IC–SOC

Design Drivers
Update

Chih-Tsun Huang

Design Technology Center
National Tsing Hua University
Network Processing

Physical Layer

Network Processing Functions

Switching

Framing
Verification Classification
Modification
Encryption Compression
Traffic Queuing
Cores

- **CPU**: PKU (X Cheng)
- **DSP**: NTHU (YL Lin)
- **SRAM/ROM/Flash**: NTHU (CW Wu & YL Lin)
- **DRAM**: Industry
- **FPGA**: UCLA (J Cong)
- **CP**: NTHU (YL Lin & CW Wu)
- **On-Chip Bus**: UCSB/NTHU (KT Cheng & CW Wu)
- **LBIST**: UCSB (KT Cheng)
- **MBIST**: NTHU (CW Wu)
Network Security Processor

- **Applications:** IPSec, SSL, VPN, etc.
- **Functionalities:**
  - Public key: RSA, ECC
  - Secret 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 (OC196)**
- **Power:** 1 to 10\(mW/MHz\) at 3V (LP to HP)
- **Die size:** 50\(mm^2\)
- **On-chip bus:** AMBA
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
Encryption Modules

- PKEM
  - Public key encryption module
  - Operations:
    - Modular multiplication
    - Multiplication over GF(p) and GF(2^m)

- SKEM
  - Secret key encryption module
  - Operations:
    - Matrix operations, manipulation

- RNG
  - Random number generator
    - FIPS 140-1, 140-2 Security Requirements for Cryptographic Modules
PKEM

- 32-bit word-based datapath
- Support both RSA and ECC
- 40K gates
- 200MHz clock
- Baud rate: 270K
- Scalable key length
SKEM

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

2002
- Design of advanced encryption module
- FPGA prototyping
- Testchip of advanced encryption module

2003
- Performance evaluation
- Instruction set simulation
- FPGA prototype of first experimental architecture
- First testchip of NSP
- AMBA interface
- Encryption engine
- SRAM, register file
- Testing
- Analysis and evaluation

2004
- FPGA prototype of improved architecture
- System-level integration
- Testchip of advanced encryption module
- Second testchip
- ARM core
- Security processor
- Flash, SRAM
- Testing
- System-level integration

2005
- FPGA prototype of optimized architecture
- Testchip of advanced encryption module
- Final testchip
- Network security system chip
- Embedded DRAM
- Testing and integration

We are here