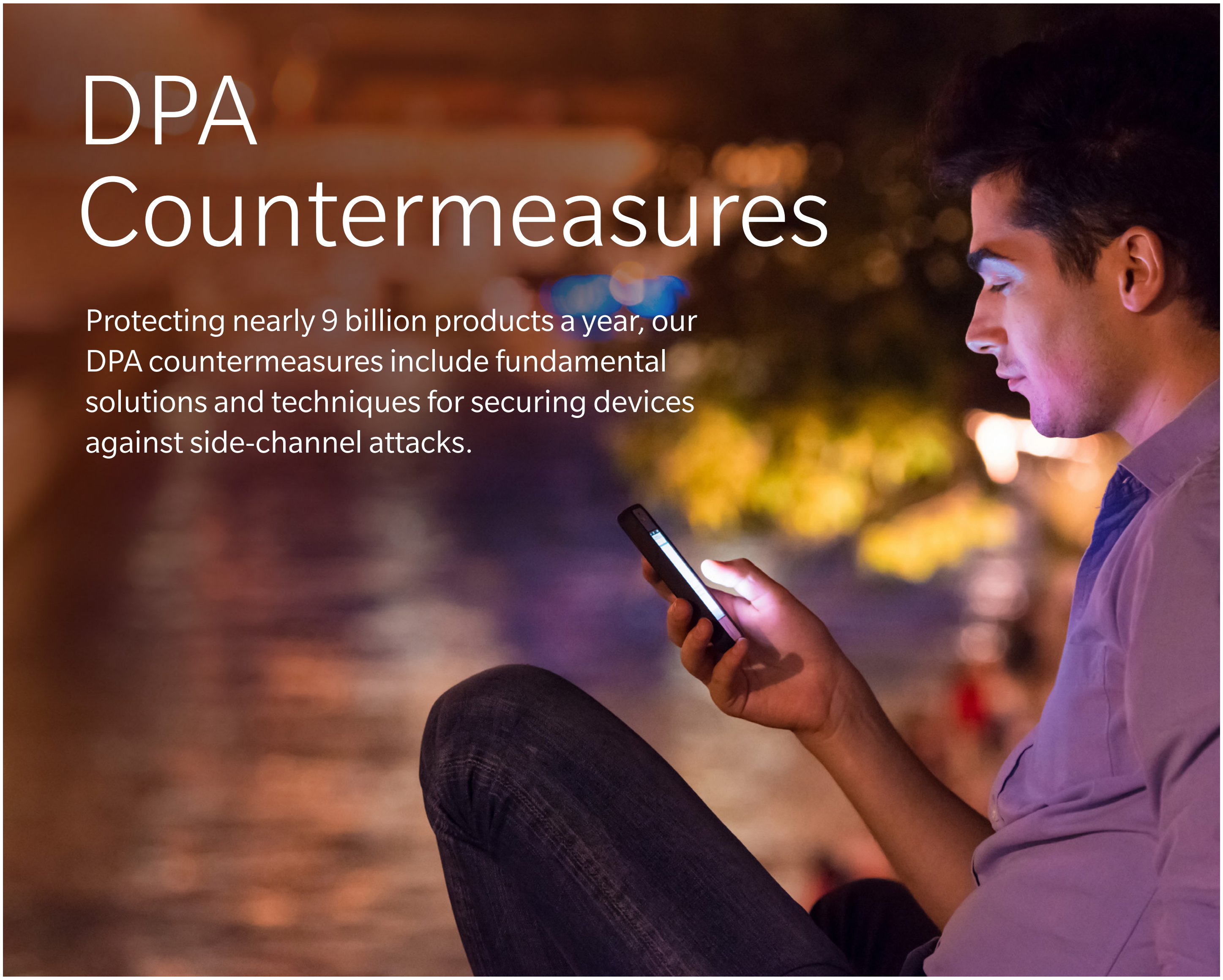


DPA Countermeasures

Protecting nearly 9 billion products a year, our DPA countermeasures include fundamental solutions and techniques for securing devices against side-channel attacks.

Superior Protection

- Robust countermeasures to protect against side-channel attacks
- Broad range of hardware, software and protocol approaches to secure tamper-resistant devices
- Cores validated to resist DPA attacks in millions of traces

Improve Time-to-Market

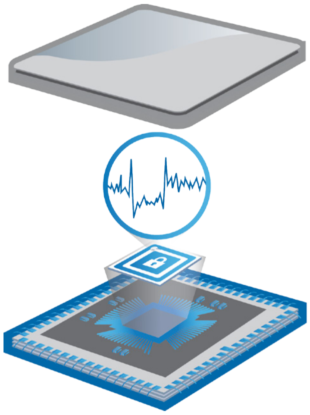
- Simplified device testing for power analysis vulnerabilities
- Training, evaluation services and analysis equipment
- Ready-to-use, DPA Resistant solutions

High Flexibility

- Solutions can be optimized for performance, size, and security level
- Solutions integrate with standard cipher modes such as CBC, ECB, etc.

Overview

Our Cryptography Research division discovered Simple Power Analysis (SPA) and Differential Power Analysis (DPA), and developed fundamental solutions and techniques for protecting devices against DPA and related side-channel attacks, along with supporting tools, programs, and services.



DPA countermeasures consist of a broad range of software, hardware, and protocol techniques that protect tamper-resistant devices from side-channel attacks in a number of ways including:

Leakage reduction – reducing information leaked into the side-channel to decrease signal-to-noise (S/N) ratios

Amplitude and temporal noise – adding amplitude or temporal noise into the side-channel to decrease S/N ratio

Balanced hardware and software – using hardware and software-based techniques to represent and process data in ways designed to minimize observable data-dependent variations within the side-channel

Incorporating randomness – representing cryptographic intermediates in forms that incorporate unpredictable information to reduce correlation between side-channels and the original intermediates

Protocol-level countermeasures – modifying cryptographic protocols using key update mechanisms to limit the amount of side-channel information available to an attacker for any particular key

Applications

- Aerospace and Defense
- Content Protection
- Mobile
- Storage
- Secure Communications
- Automotive
- Payments/Point-of-Sale
- Internet of Things

Deliverables

Solutions

- DPA Resistant Solutions – cores and software libraries (e.g., Verilog RTL AES)

Tools

- DPA Workstation^{TM} Testing Platform – a comprehensive tool suite for identifying vulnerabilities to side-channel attacks on all types of devices

Services

- Consulting and design guidance
- DPA validation program including rigorous third-party testing and certification Ecosystem of third party security core providers

Training

- DPA training workshops

Architecture License

- Patents enabling the main classes of DPA Countermeasures

Licensed DPA logo

- Trademarked Licensed DPA Logo identifies that a product is covered by a DPA countermeasures license from us

LICENSED
DPA
COUNTERMEASURES ™

rambus.com/dpa