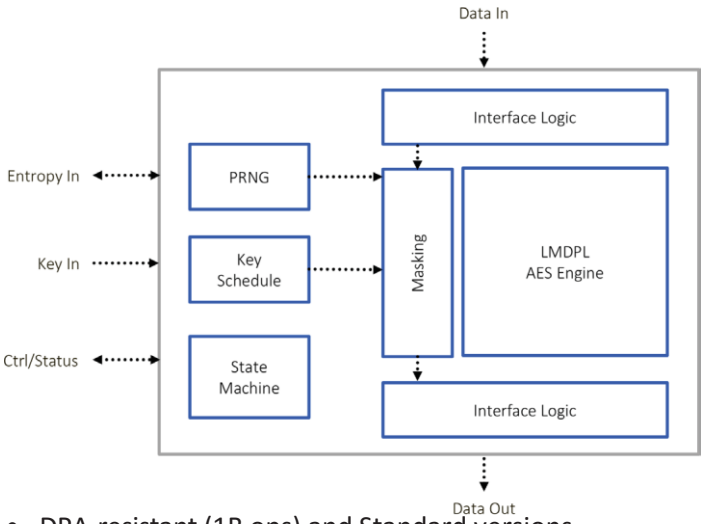
Rambus

SECURITY • CRYPTOGRAPHY
Cryptography Overview
Brochure

Cryptography Overview

Data · Faster · Safer

DPA-resistant and Standard Cryptographic Hardware Cores



DPA (Differential Power Analysis) Resistant Hardware Cores prevent against the leakage of secret cryptographic key material through attacks. Easily integrated into SoCs and FPGAs, the cores support industry standard cryptographic algorithms and random number generators such as AES, 3DES, SHA-2, HMAC, RSA and ECC. Extensively validated using the Test Vector Leakage Assessment (TVLA) methodology, and revealing no leakage beyond 100 million traces, the core is protected against univariate first- and second-order side-channel attacks beyond 1 billion operations.

- DPA-resistant (1B ops) and Standard versions
- Small, Medium and full performance grades
- 128- and 256-bit keys
- ECB, CBC, CFB, CTR, CCM, GCM

3DES
- DPA-resistant (1B ops) and Standard versions
- 112- and 168-bit keys
- ECB, CFB, CBC

ChaCha20

Poly1305

SHA-2 & SHA-3
- DPA-resistant (100M ops) and Standard versions
- Compact: 224- and 256-bit
- Full: 224-, 256-, 384- and 512-bit
- Context switch (store/restore state)

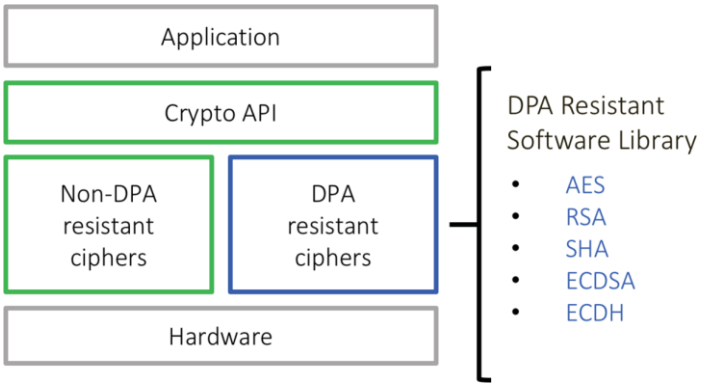
HMAC SHA-2 & SHA-3
- DPA-resistant (100M ops) and Standard versions
- Compact: 224- and 256-bit
- Full: 224-, 256-, 384- and 512-bit

Asymmetric Public Key Engine
- DPA-resistant (100M ops)
- RSA, RSA-CRT, up to 4K bits
- ECDSA, ECDH up to 521 bits
- NIST P192/224/256/320/384/521
- ANSSI-FRP256V1
- Brainpoolr1/t1 P192/224/256/320/384/512

True Random Number Generator
- RBG Random Bit Generator SP800-90C
- NRBG Entropy Source SP800-90B
- DRBG Post Processor SP800-90A

Available Legacy Algorithms
- MD5, SHA-1, others

DPA-resistant Software Library



DPA-resistant Software Libraries provide performance optimized, quantifiable tamper-resistant security for software systems with seamless integration across a wide range of applications. DPA-resistant Software Libraries are validated to resist first- and second- order DPA aAacks in over 1 million traces. They are highly flexible and easy to deploy in existing security software stacks, utilizing both pladorm neutral

C-code and ARM® Cortex™ optimized code.

