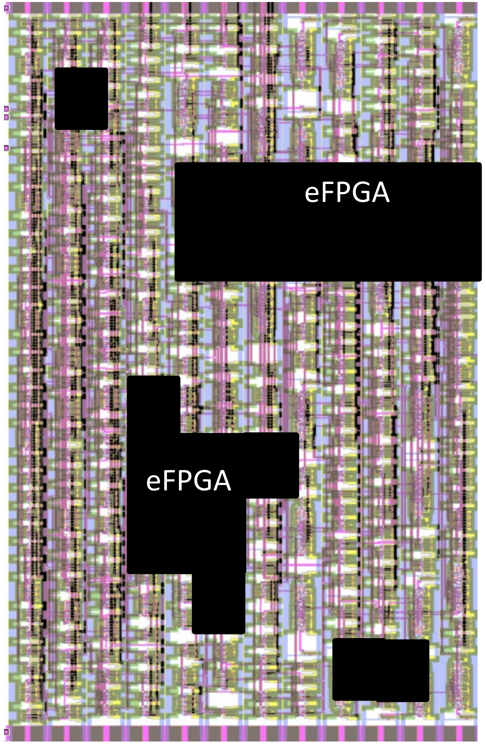
Counterfeiting

Hardware Redaction

Combat untrusted fab and reverse engineering

- Analogous to redaction of paper document before release to untrusted parties

- Designer-directed
- Fine-grained
- Redaction
- Using soft eFPGA

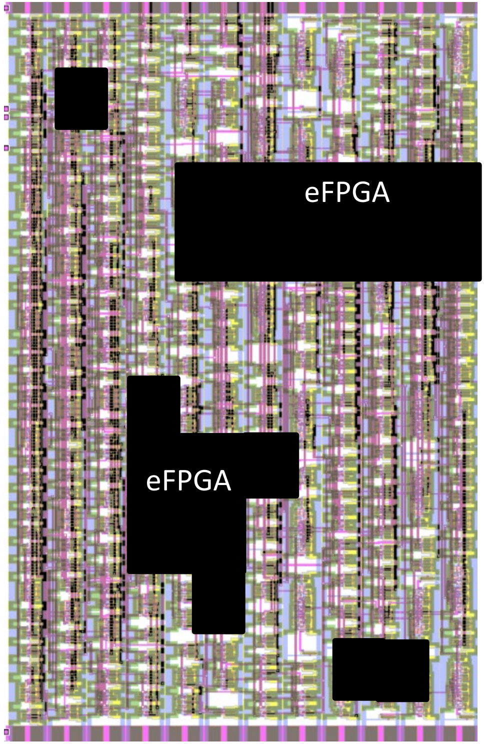


Hardware Redaction

Combat untrusted fab and reverse engineering

- Analogous to redaction of paper document before release to untrusted parties

- **Designer-directed**
    - **Designer knows what IP they want to conceal**
    - **Not reliant on tool to choose what is redacted**
- Fine-grained
- Redaction
- Using soft eFPGA

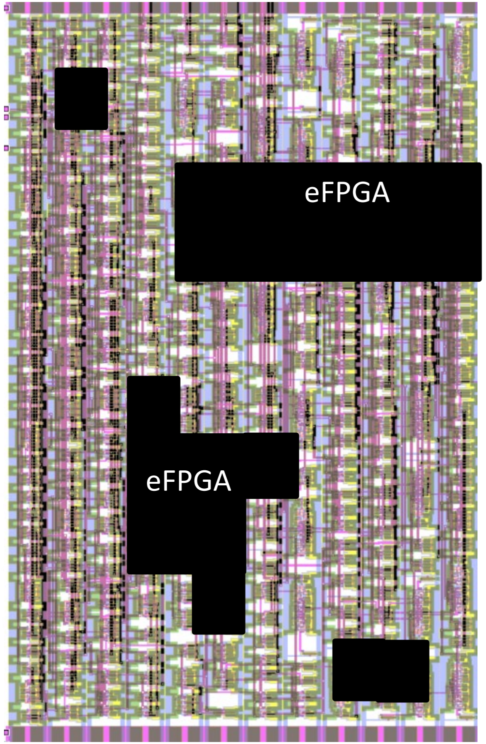


Hardware Redaction

Combat untrusted fab and reverse engineering

- Analogous to redaction of paper document before release to untrusted parties

- Designer-directed
- **Fine-grained**
  - **Can redact from a single gate to a macro block**
  - **Intercalated with rest of design → low overhead**
- Redaction
- Using soft eFPGA

