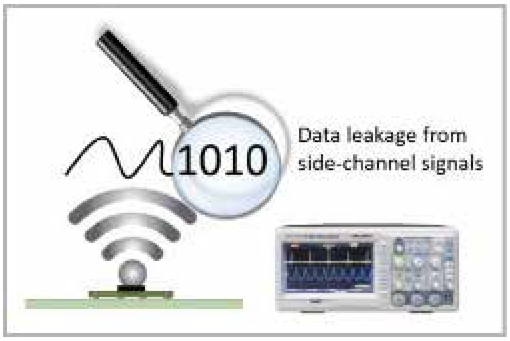
DATASHEET

Synopsys RedHawk-SC Security

IC Design Software Solution for Hardware Security and Data Integrity Analysis

Overview

Data security and privacy are essential concerns for mission critical components and modern cryptography is heavily used in automotive, financial, 5G, and IoT devices to assure information security and data integrity. Unfortunately, security can be compromised by exploiting hardware vulnerabilities in the physical implementation of integrated circuits (ICs, or chips) implementing encryption safeguards. Synopsys RedHawk-SC Security™ is a unique multiphysics simulation platform for RTL designers, physical implementation designers, and system integration engineers to verify data integrity issues in ICs. It enables a silicon design team with minimal hardware security background to assess side-channel leakage and fault injection vulnerabilities. This is much faster and cheaper than post-silicon lab analysis and avoids expensive silicon respins.



Product Highlights

Synopsys RedHawk-SC Security features fast and comprehensive pre-silicon side-channel trace generation and built-in hardware security analytics for data integrity assessment. Utilizing the RTL or gate netlist of a design, cycle-accurate power traces can be generated rapidly, enabling the assessment of early-stage power side-channel vulnerabilities and the verification of various design countermeasures. Once the physical design implementation is available, on-chip power-noise traces from power grids and off-chip electromagnetic emission traces can be simulated to pinpoint spatial and temporal side-channel leakage for chip security sign-off. RedHawk-SC Security enables shift-left security validation, leveraging the advantages of the Synopsys SeaScape™ EDA platform, the world's first cloud-native, elastic-compute architecture for electronic system design and simulation. SeaScape provides per-core scalability, flexible design data access, MapReduce-enabled analytics, and many other revolutionary capabilities.

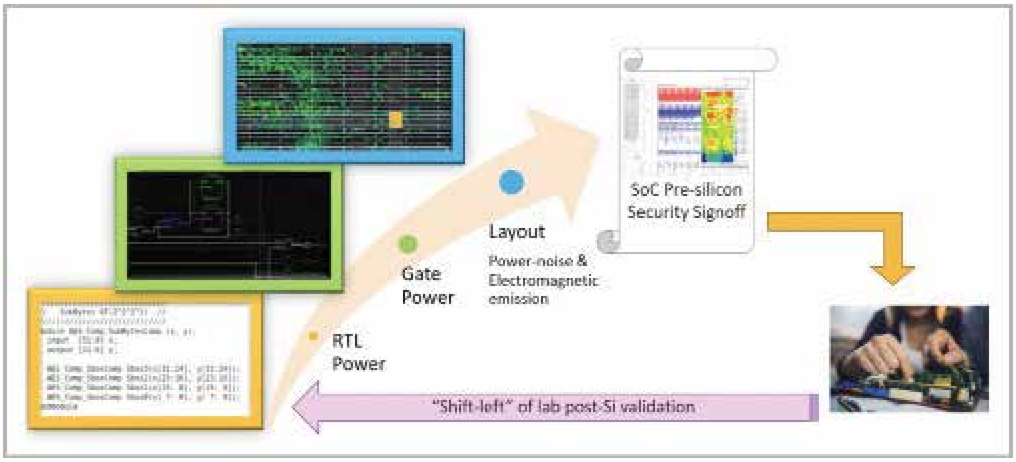
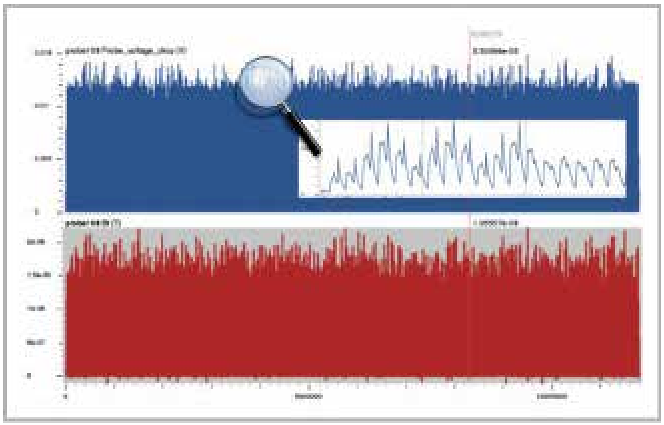


Figure 1: RedHawk-SC Security analysis flow to ensure hardware security at every stage of chip design

