IC-SOC Project
Design Driver

Cheng-Wen Wu

Design Technology Center
National Tsing Hua University
Outline

- Overall Architecture
- AMBA (Advanced Microcontroller Bus Architecture)
- ACP (Asymmetric Crypto-Processor)
- AES (Advanced Encryption Standard)
Network Security Processor

- Applications: IPSec, SSL, VPN, etc.
- Functionalities:
  - Public key: RSA, ECC
  - Private key: AES
  - True 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 10\(mW/\text{MHz}\) at 3V (LP to HP)
- Die size: 50\(mm^2\)
- On-chip bus: AMBA
NSP Architecture

- CPU
- Local SRAM
- CP
- Local SRAM
- RAM
- Status Registers
- AHB Arbiter
- AHB MUXes
- AHB Decoder
- APB
- External Memory Interface
- DMA Controller
- Test Controller
- BIST

AMBA

Status
Registers

External
Memory
Interface

DMA
Controller

Test
Controller

BIST

icsoc2.8
AMBA

- Advanced Microcontroller Bus Architecture
- Standard system bus for ARM-based chip
- Open standard for SOC on-chip bus
  - Flexible and suitable for a wide range of SOC applications
AMBA Example
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**
  - Random number generator
    - FIPS 140-1, 140-2 Security Requirements for Cryptographic Modules
An RSA cryptography engine with small area overhead and high speed

- 16/32-bit word-based modular multiplication
- Scalable word-width
- 34K gates
- 100MHz clock
- Baud rate: 270K
- 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>
<tr>
<td></td>
<td>Key Size</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Yang</td>
<td>512</td>
</tr>
<tr>
<td>Su</td>
<td>512</td>
</tr>
<tr>
<td>Hong</td>
<td>512</td>
</tr>
<tr>
<td>Hsieh (8-bit)</td>
<td>512</td>
</tr>
<tr>
<td>Our design (16-bit)</td>
<td>512</td>
</tr>
</tbody>
</table>

NB is normalized baud rate.
□ is NB / gate count.
SCM

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

- AES architecture
  - Controller
  - Datapath
  - Key storage
- Both En/Decryption and Key Expansion are implemented
- All of the round keys are pre-computed
- AMBA interface
# Test Chip

<table>
<thead>
<tr>
<th>Process</th>
<th>TSMC 0.25µm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>128CQFP</td>
</tr>
<tr>
<td>Die Size</td>
<td>2.38×2.38 mm²</td>
</tr>
<tr>
<td>Pad</td>
<td></td>
</tr>
<tr>
<td>Ext. Power</td>
<td>10 pairs</td>
</tr>
<tr>
<td>Int. Power</td>
<td>8 pairs</td>
</tr>
<tr>
<td>Input</td>
<td>53</td>
</tr>
<tr>
<td>Output</td>
<td>39</td>
</tr>
<tr>
<td>RAM module</td>
<td>16×32(×4)</td>
</tr>
</tbody>
</table>