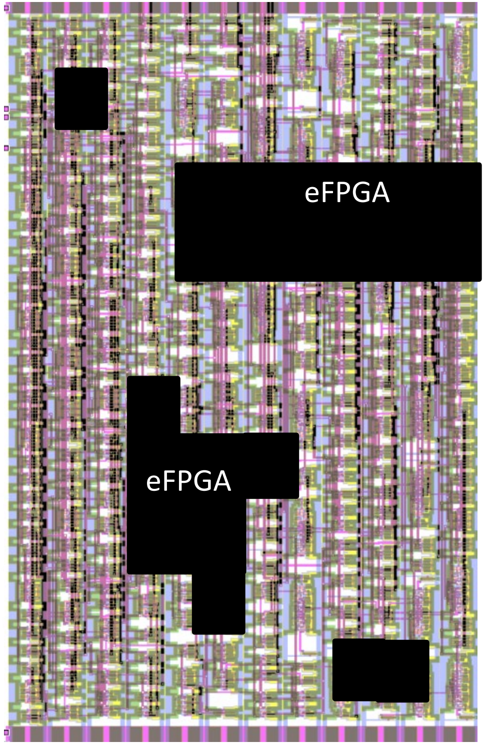


Hardware Redaction

Combat untrusted fab and reverse engineering

- Analogous to redaction of paper document before release to untrusted parties

- Designer-directed
- Fine-grained
- **Redaction**
  - **Complete removal of sensitive IP**
  - **Recast as reconfigurable block**
- Using soft eFPGA

