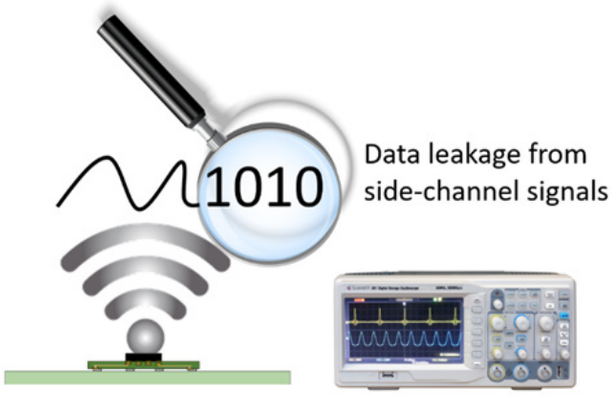
SEMICONDUCTORS

Ansys RedHawk-SC Security

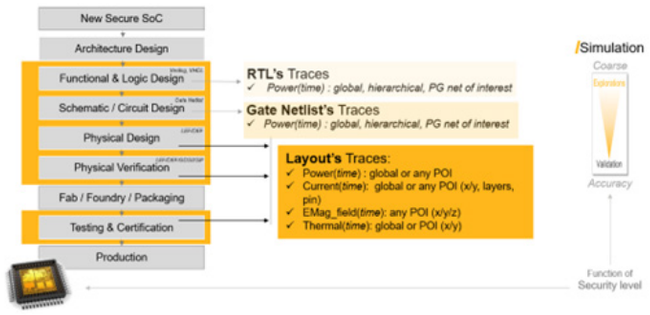
The First EDA Hardware Security Solution with Pre-silicon Side-Channel Leakage Analysis

Data security and privacy are essential concerns for mission-critical components in many electronic systems today. While modern cryptography is heavily used in automotive, financial, 5G, and IoT devices to assure information security, it can be compromised by exploiting vulnerabilities in the physical implementation of underlying integrated circuits (ICs). Ansys RedHawk-SC Security™ provides a breakthrough multiphysics simulation platform for RTL designers, physical implementation designers, and system integration engineers to verify side-channel leakage of ICs. It enables an IP and chip design team with minimum hardware security background to assess side-channel vulnerabilities and avoid silicon respin costs.



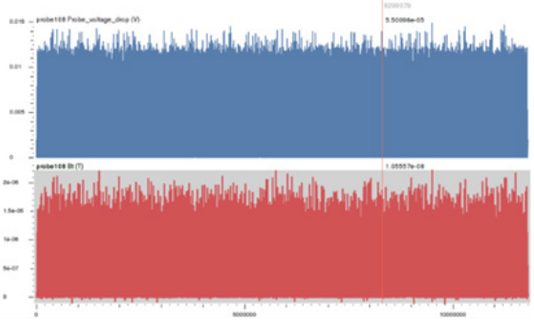
Product Highlights

Ansys RedHawk-SC Security features RTL and gate power, layout-level power noise, electromagnetic, and multiphysics simulation for fast side-channel trace generation and security analytics. With the RTL or gate netlist of a design, cycle-accurate power can be generated rapidly to assess early-stage power side-channel vulnerabilities across various microarchitectures and countermeasures. Once the physical design implementation is available, on-die and off-chip emissions can be virtually probed to pinpoint spatial and temporal side-channel leakage to prioritize physical design mitigations. RedHawk-SC Security leverages Ansys SeaScape™, the world's first custom-designed big data architecture for electronic system design and simulation. SeaScape provides per-core scalability, flexible design data access, instantaneous design bring-up, MapReduce-enabled analytics, and many other revolutionary capabilities.



