Rambus

**CRYPTOGRAPHY RESEARCH**
DPA Countermeasures
Product Brief

# DPA Resistant Solutions

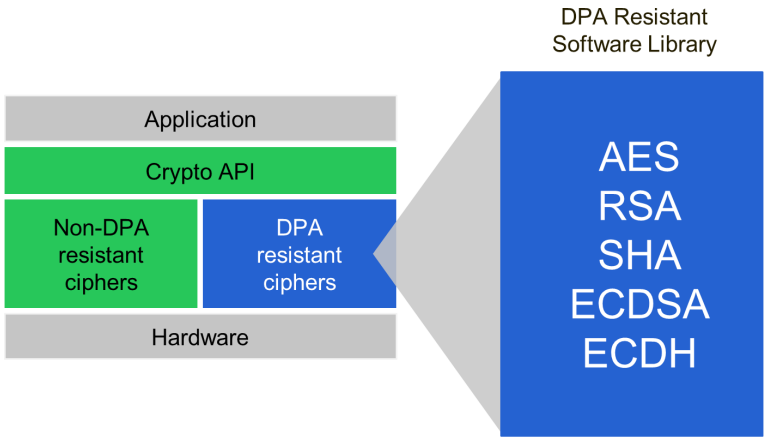
Designed to accelerate time-to-market, the family includes the DPA Resistant Software Library and DPA Resistant AES Core.

## Overview

Addressing the growing demand for readily available solutions that implement Differential Power Analysis (DPA) countermeasures, Rambus Cryptography Research developed a family of semiconductor IP cryptographic cores and software libraries that are designed to protect against side-channel attack vulnerabilities.

Our **DPA Resistant Software Library** incorporates many of the commonly used cryptographic algorithms. This library is validated to resist first- and second-order DPA attacks in over 1 million traces. It is easy to deploy in a security software stack, and is highly flexible for integration with standard cipher modes such as Cipher Block Chaining (CBC), Electronic Code Book (ECB), etc. The library implements advanced DPA countermeasures against side-channel attacks providing robust DPA resistance.

## Typical Deployment in a Security Software Stack




## Highlights

- Provide a higher level of protection than standard AES cores and libraries
- Ready-to-use, reducing implementation time
- Can be optimized for performance, size, and security level
- Easy-to-integrate with standard cipher modes such as CBC, ECB, etc.
- Enable chipmakers to devote resources to differentiating features
- DPA resistance-proven software libraries extensively validated against side-channel attacks
- Software library is easy-to-integrate into application stack
- Core is easy-to-integrate into SoCs and FPGAs
- Cores validated to resist first–and second–order DPA attacks up to 10 million traces .

**DPA Resistant Software Library**

- Reference design source code with build scripts and test vectors for the reference platform(s)
- Packaged libraries for a specific platform

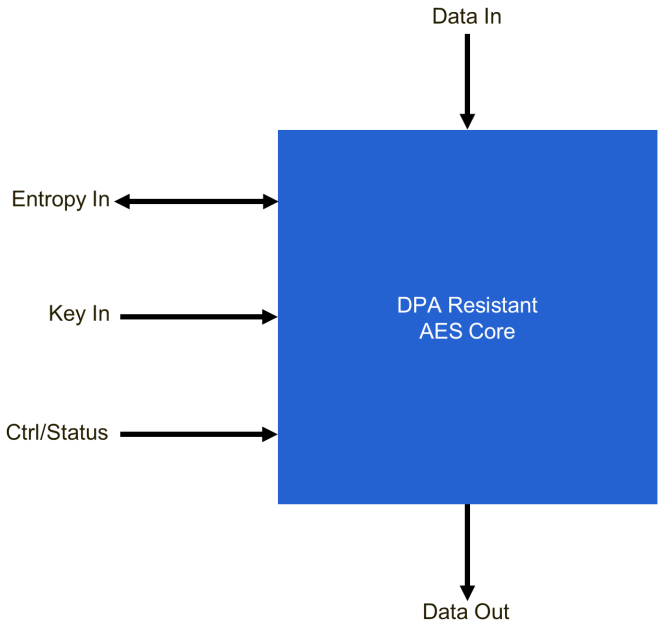
**Full Documentation:**

- Library usage guide

**Development and Test Environment (Optional)**

- DPA Workstation™ Testing Platform
- Hardware reference board for a specific platform
- Integrated testing framework

## DPA Resistant AES Core




## Capabilities

- Core implements a very high-security AES primitive
- Supports AES-128 and AES-256 encrypt and decrypt
- Simple control/status interface
- Implements DPA countermeasures such as LMDPL
- (LUT-Masked Dual-rail with Precharge Logic) gate-level masking and other schemes
- No routing constraints necessary for LMDPL
- Gate-level masking
- Delivers highest level of security with side-channel resistance prioritized

## Deliverables

**Configurable DPA-Resistant Core**
- Verilog RTL source

**Synthesis Inputs**
- SDC constraint file suitable for FPGA or ASIC synthesis

**Full Documentation**
- Usage guide

**Functional Testbench**
- NIST-compliant test vectors

**Development and Test Environment (Optional)**
- DPA Workstation™ Testing Platform
- Implementation on reference FPGA board
- Integrated testing framework

## DPA Resistant Software Library

- Library implements a very high-security primitives for AES, ECC, RSA, and SHA
- Supported platforms: ARM Cortex-A9, ARM7TDMI, and others
- AES supports 128/192/256-bit encrypt and decrypt
- ECC supports ECDSA ECDH for NIST prime fields (192/256/384/521)
- RSA supports signing and decryption at 1024/2048/4096/8192 bit lengths
- Incorporates state-of-the-art DPA countermeasures such as shuffling, blinding, and masking

## rambus.com/dpa