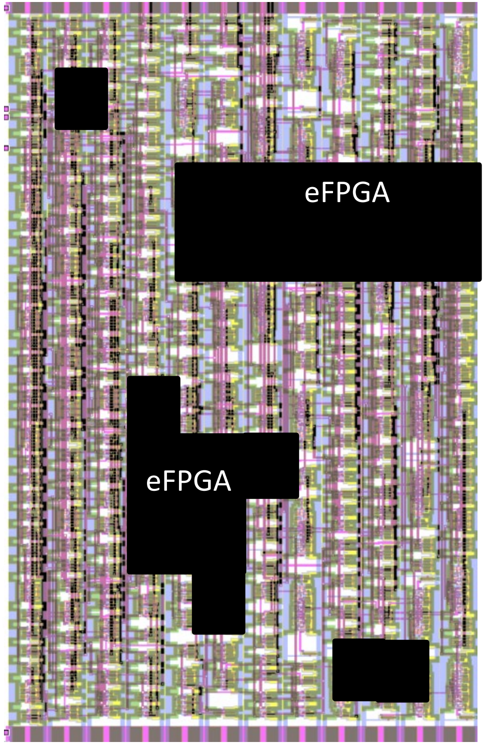


Hardware Redaction

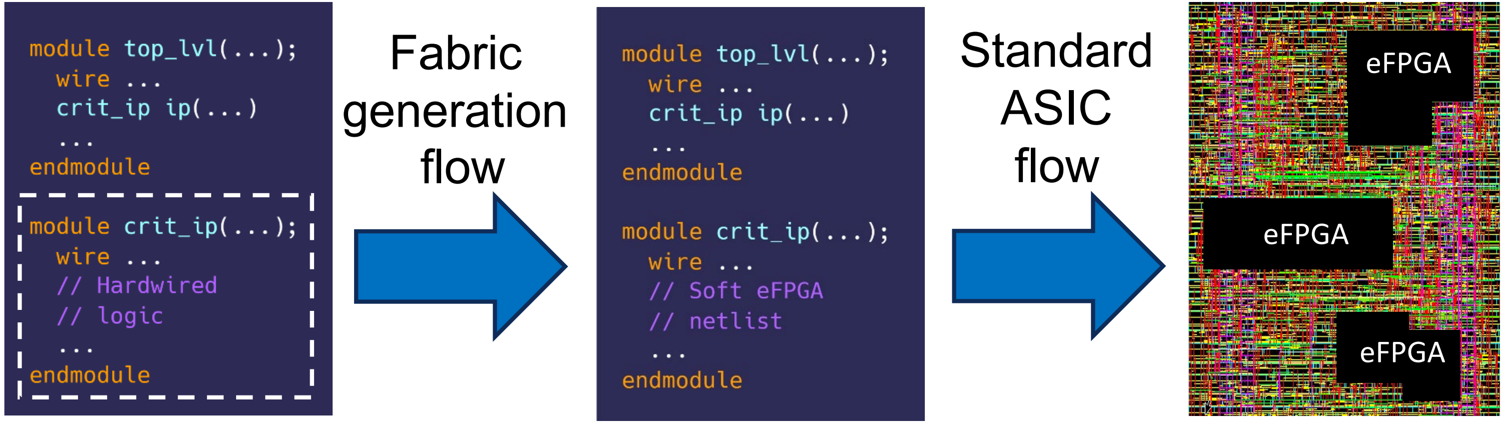
Combat untrusted fab and reverse engineering

- Analogous to redaction of paper document before release to untrusted parties

- Designer-directed
- Fine-grained
- Redaction
- Using soft eFPGA
  - No custom circuits or layout → ease of portability
  - Synthesized using standard cell library along with rest of the design



Designer-view CAD Flow



```
module top_lvl(...);
  wire ...
  crit_ip ip(...)
  ...
endmodule

module crit_ip(...);
  wire ...
  // Hardwired
  // logic
  ...
endmodule
```

Fabric generation flow

```
module top_lvl(...);
  wire ...
  crit_ip ip(...)
  ...
endmodule

module crit_ip(...);
  wire ...
  // Soft eFPGA
  // netlist
  ...
endmodule
```

