Hardware Trojan Attacks in FPGAs

Sebastian Dorn

December 13, 2023

A short view back to the past...

SolarWinds 2020 incident

- Developer of IT Management software
- A major supply-chain attack [1]
    - Compromising more than 18.000 enterprises and governments
- Malicious attackers infiltrated the software build system
- Malware was automatically deployed to customers

Supply chain attacks

- Manufacturing products involves a large supply chain [2]
  - Often involving different companies (outsourcing)
- Different security protocols per chain
- Attackers target less secure elements
  - Inject malware/modifications in the product

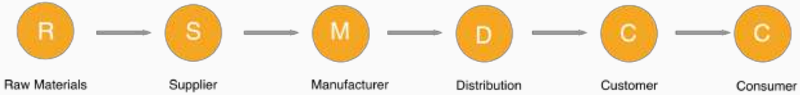


Figure 1: Demonstration of a simple supply chain [2]

How does this relate to FPGAs?

Hardware Trojan Attacks

- Malicious modification of hardware design [3]
  - Internal (infiltrated employee)
  - External (supply chain)
- Have a payload that needs to be triggered
  - Time-based
  - Action-based (remotely, specific pattern, ...)
- Activity differs by Trojan type
  - Leakage of information
  - Denial of Service
  - Escalation of Privilege
  - Fault Attacks

Hardware Trojan Attack: Threat Model

- Threat Model: Untrusted Foundry
  - Modifies the layout before chip
- Only small amount of samples have injected Trojan
  - Achieve better stealthiness

Figure 2: Inside a semiconductor foundry [4]

Dangers of Hardware Trojans

- Real-world attacks already reported
- DoS functionality in fake IC for US missiles
    - Fake Chinese ICs bought by military
    - Contained back-door
    - Could be shutdown remotely
- Information leakage in security chip
    - Actel/Microsemi ProASIC3 A3P250
    - Contained back-door which allowed complete JTAG accesses
    - Researchers found secret key to activate the Trojan

Hardware Trojan Attacks in FPGAs

- FPGAs vulnerable to Hardware Trojan Attacks
- Multiple untrusted components in the product life cycle
  - IP cores
  - Design software
  - Fabrication
- Both hardware and bitstream could contain Trojan

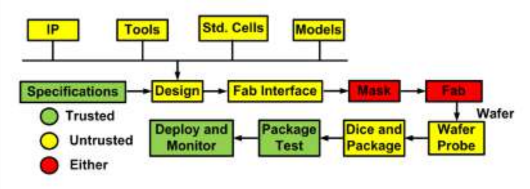


Figure 3: Sample supply chain of a FPGA [5]

Hardware Trojan Attacks in FPGAs: Threat Model

- Additionally to classic Hardware Trojan
- Threat Model: Bitstream manipulation
    - Manipulated Design Software
    - Malicious IP core
    - Manual RTL injection

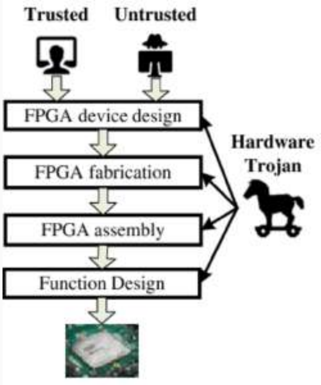


Figure 4: Different stages of FPGA development where Hardware Trojans can be injected [6]

Hardware Trojan Attack in Embedded Memory

Hardware Trojan Attack in Embedded Memory

- Wang et al. 2020 [7]
- Previously: Hardware Trojans in logic parts of ICs
- Design full Trojan in SRAM (trigger, payload, detection avoidance)
- Evades current safeguards for hardware trojans
    - Low footprint
    - Side-channel analysis
    - Behaviour testing

The trigger

The trigger

- Trojan hidden in hardware, only activated if triggered
- Either combinational (logic) or sequential (time)
- Mustn't occur during manufacturer tests
- Solution: Use rare patterns not covered by tests

SRAM test algorithms - March tests

- Designed for high test coverage and low test times
- Runtime of $O(n)$
- March C - (10n): $\updownarrow(\mathrm{w}_0); \uparrow(\mathrm{r}_0, w_1); \uparrow(\mathrm{r}_1, w_0); \downarrow(\mathrm{r}_0, w_1); \downarrow(\mathrm{r}_1, w_0); \updownarrow(\mathrm{r}_0)$
- Not intended to find Hardware Trojans

SRAM test algorithms - Exploitable patterns

- Certain patterns do not occur during March tests
- Can be used as Trojan triggers
- Starting with 4-cell patterns, all March tests are bypassed

