The IBM 4758 Secure Cryptographic Coprocessor
Hardware Architecture
and Physical Security

Steve Weingart
Senior Engineer
(561) 392 6100
c1shw@us.ibm.com

Secure Systems and Smart Cards
IBM T.J. Watson Research Center
Hawthorne, NY
4758 PCI Cryptographic Adapter/Secure Processor

- History

- IBM 4758 PCI Cryptographic Adapter
  - Architecture
    - New Features
    - Implementation
  - Physical Security
IBM Cryptographic Adapters

History

• Effort started in 1983
• Provided input and design assistance to IBM
  • IBM FBU Charlotte Castle Products (4753)
  • IBM ESD ICRF

Strengths

• Architecture Has Been In Use Since 1987, So It is Well Known.
• General Purpose Processor
• Fast DES
• Reasonably Easy to Write Code

Weaknesses

• No Hardware RSA
• No Good (Hardware) Random Number Generation.
• General Purpose Processor was Underpowered
• Existing Crypto Interface is Cumbersome for RSA and Transaction Type Processes
• Not Easy Enough to Write code
Architecture:
Product Design
New Features

- Faster Processor
- Full PC Compatibility
- PCI Bus Attach to Permit Wider HW Base
- Hardware RSA (Math Support)
- Packet Mode for Lower Overhead for Non-Bulk Operations
- Half Card PCI Design (PCI base card plus secure processor assembly)
- Physical Security (FIPS 140-1 Level 4)
- Good Random Number Generation.
Architecture:
New Features
Block Diagram

486 PC Compatible Computer

PCI Bus

Intermediate Parallel Bus

Control Gate Array

DES

FIFO

Router Gate Array

MATH

FIFO

PCI Interface

Physical Security Boundary
New Features:
Communications

- Communications Paths:
  - All Controlled From Adapter Processor
  - Data Paths to:
    - PCI Controller for Mailbox access
    - FIFOs for DES & Packet Mode
    - Directly to RSA & DES Devices
    - Controller/State Machine

- Crypto Modes:
  - DES, High Speed
    - PCI Bus or Adapter Processor Memory Space as Source, FIFOs for Speed Balancing
    - PCI Bus or Adapter Processor Memory Space as Target, FIFOs for Speed Balancing
    - DMA/Busmaster on Both Sides Controlled by State Machine
    - Once Established it is Independent of Adapter CPU
  - DES Low Speed
    - I/O From Adapter Processor (Use for Triple Encryption)
  - RSA
    - I/O From PCI Cryptographic Adapter Processor
  - Packet Mode (RSA or DES)
    - One FIFO Open From PCI Bus to PCI Cryptographic Adapter
    - One FIFO Open From PCI Cryptographic Adapter to PCI Bus
    - Lowers Overhead for Small Transaction Packets Compared to Bulk DES Overhead
New Features:
Operating Environment

- All Standard PC Functions Available, Including:
  - Address Space
  - Interrupts
  - DMA
  - Serial Communications (limited use)
  - Counter/Timer
  - RTC
- Improves Development Environment
  - Can Develop/Test On Standard PC
  - Embedded OS (CP/Q) Environment Permits Development on Host
New Features:
PCI Interface

- Permits Wide Range of Hardware Platforms
  - PC and Compatible
  - PowerPC
  - PowerMac
  - Unix Workstations
  - Improved Performance

- PCI Data Rates to 132 MBytes/sec.

- Target or Bus Master Capability

- Built in FIFOs at Max Bus Rate

- Mailbox with Interrupts for Command/Control Interface
Implementation

- **PCI**
  - 32 bit 5V card, Supports Target and Master

- **CPU** Integrated 1 Chip 486 PC (CPU + PC Support)
  - 4 Mbytes RAM
  - 2 Mbytes Flash

- **Crypto**
  - Custom DES Chip (25+ MBytes/sec (HW), 16 bit wide data interface)
  - RSA (Math) Chip (Fast, approx. 20 ops/sec for 1024 bit key/data & exponent, 2048 bit capable)
  - Gate Arrays for Router and Controller/State Machines
  - Hardware Noise-Based Random Number Generator
Physical Security Requirements

- Needed to meet FIPS 140-1 level 4

- To meet Tamper detection requirements
  - Older designs were not good enough, or were not manufacturable
  - Tamper Membrane - New Technology Membrane
    - Manufacturing issues
    - New Circuitry for New Membrane

- To Meet EFT/EFP Requirements
  - Voltage
    - All Power Supplies
      - Operating Ranges (Reset)
      - Damage Ranges (Tamper)
  - Battery
    - Low (Warning)
    - Failure (Tamper)
  - Temperature
    - Operating Range (Reset)
    - Damage Range (Tamper)
  - Radiation

- Had to do all the above on a battery budget

- Special considerations for zeroization
  - No Environmental Imprinting

- Validated FIPS 140-1 Level 4
Physical Security
Cutaway Drawing

- Metal Shield
- Tamper Detecting Membrane
- Inner Cover
- Shielded Base Card
- Flexible Data/Power Cable

4758 PCI Cryptographic Adapter/Secure Processor

Steve H. Weingart
IBM T. J. Watson Research Center, Hawthorne, NY
(561) 392-6100.
c1shw@us.ibm.com