IC-SOC Project
Crypto-Processor Core

Chih-Tsun Huang

Design Technology Center
National Tsing Hua University
Outline

- Overall Network Security Processor Architecture
- Crypto-Processor Core
- ACM (Asymmetric Crypto-Module)
- SCM (Symmetric Crypto-Module)
- Test Chip
Network Security Processor

- Applications: IPSec, SSL, VPN, etc.
- Functionalities:
  - Public (asymmetric) key: RSA, ECC
  - Private (symmetric) key: AES
  - Truly random number generator
- Target technology: $0.25\mu m$ to $0.18\mu m$
- Clock rate: 200MHz or higher (internal)
- 32-bit data and instruction word
- 10Gbps (OC192)
- Power: 1 to $10mW/MHz$ at 3V (LP to HP)
- Die size: $25mm^2$
- On-chip bus: AMBA
Crypto-Processor

- A coprocessor of NSP: scalable architecture
- Descriptor-based DMA interface

Diagram:
- DMA
- I Buffer
- O Buffer
- Channel#1
- Channel#2
- RSA/ECC
- AES
- Hashing
- RNG
- Other EU
- AHB-Lite
- Test Interface
- Power Manager
Encryption Modules

- ACM
  - Asymmetric crypto-module
  - Operations:
    - RSA
    - Modular multiplication of large numbers (1024 bits)

- SCM
  - Symmetric crypto-module
  - Operations:
    - AES
    - Matrix operations, manipulation

- RNG (Prof. T.-Y. Chang)
  - Random number generator
    - FIPS 140-1, 140-2 Security Requirements for Cryptographic Modules
An RSA cryptography engine with small area overhead and high speed
- 32-bit word-based modular multiplication
- Scalable word-width
- 34K gates
- 100MHz clock
- Scalable key length
A built-in self-diagnosis (BISD) to test 8 memory cores
Full-scan: 6 scan chains, each with 123 scan registers

<table>
<thead>
<tr>
<th>Technology</th>
<th>0.35 μm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>DIP 28 pins</td>
</tr>
<tr>
<td>Chip area</td>
<td>2.8 × 2.9 mm²</td>
</tr>
<tr>
<td>Die area</td>
<td>1.7 × 1.8 mm²</td>
</tr>
<tr>
<td>Gate count</td>
<td>34k</td>
</tr>
</tbody>
</table>
# RSA Benchmarking (Kbps)

<table>
<thead>
<tr>
<th>PC Platform</th>
<th>128 bits</th>
<th>256 bits</th>
<th>512 bits</th>
<th>1024 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-IV 1.8G</td>
<td>18.7</td>
<td>6.6</td>
<td>2.1</td>
<td>0.6</td>
</tr>
<tr>
<td>P-III 700M</td>
<td>8.0</td>
<td>2.8</td>
<td>0.83</td>
<td>0.23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clock rate f (MHz)</th>
<th>512 bits (1.79f/1000)</th>
<th>1024 bits (0.47f/1000)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>8.95</td>
<td>2.35</td>
</tr>
<tr>
<td>20</td>
<td>35.8</td>
<td>9.4</td>
</tr>
<tr>
<td>100</td>
<td>179</td>
<td>47</td>
</tr>
</tbody>
</table>
SCM

- AES cryptography
- 32-bit external interface
- 58K gates
- Over 200MHz clock
- Throughput: 2Gbps
- Support key length of 128/192/256 bits
## Test Chip

<table>
<thead>
<tr>
<th><strong>Technology</strong></th>
<th><strong>TSMC 0.25μm CMOS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Package</strong></td>
<td><strong>128CQFP</strong></td>
</tr>
<tr>
<td><strong>Core Size</strong></td>
<td><strong>1,279 x 1,271 μm(^2)</strong></td>
</tr>
<tr>
<td><strong>Gate Count</strong></td>
<td><strong>63.4K</strong></td>
</tr>
<tr>
<td><strong>Max. Freq.</strong></td>
<td><strong>250MHz</strong></td>
</tr>
<tr>
<td><strong>Throughput</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.977 Gbps (128-bit key)</td>
</tr>
<tr>
<td></td>
<td>2.510 Gbps (196-bit key)</td>
</tr>
<tr>
<td></td>
<td>2.169 Gbps (256-bit key)</td>
</tr>
</tbody>
</table>
# AES Benchmarking (Mbps)

<table>
<thead>
<tr>
<th>PC Platform</th>
<th>128 bits</th>
<th>192 bits</th>
<th>256 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-IV 1.8GHz</td>
<td>2.05</td>
<td>1.90</td>
<td>1.70</td>
</tr>
<tr>
<td>P-III 700MHz</td>
<td>0.80</td>
<td>0.71</td>
<td>0.66</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clock rate f (MHz)</th>
<th>128 bits (12.8f)</th>
<th>192 bits (10.67f)</th>
<th>256 bits (9.14f)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>64</td>
<td>53.3</td>
<td>45.7</td>
</tr>
<tr>
<td>20</td>
<td>256</td>
<td>213.3</td>
<td>182.8</td>
</tr>
<tr>
<td>100</td>
<td>1280</td>
<td>1066.7</td>
<td>914</td>
</tr>
</tbody>
</table>
CP Test Chip Spec

Clock Rate: 100 MHz (est.)

Test I/O: 32/24/17/11
Test Mode:
1. Functional
2. Muxed AES
3. Muxed RAS
4. Logic Test
5. Memory BIST

Test se from TestMode
Test_se[3:0]"\(^1\)
Test_out[3:0]"\(^2\)

For Scan test (8)

For PI500 (15)

MCK = HCLK
MBI from TestMode
MBR"\(^1\)
MBC"\(^1\)
MSI"\(^1\)
MBO"\(^2\)
MRD"\(^2\)
MSO"\(^2\)

*1,2: Shared IO