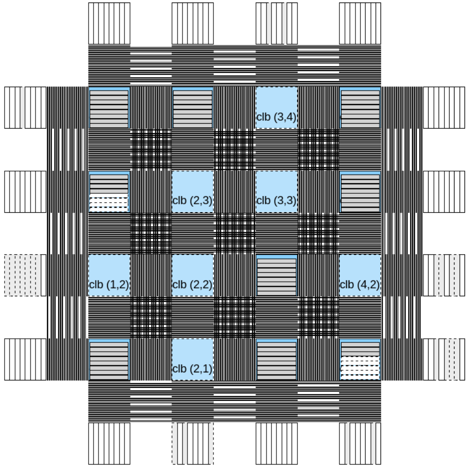
Standard ASIC flow

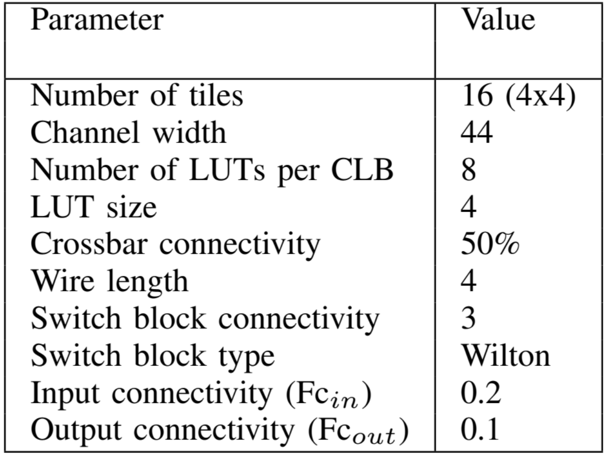
Original marked RTL

Redacted RTL

Layout

4x4 Tile eFPGA Fabric Architecture



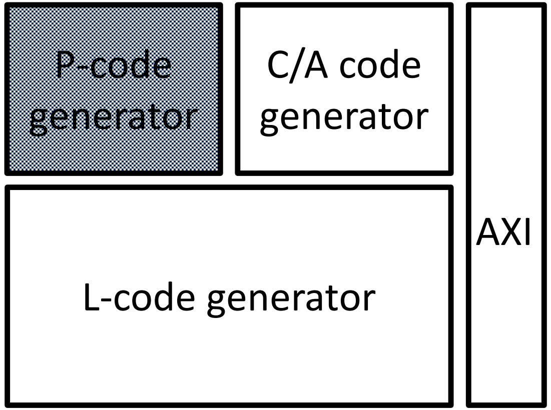


Parameter	Value
Number of tiles	16 (4x4)
Channel width	44
Number of LUTs per CLB	8
LUT size	4
Crossbar connectivity	50%
Wire length	4
Switch block connectivity	3
Switch block type	Wilton
Input connectivity (Fc_{in})	0.2
Output connectivity (Fc_{out})	0.1

- Open-source island-style eFPGA architecture (Univ. Toronto)
- eFPGA RTL spawned from Chisel scripts
- Synthesized using standard cell synthesis tool flow
- eFPGA design silicon proven in 65nm, 28nm, 22nm, and 16nm

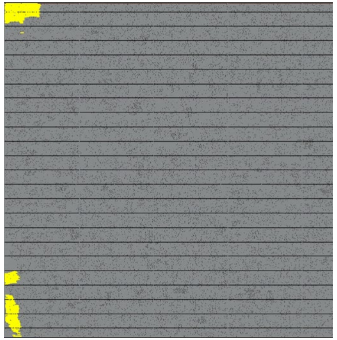
Test Circuit 1: GPS P-Code Generator

- MIT Lincoln Labs Common Evaluation Platform (CEP)
- Generates C/A code, P-code, and L-code
- P-code generator obfuscated
  - Length of the code
  - Position of the LFSR taps
  - Initialization value of the LFSR

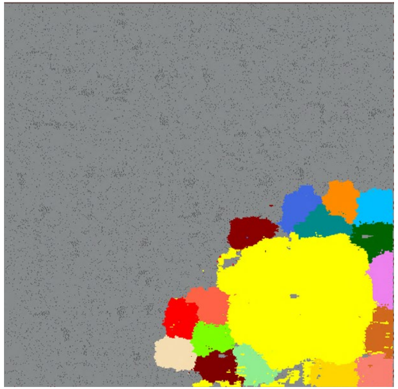


GPS core module diagram

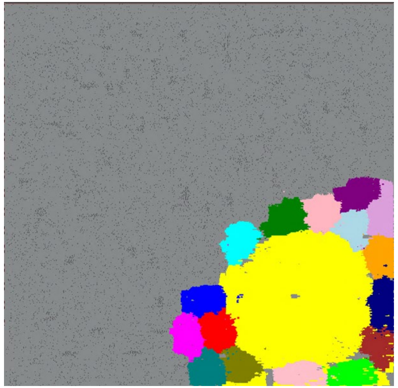
GPS P-Code Generator Layout



Original core (0.096mm^2)

