IBM PCI-*
Cryptographic Coprocessors

Presented by Tom Connors and Kyle Burden

“A flexible solution to your high-security cryptographic processing needs”
Agenda

• Introduction
• Features
• Design
• Architecture
• Performance Comparison
• Applications
Introduction

- **What is a Side Channel Attack**
  - timing attacks
  - power analysis
  - differential fault analysis

- **What is a Secure Processor**
  - a general-purpose computing environment that withstands physical attacks and logical attacks
  - able to distinguish between the real device and application, and a clever impersonator
Family of Secure Processors

- **4578 - PCI**
  - discontinued in 2005
- **4764 - PCI-X**
  - May 2011 - December 2011
  - System z
- **4765 - PCI-E**
  - introduced in 2011
  - System x
Features

- High-security processing and high-speed cryptographic operation
- Tamper Responding Hardware with diagnostics
- Flexible Hardware
- Embedded Certificate
- Hardware specialized for AES, SHA-X, RSA, ECC, and MAC
- IBM Common Cryptographic Architecture API
- Processor lockstep (error-checking)
Common Cryptographic Architecture

- API with User Defined Extension
- Encryption
- Digital Signature
- Key Distribution
- Random-Number Generation
Tamper Responding Hardware

• FIPS 140-2 Level 4 Certification
  o power sequencing
  o temperature manipulation

• Triggered?
  o destruction of certificate & data
  o permanently inoperable
Design

- IBM 4764 PCI-X
- IBM Crypto Engine
- Tamper Detection
- Security Supervisor
- Secure Clock
- Battery Backed RAM
Architecture of 4765

- 2 PowerPC 405 @400 MHz
- Secure Service Processor (SSP) @100MHz
- 128 MB of Shared DRAM
- 64 MB of Flash Memory
- 3.5 MB of BBRAM
  - 3 KB High-Speed Erase
Architectural Evolution

- Multiprocessor Environment
  - Error Detection
- Separation of concerns between MCPU’s & SSP
- Flexible hardware
- BBRAM with high-speed erase
- Higher throughput
- Improved diagnostics
Architectural Evolution continued
Architectural Evolution continued ...

<table>
<thead>
<tr>
<th>Location, 4764</th>
<th>Firmware code segments</th>
<th>Location, 4765</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerPC</td>
<td>Segment 3 (reloadable)</td>
<td>PowerPC</td>
</tr>
<tr>
<td></td>
<td>Application (CCA)</td>
<td></td>
</tr>
<tr>
<td>PowerPC</td>
<td>Segment 2 (reloadable)</td>
<td>PowerPC</td>
</tr>
<tr>
<td></td>
<td>O/S and drivers (Linux**)</td>
<td>PowerPC</td>
</tr>
<tr>
<td>PowerPC</td>
<td>Segment 1 (reloadable)</td>
<td>PowerPC</td>
</tr>
<tr>
<td></td>
<td>POST1, Miniboot1</td>
<td></td>
</tr>
<tr>
<td>PowerPC</td>
<td>Segment 0 (permanent)</td>
<td>SSP</td>
</tr>
<tr>
<td></td>
<td>POST0, Miniboot0</td>
<td></td>
</tr>
</tbody>
</table>
## Performance Comparisons

<table>
<thead>
<tr>
<th>(4096 Block Size)</th>
<th>Haswell i5-4570 (cycles per byte)</th>
<th>4765 (cycles per byte)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128</td>
<td>9.15</td>
<td>9.86</td>
</tr>
<tr>
<td>AES-256</td>
<td>13.59</td>
<td>12.2</td>
</tr>
<tr>
<td>SHA-256</td>
<td>11.92</td>
<td>7.91</td>
</tr>
<tr>
<td>Keccak</td>
<td>10.85</td>
<td>? - 38.14</td>
</tr>
</tbody>
</table>
Applications

• High-Speed Data Encryption
• Digital Signing
• Secure Storage
• Custom Cryptographic Applications
Summary

• Introduction
• Features
• Design
• Architecture
• Performance Comparison
• Applications
ARE YOU NOT ENTERTAINED?
References


