Rambus

CRYPTOGRAPHY RESEARCH
CryptoFirewall Cores
Product Brief

CryptoFirewall Consumable Protection System

Our hardware-based system provides the most cost-effective and robust security solution to prevent the counterfeiting of printer supplies.

Overview

Highest Security at the Lowest Cost

Counterfeit printer consumables sales total about $2.4 billion annually or 4% of the $60 billion ink and toner cartridge market.[1] These counterfeit cartridges can produce poor quality output, damage printers, frustrate consumers and tarnish printer OEM reputations. Off-brand supplies comprise an additional 16% ($9.6 billion) of the market and can also cause poor customer experiences.

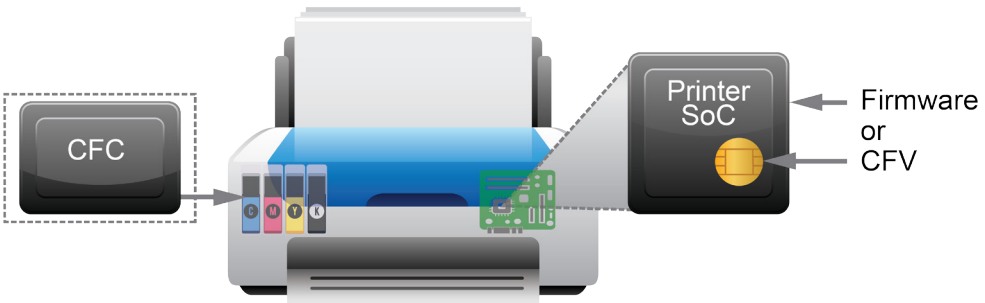
Our CryptoFirewall™ Consumable Protection System (CPS) is a cost-effective way to achieve extremely robust security. It does not require a separate security chip in the printer, and the technology can be customized to meet specific customer requirements for high-volume applications.

Advantages of Hardware-Based Security

Printer manufacturers have historically had a limited set of anti-counterfeiting options, such as holograms and visual stickers. However, these approaches are not easily authenticated by printers, consumers, or even customs officers. More recently, printer OEM have used repurposed smart card designs or other microprocessor-based chips, but such approaches are susceptible to software bugs, invasive attacks, fault induction, side-channel analysis, or other vulnerabilities, and have often proven insufficient in the field.

Our CryptoFirewall CPS is a dedicated hardware solution that does not depend on software or CPUs for security. It provides robust tamper resistance, and complements existing security measures.

1.Lyra Research Inc. (2009, 2010), Enhanced Protection for Imaging



Highlights

Superior Security

- Highest level of security and tamper resistance
- Flexible security and compatibility with existing policies

Improved Profitability

- Stops revenue loss to counterfeit ink and toner cartridges
- Cost-effective supply chip; printers do not need a separate security chip
- Easy integration into existing systems and compatible with six standard chip manufacturing processes

How It Works

Cartridge chips must have robust security to prevent attackers from exploiting the secrets from one chip then mass-producing counterfeits. Our hardware in each cartridge chip is a robust, self-contained cryptographic security core engineered with a security perimeter that assumes all external inputs are malicious. Restricted, well-defined state machines manage security operations, and are cross-checked during computations.

The CryptoFirewall consumable security chip (CFC) is authenticated by the printer SoC via firmware or by an integrated CryptoFirewall Verifier (CFV) core. Firmware-based verification avoids the need for any special hardware support in the printer, while the optional CFV adds protection against firmware tampering.

Our CryptoFirewall architecture is designed for easy integration into high-volume products. Personalization and keying can be performed in multiple stages to prevent insider attacks and to allow the use of lower-cost manufacturing without sacrificing security. Compatibility with standard cell ASIC design flows and chip fabrication ensure high yield and minimize costs. With support for both ink and toner platforms and flexible usage scenarios, the CryptoFirewall CPS provides a compelling solution to the counterfeiting problem.

Features

A complete solution to protect against the full range of attacks, including:

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

Device Authentication: Each cartridge contains a low-cost CFC chip that communicates with either a CFV or with firmware on the printer to authenticate the cartridge.

Usage Authentication: The CFC chip contains usage counters whose balances are used to authorize printing. Balances are decremented during printing, and once the balance reaches zero, the CFC can no longer authenticate.

Deliverables

Gate-level netlist targeted to vendor-specified cell library

Full technical documentation:

- Interface specification
- Integration guide
- Validation guides
- Manufacturing test and personalization specs

Test and Verification:

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

rambus.com/cryptofirewall