Thwarting Scan-Based Attacks on Secure-ICs With On-Chip Comparison

Abstract
Hardware implementation of cryptographic algorithms is subject to various attacks. It has been previously demonstrated that scan chains introduced for hardware testability open a back door to potential attacks. Here, we propose a scan-protection scheme that provides testing facilities both at production time and over the course of the circuit’s life. The underlying principles to scan-in both input vectors and expected responses and to compare expected and actual responses within the circuit. Compared to regular scan tests, this technique has no impact on the quality of the test or the model-based fault diagnosis. It entails negligible area overhead and avoids the use of an authentication test mechanism.
RTL schematic
Technology schematic

Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Design Summary

Design Properties
- Enable Message Filtering
- Optional Design Summary Contexts
  - Show Clock Report
  - Show Timing Constraints
  - Show Warnings
  - Show Errors

Device Utilization Summary (estimated values)

- Logic Utilization
  - Used
  - Available
  - Utilization
  - Number of Sites
  - Number of Site Flip Flops
  - Number of Inverters
  - Number of bonded IOs
  - Number of GCLs

Detailed Reports

- Report Name
- Status
- Generated
- Errors
- Warnings
- Info
  - Synthesis Report
  - Translation Report
  - Place and Route Report
  - Power Report
  - Post-Place Static Timing Report
  - Utilization Report

Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Simulation output
Further Details Contact: A Vinay, Ph- 9030333433, 08772261612

Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com
Further Details Contact: A Vinay, Ph- 9030333433, 08772261612
Email: takeoffstudentprojects@gmail.com | www.takeoffprojects.com