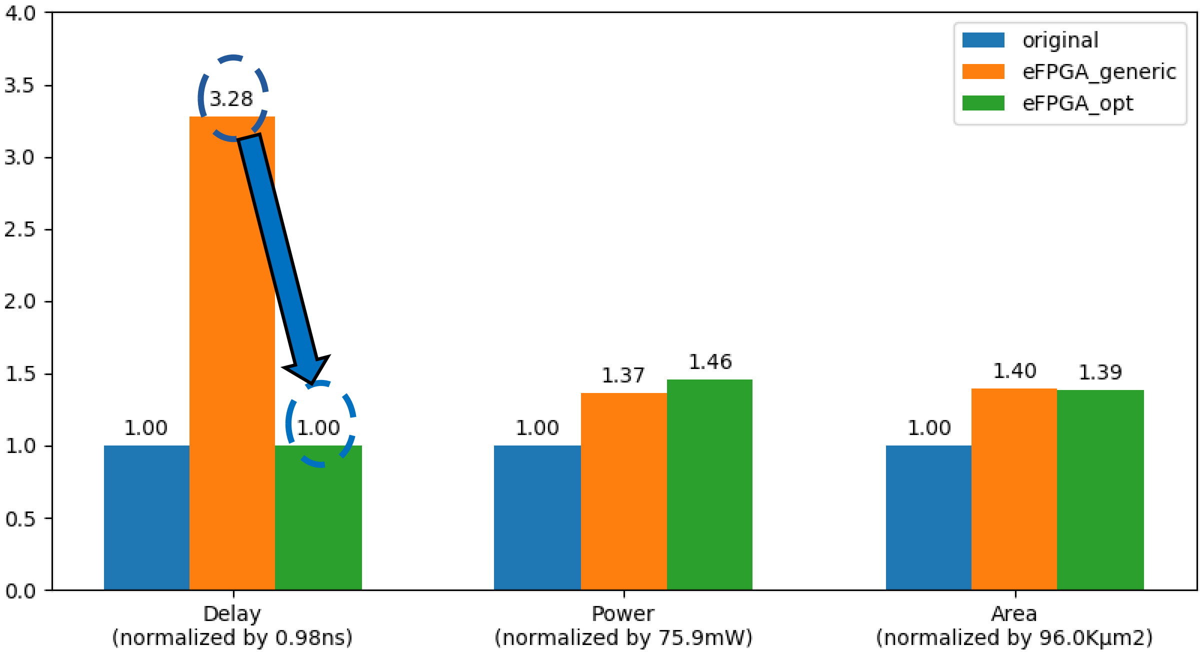


eFPGA_generic (0.134mm^2)



eFPGA_opt (0.133mm^2)

GPS VLSI Metrics



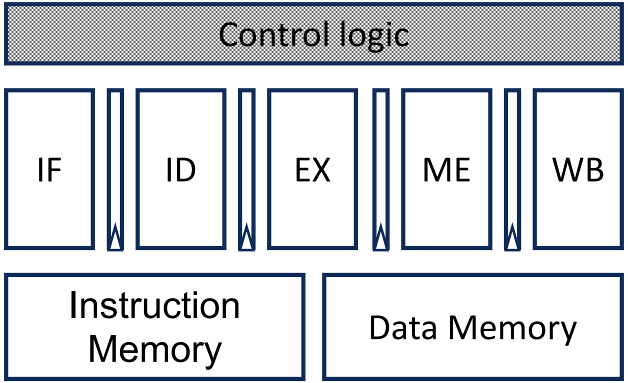
Test Circuit 2: RISC-V CPU

- RV32I architecture

- 5-stage pipelined

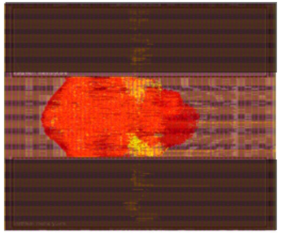
- 16 KB separate I and D memory

- Control logic obfuscated
  - Low percentage of the gates, and renders the entire CPU unusable

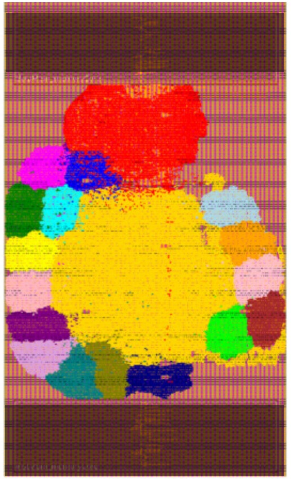


RISC-V CPU module diagram

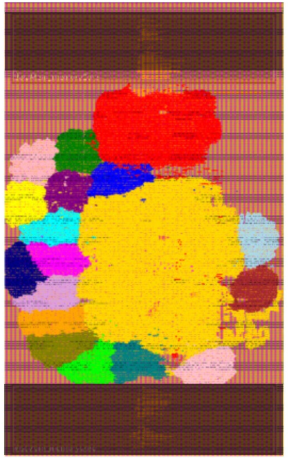
RISC-V Layout



Original core
(4.28K μm^2)

