Rambus

CRYPTOGRAPHY RESEARCH
CryptoFirewall Cores
Solution Overview

CryptoFirewall Cores

Our cores complement existing security implementations, and are ideal for protecting digital content and preventing counterfeiting in a broad number of applications.

Superior Security

- Highest level of security for content protection and anti-counterfeiting
- Independent hardware core maintains security even if other parts of the chip are compromised

Improve Profitability

- Reduce revenue lost to unauthorized access and counterfeits
- Easy integration in existing systems
- Compatible with standard manufacturing processes
- Simplifies device validation to improve time-to-market

High Flexibility

- Support distribution of various Over-the-Top (OTT) content to STBs and Smart TVs
- Supports all content distribution platforms – satellite, cable, IPTV and OTT

Overview

Designed to prevent tampering, the hardware-based CryptoFirewall™ security core minimizes the risk of security failure and helps simplify product development. Comprising a security boundary inside a chip, the core stores private keys and maintains security – even if the rest of the system is compromised. CryptoFirewall solutions complement existing security implementations and are ideal for a wide range of applications, including digital entertainment, electronic devices, printers and ink toners.

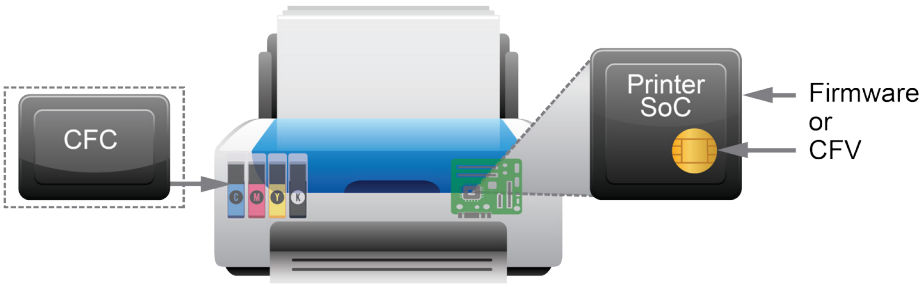
Our CryptoFirewall line-up includes cores for protecting digital entertainment and preventing counterfeiting.

Content Protection Application:

Piracy is an enormous challenge for the digital entertainment industry, costing content owners and operators billions of dollars in revenue each year. Designed for securing digital content, our CryptoFirewall core is an independent hardware core within the SoC that provides comprehensive key management and secure video decryption. Easily integrated with leading CAS and DRM systems, the core effectively thwarts the unauthorized access of content by securing multimedia-decoding chips found in set-top boxes and smart TVs.

Anti-Counterfeiting Application:

Our hardware-based Consumable Protection System is a cost-effective and robust security solution designed to prevent counterfeiting of mass-market consumables such as printer supplies. This tamper-resistant security core can be integrated into existing chips, or implemented as a discrete security chip on consumables for unsurpassed protection against counterfeiting.



Features

Protects against a broad range of attacks including:

- Software bug vulnerabilities
- Reverse engineering
- Glitching/fault induction
- Power analysis (SPA/DPA)
- Test/debug mode exploits
- Protocol attacks
- Microprobing
- Cryptanalysis
- Focused ion beam analysis
- Imaging/microscopy
- Software emulation
- Insider attacks

Anti-Counterfeiting:

- Secure device authentication
- Secure usage authentication

Content Protection:

- Provides the most robust hardware protection
- Supports multiple security domains
- Cost-effective security in the SoC — no external interface to attack
- Meets studio security requirements including UHD/4K content, facilitating licensing of premium content
- Supports all major content distribution platforms - satellite, cable, IPTV, OTT, physical media

Deliverables

Gate-level netlist targeted to vendor-specified cell library

Full technical documentation:

- Interface specifications
- Integration guides
- Validation guides
- Manufacturing test and personalization specs

Test and Verification:

- Verification models
- Emulation boards
- Functional verification tests
- System and validation tests

rambus.com/cryptofirewall

© Rambus Inc. 1050 Enterprise Way, Suite 700
Sunnyvale, CA 94089 • rambus.com