Long-Vector Trace Simulation

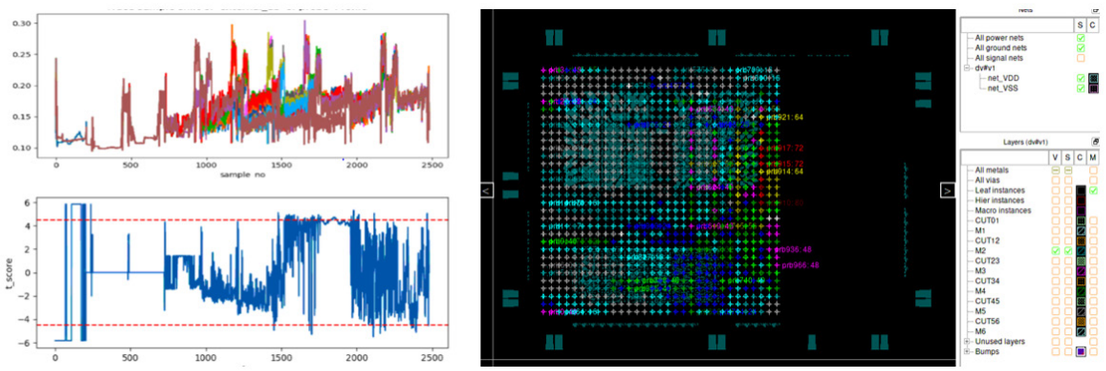
Relying on a novel algorithm to build a security-aware switching scenario and a security-critical side-channel probing configuration, side-channel trace simulation in RedHawk-SC Security can handle long vectors spanning billions of cycles. Unlike post-silicon measurements that are impacted by environment noise and have to be repeated over days and weeks, RedHawk-SC Security's side-channel trace simulation works efficiently with noise-free vectors. Vectorless switching of non-critical instances in the design can be modeled to imitate the silicon noise as



well. The trace generation and side-channel analytics are **exceptionally** fast, thanks to the innovative SeaScape architecture with parallel computing and cloud-native scalability.

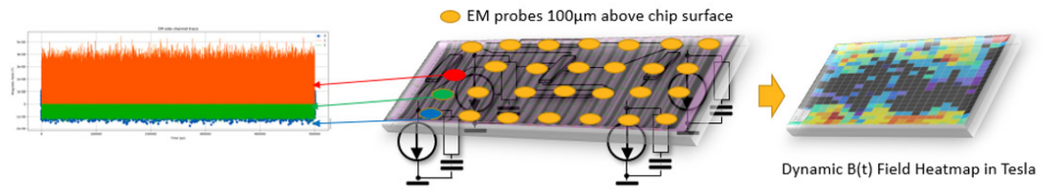
Root-Cause Side-Channel Leakage Across Design Stages

Side-channel leakage can be detected across design implementation stages. There can be multiple types of leakage mechanisms, and these can be detected at multiple locations. If security vulnerabilities are identified on silicon, they are often a black box to the IP/SoC designers, hindering meaningful design countermeasures. To avoid cost-prohibitive silicon re-spins, RedHawk-SC Security enables pre-silicon assessment of the most effective combinations of design countermeasures to optimally mitigate side channel leakage analysis using early-stage RTL power analysis, post-synthesis gate-level power analysis, and sign-off layout-level analysis.



Virtually probe electromagnetic side-channels

RedHawk-SC security enables layout-level near-field electromagnetic simulation to pinpoint side-channel leakage beyond the on-chip emissions. Simulation of dynamic magnetic field traces, represented by B(t), at user-given virtual probe locations can provide a comprehensive coverage of electromagnetic emission locations, enable the debug of leakage issues, and guide POI (point-of-interest) scanning in silicon laboratory tests.

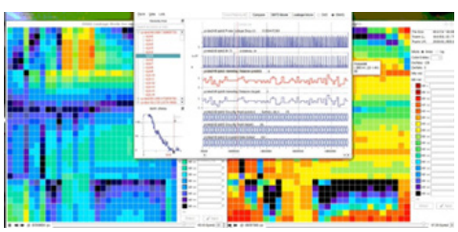


Side-Channel Analytics in-a-box

RedHawk-SC Security empowers chip designers with the 'Security Insight' GUI to visualize side-channel traces and security metrics. By analyzing metrics such as T-score, Ansys side-channel leakage score, and simulation MTD (measurement-to-disclosure), users can obtain location-dependent leakage information, debug design weakness, and validate the quality of simulation.

Industry-Golden Multiphysics Solvers

RedHawk-SC Security leverages industry-golden multiphysics engines including, but not limited to, RTL and gate level power from Ansys PowerArtist™, dynamic voltage drop from Ansys RedHawk-SC™, and thermal profile from Ansys RedHawk-SC Electrothermal™. The accuracy of the device modeling, power grid extraction, power integrity, and thermal reliability is certified by all major foundries. Both the power and electromagnetic side-channel analysis results have been correlated with real silicon to reflect the critical data leakage cycles and locations.



ANSYS, Inc.
www.ansys.com
ansysinfo@ansys.com
866.267.9724