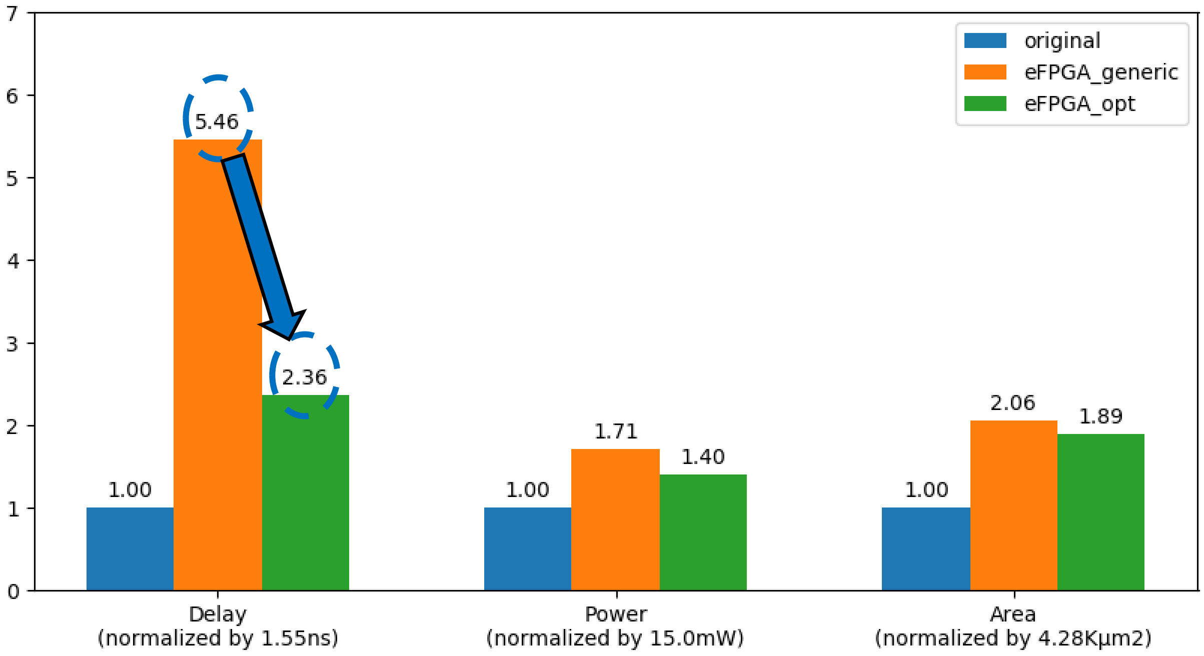


eFPGA_generic
(8.80K μm^2)