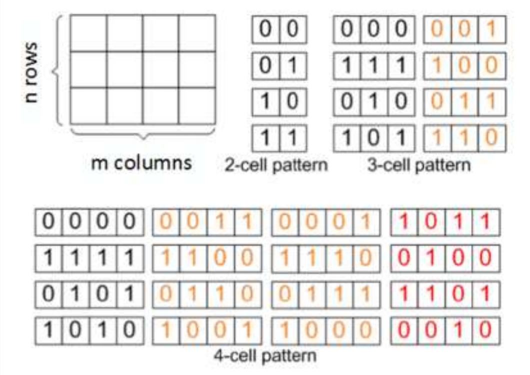


Figure 5: Data patterns that can be leveraged for Trojan trigger [7]

The payload

Resistive Short/Bridge

- nMOS pass transistors concatenated in series
- Connected to nodes for trigger condition
- With Trojan inactive, v-cell has high resistance and no change in functionality
- Bridge can be implemented in similar manner

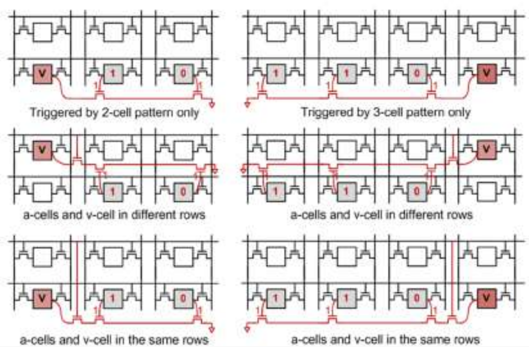

V
1
0
Triggered by 2-cell pattern only
Triggered by 3-cell pattern only
a-cells and v-cell in different rows
a-cells and v-cell in different rows
a-cells and v-cell in the same rows
a-cells and v-cell in the same rows

Figure 6: Trojans triggering short to V_{ss} [7]

Resistive Short: Visualisation

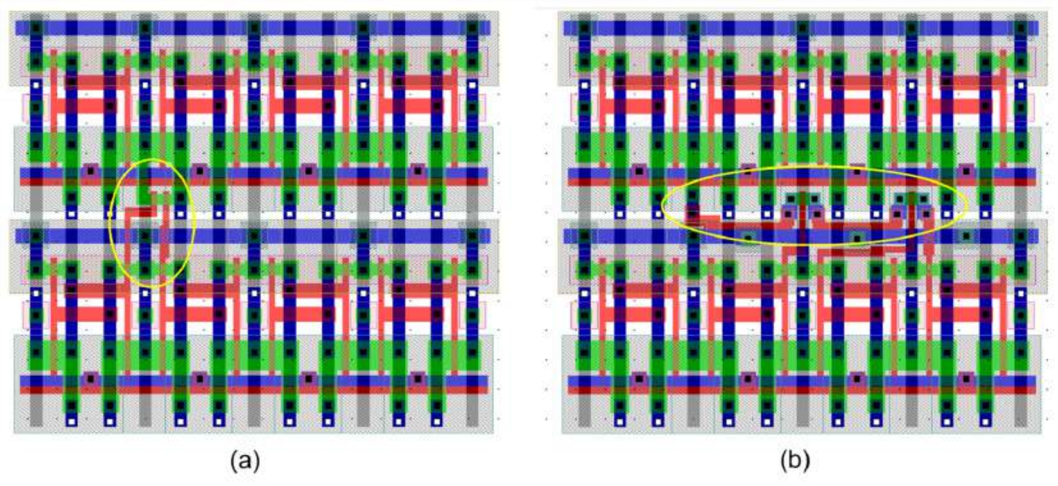
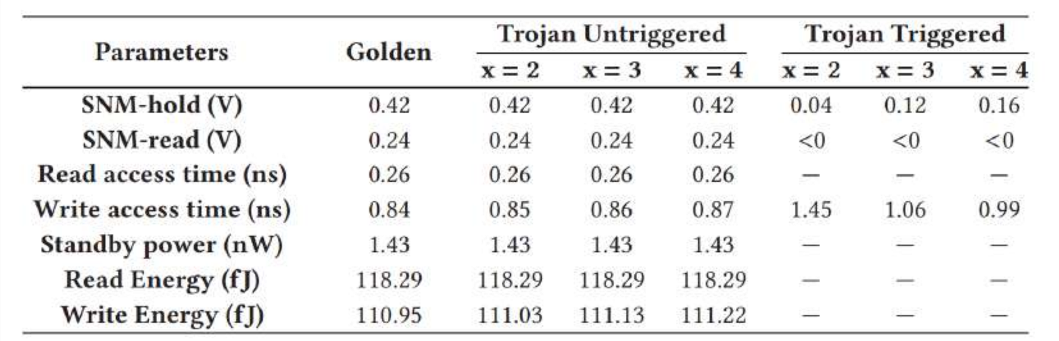


Figure 7: Layout of Trojans causing short defects [7]

