

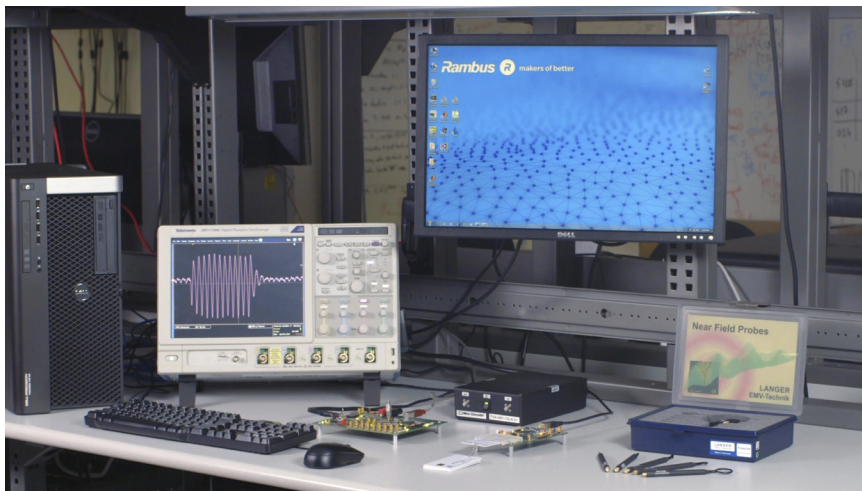


DPA Workstation Testing Platform

Powerful, flexible, and customizable testing platform for side-channel analysis.

Overview

Our DPA Workstation™ (DPAWS) 8 is a comprehensive analysis platform for the evaluation of device resistance to side-channel attacks, including SPA, DPA, HO-DPA, and EMA. Side-channel attacks are low-cost, non-invasive methods that enable attackers to extract secret cryptographic keys from electronic devices during normal operations. Build to support every stage of the side-channel analysis process, DPAWS 8 enables customers to quickly and easily identify and address potential security flaws in tamper-resistant systems and SoCs.



DPA Workstation 8 Testing Platform

The testing platform is optimized for ease-of-use and productivity and is ideal for cryptographic device vendors, system integrators, and testing labs to assess the robustness of side-channel attack countermeasures.

The platform is useful for non-invasive side-channel testing of complex systems and SoC-based designs. Devices that can be analyzed by the DPA Workstation include:

- Mobile computing devices
- Payment systems, Point of Sale terminals (POS)
- Authentication products
- Content protection, Pay TV
- Secure communication devices
- Embedded and general purpose CPUs

Highlights

Complete Testing Solution

- Turnkey platform for power and electromagnetic analysis (SPA, DPA, HO-DPA, SEMA, DEMA)

Powerful Analysis

- Specialized software and hardware focused on providing accurate and fast results

Customizable

- Source code is provided for increased flexibility

Integrated Project and Data Management

- Project Library Manager provides easy control of scripts and collected data

User-friendly, Powerful Data Visualization

- Highly intuitive user interface, dynamic displays and high performance

Project-oriented Analysis Environment

- Highly-integrated and project-centric designed to optimize the efficiency of side-channel analysis

Third-party Tool Integration

- Scripting shells for Matlab and Python

Device Flexibility

- Supports multiple side-channel sensors, device protocols, and form factors

Large Dataset Handling

- High-speed analysis of billions of traces, improving sensitivity and coverage

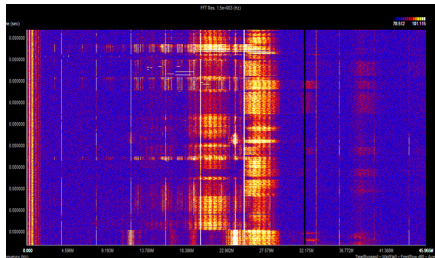
Robust Integrated Help Section

- Integrated FAQ, tutorials and wizards

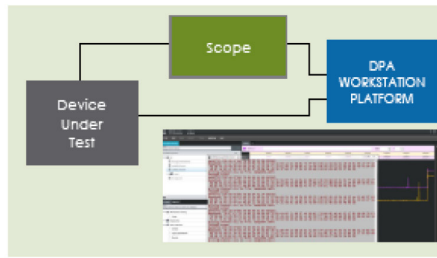
Legacy and Third Party Hardware Support

- Out-of-the-box support for SASEBO and other third party hardware

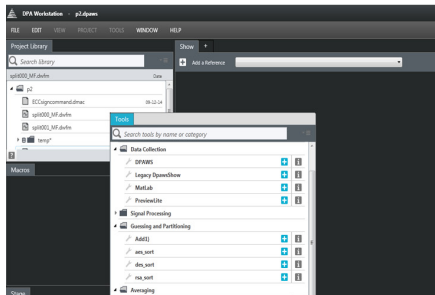
DPAWS includes wizard-like tools, as well as scripts to guide users through workflows, providing extraordinary visualization and analysis. Additionally, the intuitive Help section is provided to improve productivity and the effectiveness of the DPAWS platform.



Explore signals to identify leakage



Collect data via automated device interactions



Process with alignment and signal compression tools



Evaluate and perform leakage analysis

Deliverables

Analysis workbench

- DPAWS device interface and data collection environment
- Signal processing
- Hypothesis and Prediction generation
- Optimized DPA analysis utilities
- Analysis tools

Hardware

- Custom-configured workstation
- Oscilloscope
- Support for DPAD FPGA testing platform
- Smart card test fixture
- Support for PCI high-speed sampling cards
- Signal amplifier
- EM probes and filters
- Power supply

Proprietary software and source code to allow customization and adaptation

Capabilities

Data Collection	Scriptable data collection environment automates device interactions and data collection. A variety of connection interfaces, communication protocols, and sampling equipment, including RF receiver and EM probes for EM emissions are supported.
Signal Visualization	The DPA Workstation Show tool enables efficient signal navigation and visualization, offering quick operator feedback at all stages of the analysis process. It is an interactive visualization and signal processing tool for isolating signals of interest from noise and interference. Filters can be applied to power/EM traces being captured in real time, or on pre-recorded data.
Signal Processing	Includes alignment and signal compression tools for improving the quality of collected data.
Leakage Analysis	A comprehensive toolkit performs leakage analysis and key recovery for a variety of cryptographic implementations (AES, RSA, ECC, DES, SHA, and others).
Security Testing Profiles	Common criteria, FIPS 140, EMVco, DoD Anti-tamper, Payment and Card Industry (PCI), and GlobalPlatform

rambus.com/dpa