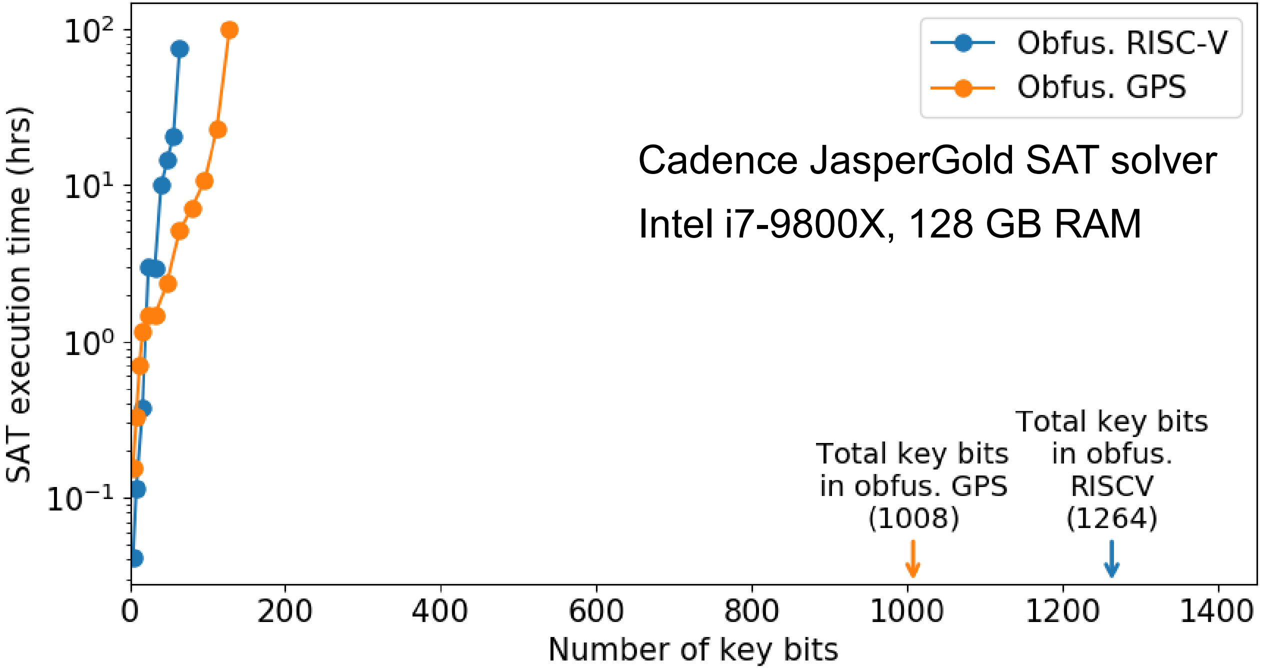


eFPGA_opt
(8.08 μm^2)

RISC-V VLSI Metrics

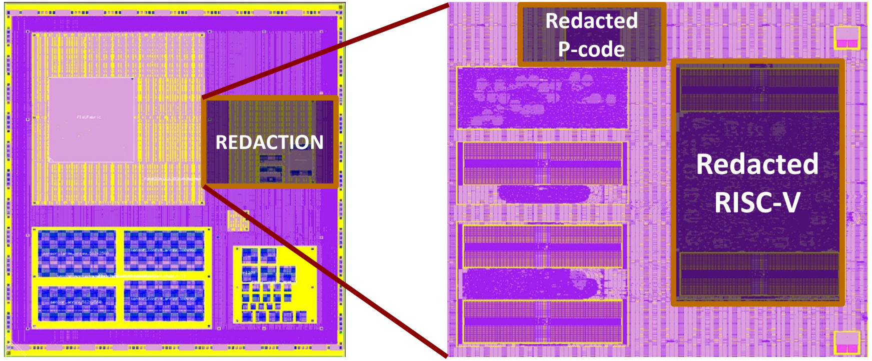


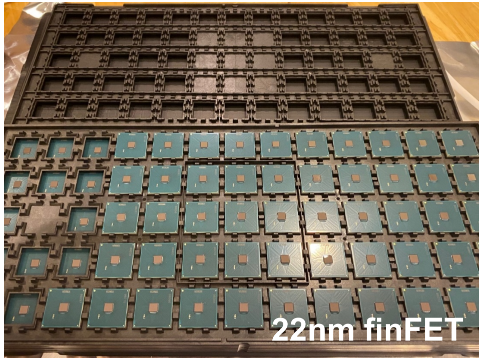
SAT Attack Results



Essentially requires attacker to generate eFPGA configuration bitstream without any information about design structure

Testchips





- Testchips in multiple process technology nodes
  - 28nm planar MOSFET and 22nm finFET technologies
  - Testchips functional at speed
- Soft eFPGA enables fast easy porting between processes
  - eFPGA fabric implemented using standard cells
  - No custom process-specific layout or circuit design

Status and Next Steps

Status

- CAD tool flow from original RTL to redacted RTL completed
- Testchips at multiple process nodes fully functional at speed

Next steps

- Techniques for reducing eFPGA VLSI overheads → latch-based storage
- Enhance eFPGA with block-RAMs and custom macros
- Improve attack infrastructure and conduct longer run-time experiments