AES Library
- 128/256 keys
- Modes: ECB, CBC, CTR, CFB, GCM

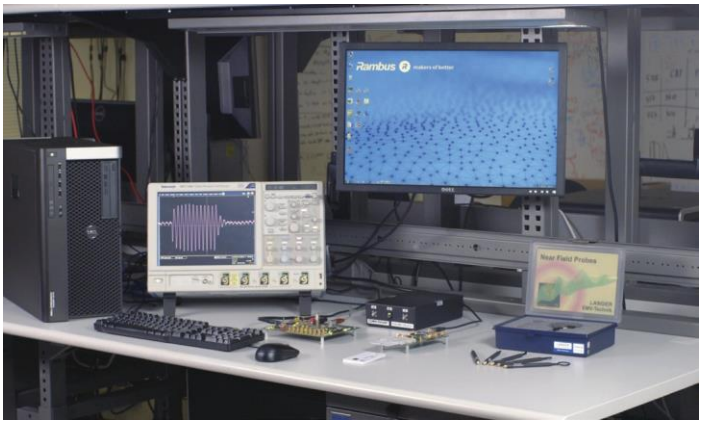
3DES Library
- 112/168 keys
- Modes: ECB, CBC, CFB

HMAC SHA-2 Library
- SHA-2 and HMAC

RSA Library
- RSA/RSA-CRT, up to 4K bits

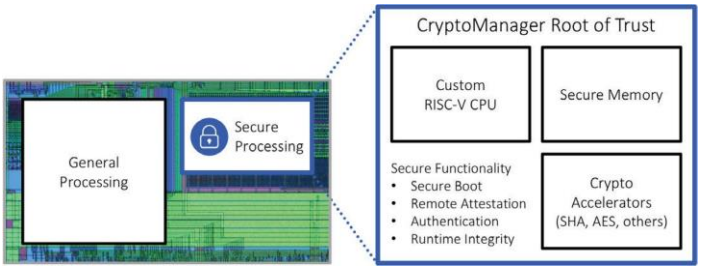
ECC Library
- ECDSA, ECDH up to 521 bits
- NIST P192/224/256/320/384/521

DPA Workstation Testing Platform



The DPA Workstation analysis platform is the world's premier side-channel analysis platform, including all of the hardware, software, and training needed to evaluate and certify secure devices. DPA Workstation 8 is a powerful and flexible testing platform that includes an integrated suite of hardware and powerful data visualization software for testing and analyzing the vulnerabilities of cryptographic chips and systems to power and electromagnetic (EM) side-channel attacks. Designed to support every stage of the side-channel analysis process, DPAWS 8 enables users to quickly and easily identify and address potential security flaws in tamper-resistant systems and SoCs.

CryptoManager Hardware Root of Trust



The CryptoManager Root of Trust is an independent hardware security block for integration into semiconductor devices, offering secure execution of user applications, tamper detection and protection, secure storage and handling of keys and security assets, and resistance to side-channel attacks. The core mitigates against attacks like Meltdown and Spectre by allowing secure processing to be separated from general processing in a siloed architecture.

The Root of Trust is easily integrated with industry- standard interfaces and system architectures and includes hardware cryptographic accelerators for standard algorithms such as AES, SHA, RSA, ECDSA & ECDH.