Resistive Short: Evaluation



Parameters	Golden	Trojan Untriggered			Trojan Triggered		
		x = 2	x = 3	x = 4	x = 2	x = 3	x = 4
SNM-hold (V)	0.42	0.42	0.42	0.42	0.04	0.12	0.16
SNM-read (V)	0.24	0.24	0.24	0.24	<0	<0	<0
Read access time (ns)	0.26	0.26	0.26	0.26	—	—	—
Write access time (ns)	0.84	0.85	0.86	0.87	1.45	1.06	0.99
Standby power (nW)	1.43	1.43	1.43	1.43	—	—	—
Read Energy (fJ)	118.29	118.29	118.29	118.29	—	—	—
Write Energy (fJ)	110.95	111.03	111.13	111.22	—	—	—

Figure 8: Impact of a resistive short trojan in a 32 × 64 SRAM Array [7]

Resistive Open

- Needs additional circuitry in target path, difficult in SRAM array
- Simplest needs one nMOS, multiple could be needed
- Potentially detectable by March tests

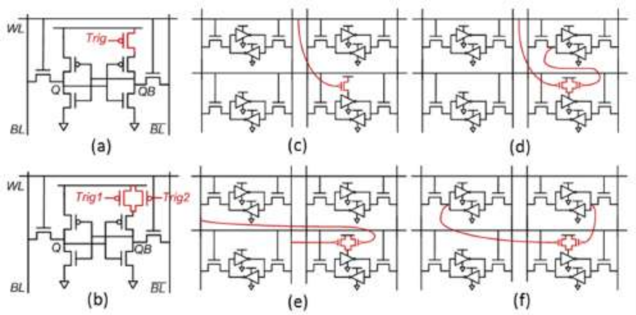


Figure 9: Trojans triggering open defect [7]

Resistive Open: Visualisation

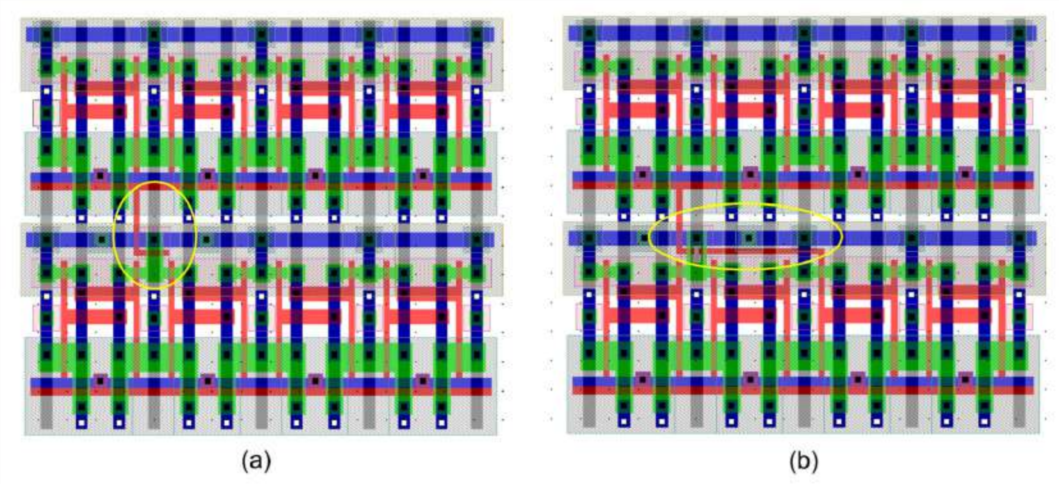
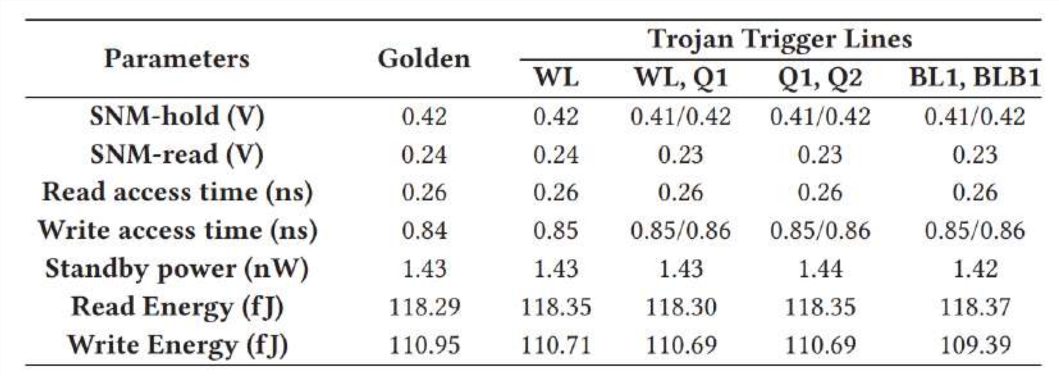


