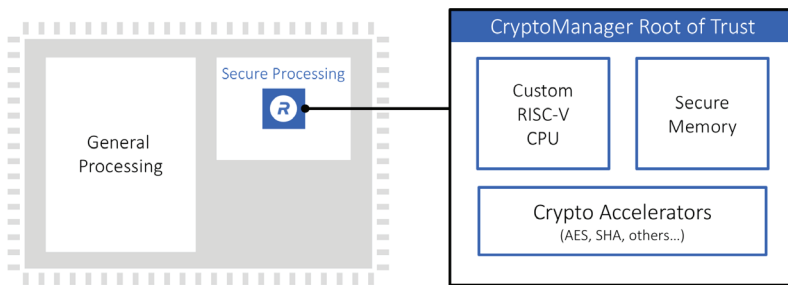# CryptoManager Root of Trust RT-670

Fully-programmable, embedded FIPS 140-2 CMVP certified hardware security co-processor for Military Applications

Overview

The CryptoManager Root of Trust is a fully-programmable hardware security core that protects against a wide range of attacks with state-of-the-art anti-tamper and security techniques. Military semiconductors are targets for adversaries, and must be secured with the highest resistance possible. To address present and future military threat requirements, Rambus has created the RT-670. FIPS 140-2 CMVP certified, the RT-670 features a custom 32-bit RISC-V siloed and layered secure co-processor, along with dedicated secure memories. Within the co-processor are DPA-protected cryptographic cores like AES-AE-16, HMAC 512, 3DES, RSA 4K, ECC 521, and a NIST-compliant Random Bit Generator. For Type 1 designs, wrappers with placeholders for Suite A crypto cores are provided. Designed for deployment onto a variety of military devices, the RT-670 Root of Trust offers the highest security Rambus provides.

Secure Processing

Highlights

Superior Security
- Hardware root of trust featuring a custom RISC-V processor
- Secure in-core processing and industry-leading anti-tamper
- Multi-layered security model provides protection of all components in the core
- FIPS 140-2 CMVP certified
- DPA-resistant cryptographic accelerators

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; standard use case containers provided
- Support for secure provisioning of keys and firmware at manufacturing or in the field
- Support multiple roots of trust within a single core

How It Works

The CryptoManager Root of Trust RT-670 is a siloed hardware security block for integration into semiconductors, 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 Root of Trust is easily integrated with industry-standard interfaces and system architectures and includes standard DPA-resistant hardware cryptographic cores. Access to crypto modules, keys, memory ranges, I/O, and other resources is enforced in hardware. Critical operations, including key derivation and storage, are performed in hardware with no access by software.

The CryptoManager Root of Trust is based on a custom 32-bit RISC-V CPU designed specifically to provide a trusted foundation for secure processing in the core and system. The RISC-V CPU runs signed code modules called containers, which include permissions and security-related metadata. These containers can implement standard security functionality provided by Rambus, or complete customer-specific security applications, including key and data provisioning, security protocols, biometric applications, secure boot, secure firmware update, and many more.

Hardware-enforced, Software-configurable Operation

The CryptoManager Root of Trust is integrated as an independent hardware security block in semiconductor devices where security is needed. Once integrated into a semiconductor device, it provides a secure environment for performing a wide range of security functions in a simple and cost-effective manner, providing enhanced security functionality while providing faster time-to-market and significant differentiation.

Root of Trust Integration
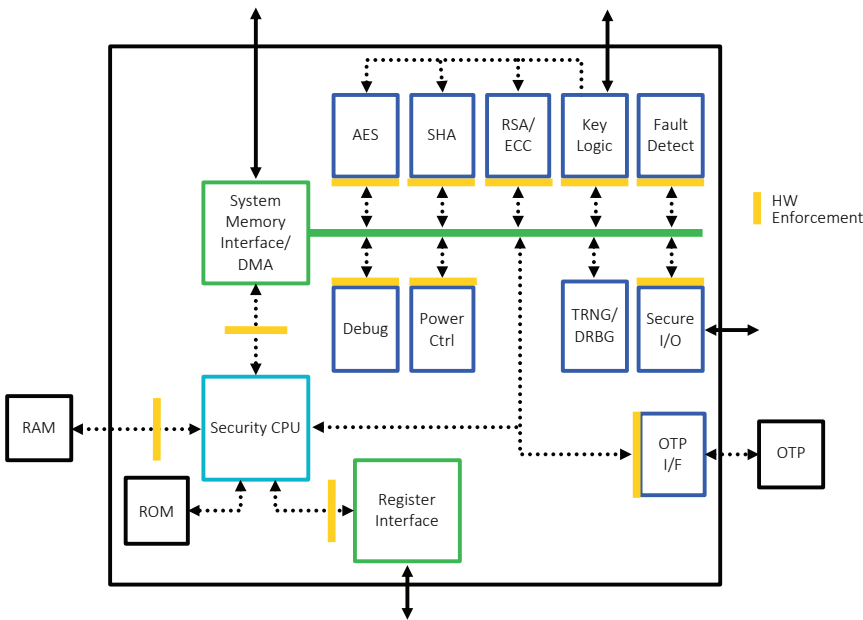
Features

- 32-bit secure RISC-V processor
- Security model include hierarchical privilege model, secure key management policy, hardware-enforced isolation/access control/ protection, error management policy
- Standard DPA-resistant hardware cryptographic accelerators, including AES-AE-16, HMAC 512, 3DES, Suite A placeholders, RSA 4K, ECC 521, and RBG. FIPS 140-2 CMVP compliant
- Multi-layered security model protects all core components against a wide range of attacks
- Includes a wide range of security modules, including True Random Number Generator, Canary logic for protection against glitching and overclocking, secure key derivation and key transport, life cycle management, secure test and debug, feature management

Deliverables

Complete Documentation
- Hardware integration guide
- Hardware and software reference manuals
- Programming guides

Tools and Scripts
- Verilog for synthesis and simulation
- All scripts and support files needed for standard EDA tool flows

Integration Deliverables
- Complete verification test bench and comprehensive set of test vectors
- Boot loader and firmware, including secure RTOS and security monitor
- HLOS APIs for accessing capabilities
- Complete development environment, including compiler, assembler, debugger, simulator, reference code
- Available FGPA-based development board

Use Cases

- Secure data and key storage
- Device personalization
- Key and data provisioning
- Authentication and attestation
- Secure boot
- Secure firmware update
- Runtime integrity checking
- Feature/configuration/ SKU management

rambus.com/cryptomanager