Superior Security

- Hardware root of trust featuring a custom 32-bit RISC-V processor
- Secure in-core processing and industry-leading anti-tamper
- Built-in tamper detection and resistance to side-channel attacks
- Multi-layered security model provides protection of all components in the core

Enhanced Flexibility

- 3rd-party applications run securely within trusted boundary
- Complete development environment allows users to easily develop secure applications leveraging all capabilities of the core
- Support for secure provisioning of keys and firmware at manufacturing or in the field
- Support multiple roots of trust within a single core

Security Models

- Hierarchical privilege
- Secure key management policy
- Hardware-enforced isolation/access control/protection
- Error management policy

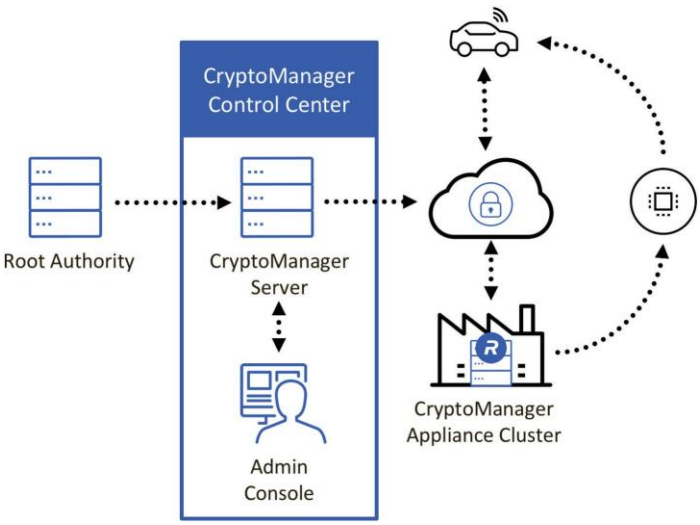
Cryptographic Accelerators

- Standard AES, SHA, Public Key Engine (implementing RSA & ECC)
- Optional 3DES, ChaCha20, Whirlpool, DPA-resistant crypto engines and proprietary entropic array logic

Security Modules

- True Random Number Generator
- Anti-tamper logic for protection against glitching and overclocking
- Secure key derivation and key transport
- Life cycle management
- Secure test and debug
- Feature management

CryptoManager Infrastructure



Our CryptoManager Infrastructure is a high-performance enterprise class device provisioning solution that reduces operating costs and accelerates time-to-market. It is designed to seamlessly integrate into existing manufacturing flows with minimal interruption, and enables the secure provisioning of cryptographic information throughout the distributed manufacturing supply chain. The cryptographic information covers a broad range of secure transactions, including key delivery and programming, protection of debug modes, and chip feature management. It can be used to provision the device specific information to any security IP core, including our CryptoManager Root of Trust.

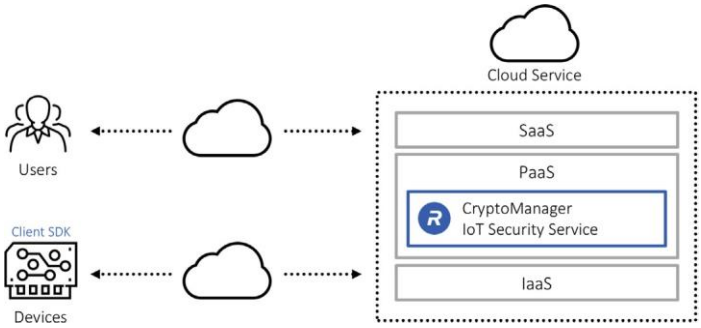
Enterprise

- Cluster support for high availability and scalability
- Dynamic SKU management
- Ability to provision secure data to any secure IP core or chipset
- Comprehensive system monitors and alerts
- Advanced key and data management
- Verify manufacturing volumes, yields, and configurations. Monitor production status, availability, and inventory level

Security Features

- Protect against cloning, reverse engineering, counterfeiting, and overbuilding
- Root Authority for system permissions and authorizations
- Provision cryptographic information securely in untrusted environments
- Advanced encrypted key and data storage
- Two-factor user authentication

CryptoManager IoT Security Service



The CryptoManager IoT Security Service is a Security-as-a-Service offering that provides seamless secure device connectivity, security lifecycle management, and advanced device monitoring capabilities by supporting a combination of multiple cloud solutions and client hardware architectures. The service is pre-integrated with leading IoT chipset and PaaS providers creating an out-of-the box secure connection between IoT endpoints.