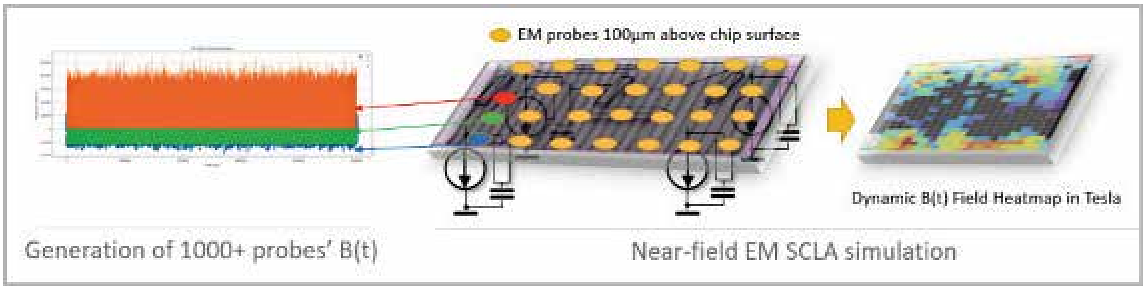
Long-Vector Trace Simulation

Pre-silicon side-channel leakage analysis (SCLA) requires statistical data analysis of a myriad of functional workloads to evaluate data integrity. The trace generation and side-channel analytics are exceptionally fast in RedHawk-SC Security. This is made possible by links to Synopsys ZeBu® hardware emulator for real-world activity data and by the innovative SeaScape architecture with parallel computing and time-slicing techniques. The novel cycle selection methodology in RedHawk-SC Security, allows the generation of billion-cycle vectors driving side-channel trace simulation and conducting security analytics within a single day. Trace re-generation, debugging, and 'what-if' analysis can be performed efficiently with noise-free functional vectors and controllable vectorless noise, avoiding the tedious post-silicon lab validation spanning days and weeks.



Near-Field Electromagnetic Side-Channel Analysis

RedHawk-SC security enables layout-level near-field electromagnetic (EMag) simulation to pinpoint side-channel leakage beyond the on-chip side-channel leakage. Given the transient current flowing in the on-chip power distribution network (PDN), a fast quasistatic electromagnetic solver is employed to simulate the 3D transient EMag traces. The EMag field heatmap can be generated using thousands of user-given virtual probe locations which provides a comprehensive coverage of EMag side-channel emission distribution. This highlights the root cause of data integrity issues and provides guides for scanning the POI (point-of-interest) in silicon laboratory tests for hardware security.

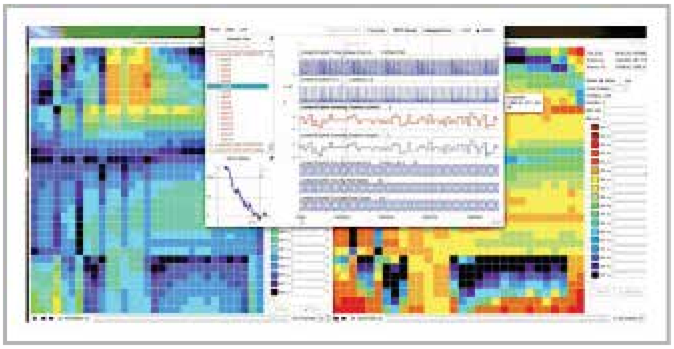

EM probes 100µm above chip surface
Dynamic B(t) Field Heatmap in Tesla

Generation of 1000+ probes' B(t)

Near-field EM SCLA simulation

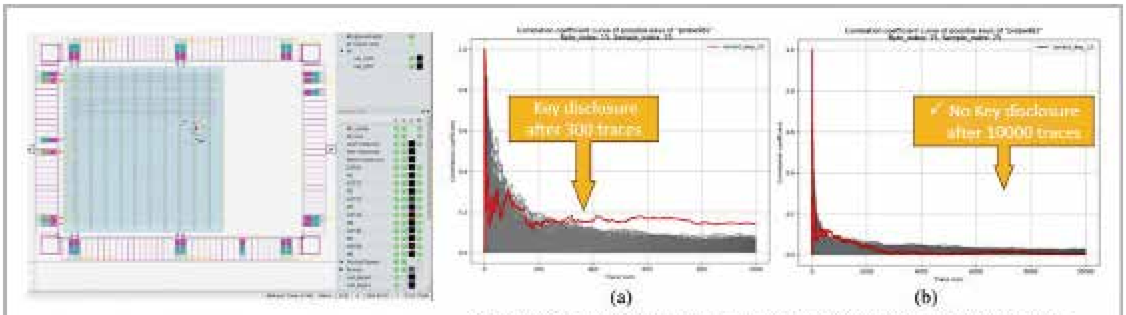
Side-Channel Analytics In-a-Box

RedHawk-SC Security empowers chip designers with the 'Security Insight' GUI to visualize side-channel traces and security signoff metrics. In detection mode, statistical metrics such as T-score are generated to validate the side-channel vulnerability with a pass-fail criterion for design security. By modeling multiphysics effects such as voltage drop, temperature change and EM coupling, user can further assess the security implication under various layout-level fault injection conditions. In cryptographic key disclosure mode, a classical or custom leakage model is used to quantify the statistical correlation between security assets and simulation traces. Built-in correlation-based security analytics can report sign-off metrics such as sensitivity score and simulation MTD (measurement-to-disclosure). Within the same GUI with security insights, users can assess all types of side-channel leakage traces including RTL power, gate power, on-chip power-noise, near-field EMag, and more.



Root-Cause Side-Channel Leakage

To efficiently mitigate data integrity issues, RedHawk-SC Security provides what-if analysis capabilities for a step-by-step diagnosis of potential design weaknesses and determination root causes. Once the side-channel leakage issue is identified temporally and spatially, the tool leverages the SeaScape Python API for querying the gate instances with the greatest impact on the data leakage mechanism. An interactive layout GUI can help the user visualize and scrutinize the problematic gates or metal wires to prioritize design fixes, with a rapid simulation turn-around-time of re-evaluation.



List of gate instances contributing into leakage

Correlation coefficients vs. trace number (a) before and (b) after the leaky instances are masked