Rambus

CRYPTOGRAPHY RESEARCH
DPA Countermeasures
Product Brief

DPA Resistant AES Core

High-security, high-performance AES primitive designed with built-in side-channel resistance for cryptographic functions.

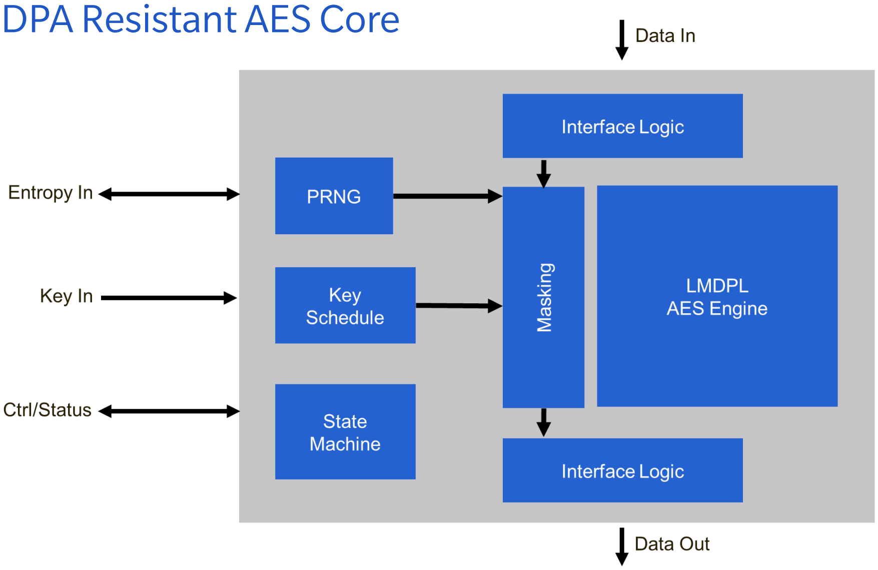
Overview

The DPA Resistant AES Core is a high-security AES primitive that offers chipmakers an easy-to-integrate security solution with built-in side-channel resistance for cryptographic functions across a wide range of connected devices.

This high-performance core offers both encryption and decryption functions with key size options of 128- and 256-bits.

It provides robust, flexible side-channel resistance for cryptographic functions validated to different security and performance levels based on product requirements. The high-performance core provides chipmakers with a seamless solution that enables them to devote resources to differentiating features and reduce implementation time.

DPA Resistant AES Core



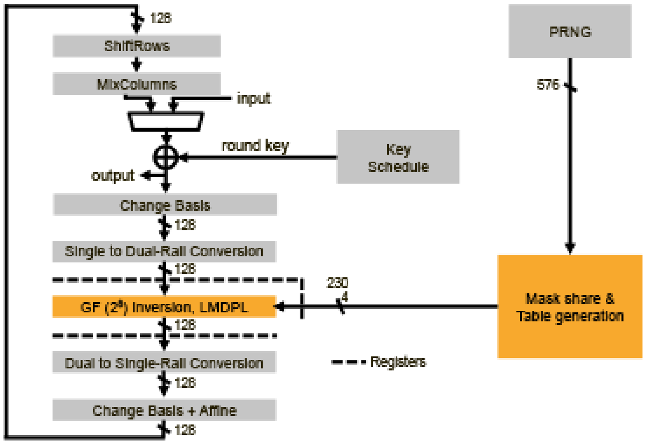
Highlights

- High-performance and DPA resistance-proven AES cryptographic core
- Provides a higher level of protection than standard AES cores
- Extensively validated against side-channel attacks of first-and second-order up to 10 million traces
- Highly flexible for integration with standard cipher modes such as CBC, ECB, etc.
- Easy-to-integrate into SoCs and FPGAs
- Optimized and validated for different performance, size, and security levels
- Countermeasures are portable to any FPGA and ASIC technologies
- Rambus Cryptography Research discovered DPA and developed a broad portfolio of countermeasures to protect against this vulnerability

Applications

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

Architecture Of The AES Implementation



Features

- 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 Pre-charge 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

Core	AES-128			AES-256		
	cycles	clk/B	MB/Sec*	cycles	clk/B	MB/Sec*
LMDPL-16	25	1.56	320.0	33	2.06	242.4
LMDPL-4	85	5.31	94.1	117	7.31	68.4
LMDPL-1	329	20.56	24.3	457	28.56	17.5

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

rambus.com/dpa