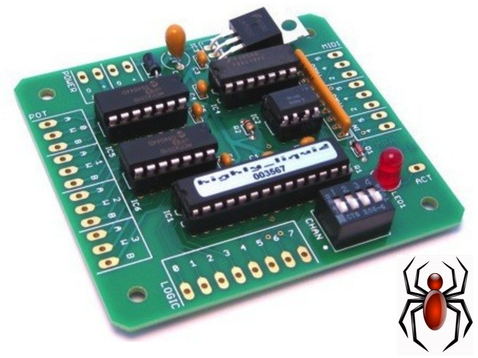
Hardware Trojan Detection using SAT

By: David Kebo Houngninou, Advisor: Dr. Mitch Thornton
Computer Science and Engineering Department, Bobby B. Lyle School of Engineering
Southern Methodist University, P.O. Box 750122, Dallas, TX 75275-0122

WHAT IS A HARDWARE TROJAN ?



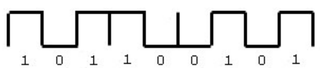
A hardware Trojan is a malicious circuitry that creates a security breach in a system.

The breach can result in unpredicted behavior of the circuit, leak of information, or create a back door for an intruder.

SIMULATION vs. FORMAL VERIFICATION

Simulation

stimulates the design inputs and checks the outputs against expected values.



Formal verification

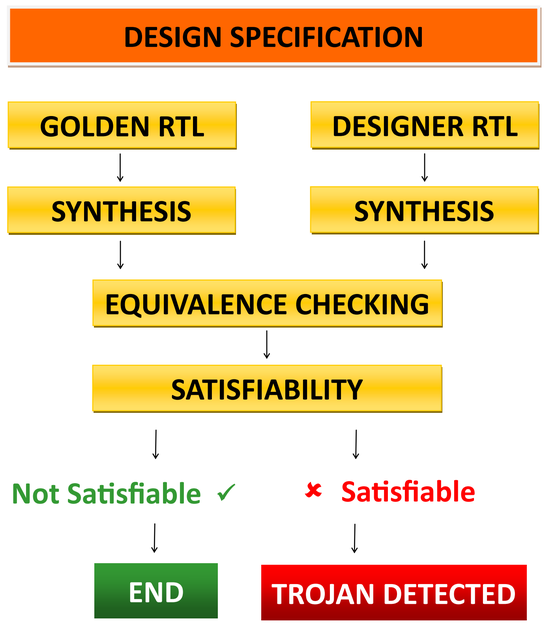
formally proves that two designs have identical behavior.

WHAT IS SAT ?

Satisfiable Assignment

X1: 0
X2: 0
X3: 1
X4: 0
X5: 1
X6: 1
X7: 1

Given a Boolean function **f(x1 , x2 … , xn)** **Satisfiability (SAT)** is a property that determines a variable assignment such that function f evaluates to **1**.



ILLUSTRATION

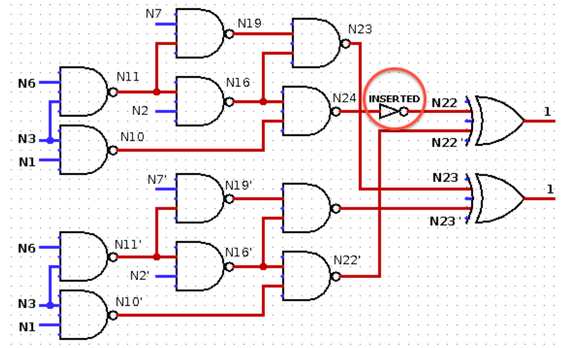
Are these two circuits identical ?

1. Original

nand G1 (N10, N1, N3);
nand G2 (N11, N3, N6);
nand G3 (N16, N2, N11);
nand G4 (N19, N11, N7);
nand G5 (N24, N10, N16);
nand G7 (N23, N16, N19);

2. Modified

nand G1 (N10, N1, N3);
nand G2 (N11, N3, N6);
nand G3 (N16, N2, N11);
nand G4 (N19, N11, N7);
nand G5 (N24, N10, N16);
not G6 (N22, N24);
nand G7 (N23, N16, N19);



RESULT

Circuit 1 and 2 have the same # of inputs? Yes ✓

Circuit 1 and 2 have the same # of outputs? Yes ✓

Is circuit 1 equivalent to circuit 2? No ✘

How? The SAT checker proves this by returning a satisfiable assignment

Why? One of the outputs is inverted

BDD vs. SAT

SAT compared to another equivalence checker method, the **Binary Decision Diagram (BDD)**

Performance comparison

Testbench circuits		BDD	SAT
C17	C17	0ms	0ms
C432	C432nr	0ms	0ms
C499	C499nr	10ms	0ms
C880	C880	64ms	5ms
C1355	C1355nr	50ms	8ms
C1908	C1908nr	90ms	22ms

SAT is:

- Memory efficient
- Faster than the BDD method

APPLICATIONS

Where can we use this ?

Military (Counterfeit parts detection)

Real time systems

Encryption / Decryption circuits

Telecom routers (Decoders)