**WHAT IS SAT?**

A hardware Trojan is a malicious circuitry that creates a security breach in a system. The breach can result in unpredictable behavior of the circuit, leak of information, or create a back door for an intruder.

**Satisfiable Assignment**

Given a Boolean function \( f(x_1, x_2, ..., x_n) \), 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
   - \( \text{nand G1 (N10, N1, N3)} \)
   - \( \text{nand G2 (N11, N3, N6)} \)
   - \( \text{nand G3 (N16, N2, N11)} \)
   - \( \text{nand G4 (N19, N11, N7)} \)
   - \( \text{nand G5 (N24, N10, N16)} \)
   - \( \text{not G6 (N22, N24)} \)
   - \( \text{nand G7 (N23, N16, N19)} \)

2. Modified
   - \( \text{nand G1 (N10, N1, N3)} \)
   - \( \text{nand G2 (N11, N3, N6)} \)
   - \( \text{nand G3 (N16, N2, N11)} \)
   - \( \text{nand G4 (N19, N11, N7)} \)
   - \( \text{nand G5 (N24, N10, N16)} \)
   - \( \text{not G6 (N22, N24)} \)
   - \( \text{nand G7 (N23, N16, N19)} \)

**DESIGN SPECIFICATION**

**GOLDEN RTL**

\[ \text{SYNTHESIS} \]

**DESIGNER RTL**

\[ \text{SYNTHESIS} \]

**EQUIVALENCE CHECKING**

**SATISFIABILITY**

Not Satisfiable \( \checkmark \) \hspace{1cm} Satisfiable \( \times \)

**RESULT**

Circuit 1 and 2 have the same # of inputs? Yes \( \checkmark \)

Circuit 1 and 2 have the same # of outputs? Yes \( \checkmark \)

Is circuit 1 equivalent to circuit 2? No \( \times \)

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

Why? One of the outputs is inverted

**APPLICATIONS**

Military (Counterfeit parts detection)

Real time systems

Encryption / Decryption circuits

Telecom routers (Decoders)