CryptoFirewall Cores

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

**Superior Security**
- Highest level of security for 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
- Simplifies device validation to improve time-to-market

**High Flexibility**
- Compatible with standard manufacturing process
- Support for a wide array of applications and easy integration into existing and new designs
CryptoFirewall Cores

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 electronic devices, printers and ink toners.

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

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