HT and Trusted IC -- Trusted IC Design with HT Prevention

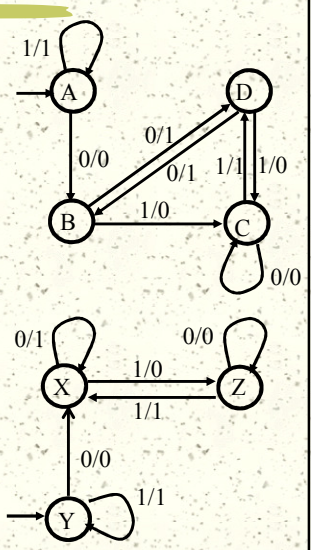
Cybersecurity Specialization
-- Hardware Security

HT Prevention: Pre-Synthesis

- Ensure IPs are trusted before use them
- Formal verification
  - Property/model/equivalence checking
  - f(x)=g(x) iff f(x)g'(x) + f'(x)g(x) = 0
    - Use SAT (Boolean satisfiability) solver to verify f(x)g'(x) + f'(x)g(x) is unsatisfiable (constant 0).
  - FSM equivalency: product machine
- Test and validation
  - Testing methods
  - HT detection approaches

FSM Equivalence

- Two FSMs are equivalent iff they produce the same output on any input sequence.
- Example
  - M1: {A,B,C,D} start with state A
  - M2: {X,Y,Z} start with state Y
  - On input 0: (0,0); 1: (1, 1)
  - On input 00: (01,01); 01 (00,00); 10: (10, 10); 11(11, 11)
  - On input 000: (011, 011); …

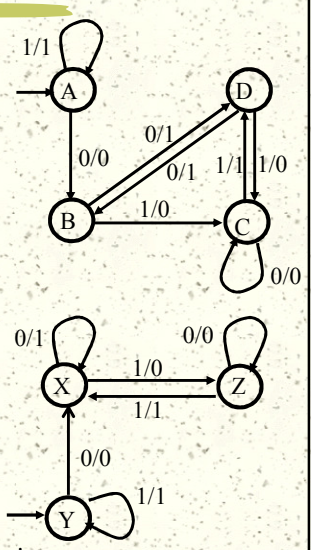


Product Machine

- M1: {A,B,C,D} start with state A
- M2: {X,Y,Z} start with state Y
- The product machine
  - (A,Y) On input 1: → (A,Y), output 1
    On input 0: → (B,X), output 0
  - (B,X) On input 1: → (C,Z), output 0
    On input 0: → (D,X), output 1
  - (C,Z) On input 1: → (D,X), output 1
    On input 0: → (C,Z), output 0
  - (D,X) On input 1: → (C,Z), output 0
    On input 0: → (B,X), output 1

When there is no new state produced, M1 and M2 are equivalent, stop.

If M1 and M2 give different outputs, not equivalent, stop.

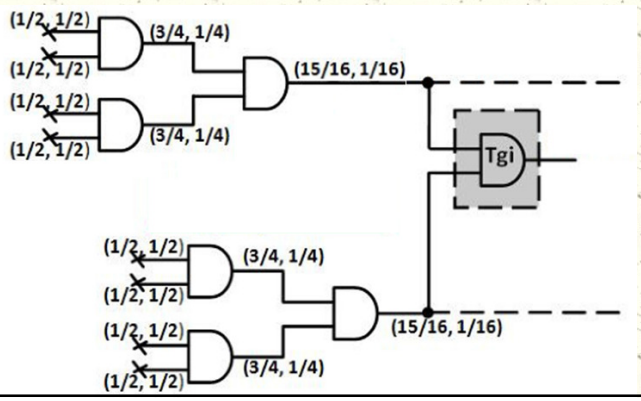


HT Prevention: Post-Synthesis

- Removal of dead spaces
  - Prevent direct HT insertion, limit big HTs
- Circuit obfuscation
  - Make reverse engineering harder
- Shielding wires
  - Prevent EM radiation
- Interface protection: I/O pins, internal module interface, power/clock, scan chain
  - Control HT triggers

HT Prevention: Rare Event Removal

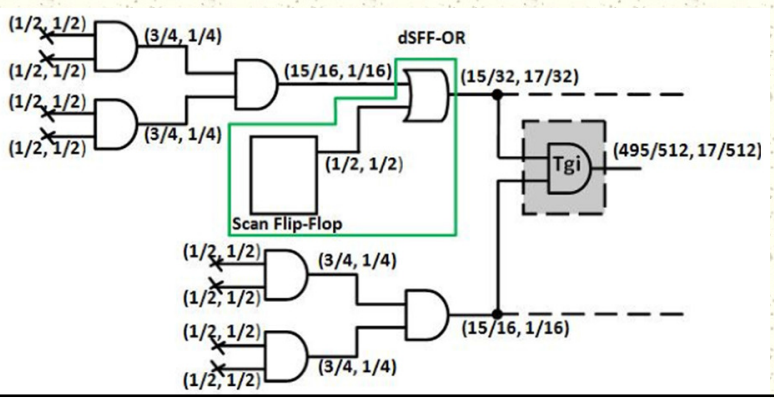
- HTs use rare events as triggers, if we remove rare events, it will be easier to detect/activate HTs



H. Salmani, M. Tehranipoor, J. Plusquellic, New design strategy for improving hardware Trojan detection and reducing Trojan activation time, HOST 2009.

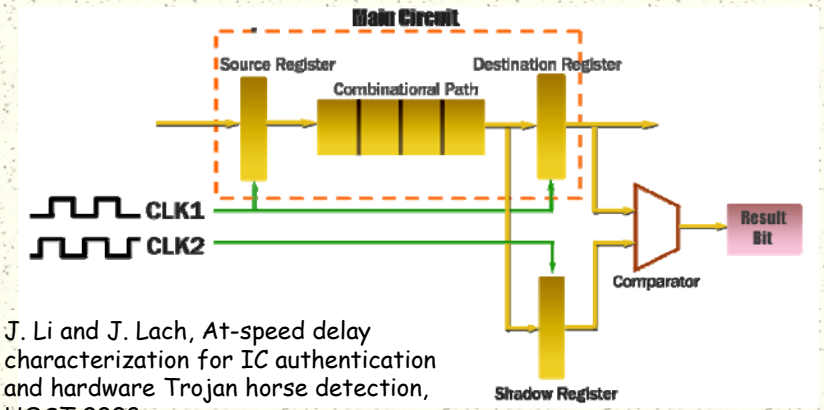
HT Prevention: Rare Event Removal

- HTs use rare events as triggers, if we remove rare events, it will be easier to detect/activate HTs



HT Prevention: Shadow Register

- Path delay based HT detection fails if we cannot measure the internal path delay



J. Li and J. Lach, At-speed delay characterization for IC authentication and hardware Trojan horse detection, HOST 2008.

HT Prevention: Other Methods

- M. Banga and M. Hsiao, VITAMIN: voltage inversion technique to ascertain malicious insertion in ICs, HOST 2009.
- J. Gu, G. Qu, and Q. Zhou, Information hiding for trusted system design, DAC 2009.
- R.S. Chakraborty and S. Bhunia, Security against hardware Trojan through a novel application of design obfuscation, ICCAD 2009.
- M. Potkonjak, Synthesis of trustable ICs using untrusted CAD tools, DAC 2010.
- E. Love, Y. Jin, and Y. Makris, Enhancing security via provably trustworthy hardware intellectual property, HOST 2011.
- C. Dunbar and G. Qu, Designing trusted embedded systems from Finite State Machines, TECS 2014.