Figure 10: Layout of Trojans causing open defects [7]

Resistive Open: Evaluation



Parameters	Golden	Trojan Trigger Lines			
		WL	WL, Q1	Q1, Q2	BL1, BLB1
SNM-hold (V)	0.42	0.42	0.41/0.42	0.41/0.42	0.41/0.42
SNM-read (V)	0.24	0.24	0.23	0.23	0.23
Read access time (ns)	0.26	0.26	0.26	0.26	0.26
Write access time (ns)	0.84	0.85	0.85/0.86	0.85/0.86	0.85/0.86
Standby power (nW)	1.43	1.43	1.43	1.44	1.42
Read Energy (fJ)	118.29	118.35	118.30	118.35	118.37
Write Energy (fJ)	110.95	110.71	110.69	110.69	109.39

Figure 11: Impact of a resistive open trojan in a 32 × 64 SRAM Array [7]

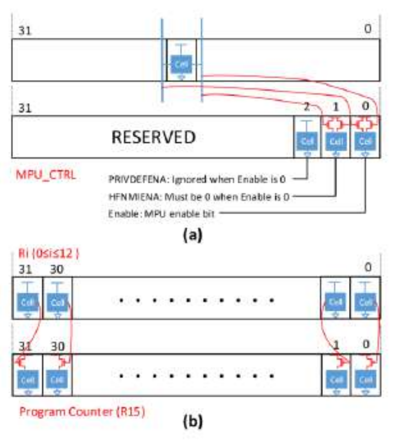
The complete system attack

System attacks with SRAM

- Shown Trojans can be used for data corruption or denial of service
- Hardware Trojans allow for more sophisticated attacks
- Threat Model: Two adversaries
    - One in foundry or bitstream design inserting the Trojan
    - One working with the deployed hardware
    - Can be the same person

Privilege Escalation with SRAM Trojan

- No need for software vulnerabilities, using fault attacks
- Memory Protection Unit (MPU)
    - Attack with power glitches to disable MPU
    - Allows unrestricted memory access for unprivileged software
- Program Counter (PC)
    - Power glitch during privileged syscall of unprivileged software
    - PC changed to malicious location with privileged access



(a)

(b)

Figure 12: Privilege Escalation using the MPU (a) or PC (b) [7]

Trojan Attack on AES

- AES depends on s-box that is resistant to cryptanalysis
- Simple FPGA Hardware Trojan: Modify bitstream, set s-box to 0
- Hardware Trojan: Trojan in L2 cache
    - Trojan trigger nodes sense for s-box content in cache
    - Once triggered, s-box content is changed

Countermeasures

Current Countermeasures

- Many countermeasures invalidated against SRAM Hardware Trojans [6]
    - Side-channel analysis
    - SRAM testing algorithms
- FPGAs additional security measurements rendered useless
    - Bitstream Encryption
    - Error Correcting Codes (ECC)
    - Adress Space Layout Randomization (ASLR)

Proposed Countermeasures

- Reverse Engineering of final product
  - Both of bitstream and hardware
  - Time-intensive
  - Needs to be done for multiple boards
- Optical imaging-based techniques
  - Currently only done in post-deployment failures
  - Needs to be also done in post-manufacturing tests

Figure 13: Image-based analysis of FPGA [6]

References

[1] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, **Solar winds hack: In-depth analysis and countermeasures,** in 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2021, pp. 1–7.

[2] Wikipedia contributors, **Supply chain — Wikipedia, the free encyclopedia,** [Online; accessed 11-December-2023], 2023. [Online]. Available: `https://en.wikipedia.org/w/index.php?title=Supply_chain&oldid=1184111370`.

[3] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, **Hardware trojan attacks: Threat analysis and countermeasures,** Proceedings of the IEEE, vol. 102, no. 8, pp. 1229–1247, 2014.

References ii

[4] REUTERS, **Inside a samsung foundry,** [Online]. Available: `https://media0.faz.net/ppmedia/aktuell/3154841552/1.8371398/width610x580/chipfabrik-von-samsung-in.jpg`.

[5] M. Beaumont, B. Hopkins, and T. Newby, **Hardware trojans-prevention, detection, countermeasures (a literature review),**, 2011.

[6] S. Mal-Sarkar, A. Krishna, A. Ghosh, and S. Bhunia, **Hardware trojan attacks in fpga devices: Threat analysis and effective counter measures,** in Proceedings of the 24th Edition of the Great Lakes Symposium on VLSI, 2014, pp. 287–292.

[7] X. Wang, T. Hoque, A. Basak, *et al.*, **Hardware trojan attack in embedded memory,** ACM Journal on Emerging Technologies in Computing Systems (JETC), vol. 17, no. 1, pp. 1–28, 2021.