Computer Engineering Group
Professor Ming-Bo Lin

Ph.D., University of Maryland at College Park, U.S.A.
Field of study: Information Engineering and VLSI design.
Key words: VLSI、ASIC、SoC/SoPC、embedded systems design
URL: http://homepage.ntust.edu.tw/mblin /
Email: sanlee@et.ntust.edu.tw
Phone: 886-2-27376415(voice), 886-2-27376424(Fax)

1. The Subject and Aims of Research

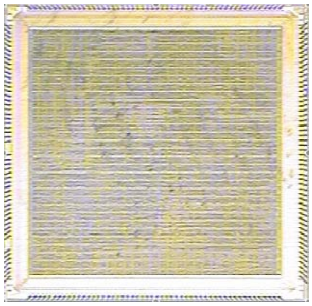
We have three major research areas:

(1). SoC platform IP design and development: design and develop SoC related platform IP, such as ARM v4/v5 and 6502 compatible IP.
(2). FPGA SoC platform (SoPC) application system design and development: Use FPGA SoC platform to design related application systems. The SoPC system is characterized by the codesign of both hardware and software so as to optimize the system performance and reach a cost-effective result.
(3). Dedicated ASIC IP design: data compression/decompression chip, Viterbi decoder IP, RSA encryption/decryption IP, AES encryption/decryption IP, ECC encryption/decryption IP, IEEE 1394 data link IP high-speed USB peripheral controller IP.

2. Related Recent Research Topics

(a). An ARM v4 ISA compatible CPU IP and related peripheral modules

In this research, we design an ARM v4 ISA compatible CPU IP and related peripheral interface modules. The design includes an ARM v4 ISA compatible microprocessor IP, an AMBA bus controller and most widely used peripherals, such as the memory interface, an interrupt controller, a DMA controller, 32 GPIO ports, a UART controller, a programmable PWM controller, and a 32-bit timer.

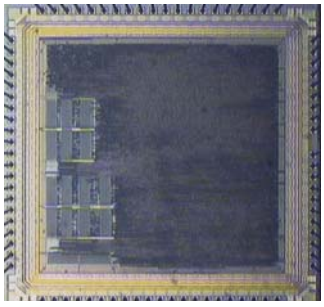


Process	TSMC 0.35μm 2P4M
Package type	CQFP 208
Die area	5. 434×5.434 mm²
Core area	4.704×4368 mm²
Gate count	94, 131
Power dissipation	179~191 mW

(b). A scalable elliptic curve encryption/decryption IP

In this research, two scalable elliptic curve encryption/decryption IP (Intellectual Property) blocks are presented, which are parametric scalable architecture and scalable architecture, respectively. The hardware of parametric scalable architecture is regular. Arbitrarily key-sized soft IP of parametric scaleable architecture can be generated by using high-level program with given input parameters. The soft IP of scalable architecture refers to a dedicated design of the hardware with a fixed maximal key size. Hence, it has better performance although it has less regularity. All of the IP carry out the projective version of the Montgomery scalar multiplication algorithm with polynomial-basis representation.

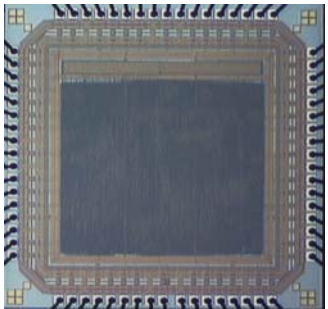
The result of a scalable encryption/decryption chip whose maximal key size is 256 bits is shown in the following die photo. The chip has a flexible interface for interfacing with common microprocessors, and the data bus width can be set to 8, 16, 32 bits suitable for all kinds of bus width of modern microprocessors.



Process	TSMC 0.35μm 2P4M
Package type	84-pin CLCC
Die area	3. 633×3.633 mm²
Core area	2.723×2.723 mm²
Gate count	61,406
Power dissipation	716 mW
Operating frequency	125 MHz
Data rate	42 kbps @ 256-bit key

(c). An AES plus CBC mode encryption/decryption IP

In the research, a pipelined architecture of AES plus CBC Encryption/Decryption IP (Intellectual Property) is proposed. This architecture implements the AES algorithm, the input data is a sequence of 128 bits and the cipher key may be a sequence of 128, 192, or 256 bits. To provide the flexibility of interfacing with common microprocessors,

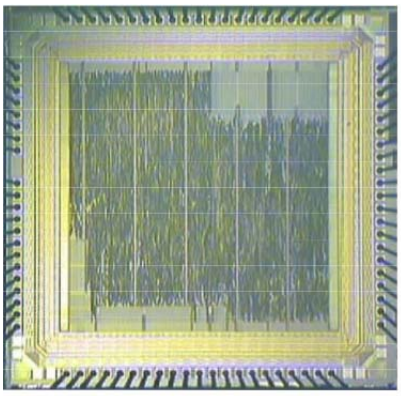


Process	TSMC 0.25 μm
Package type	68-PIN CLCC
Die area	2,550 μm × 2,550 μm
Core area	1,672 μm × 1,672 μm
Gate count	76,610
Data rate	1.2 Gbps
Operating frequency	156.25 MHz
Power dissipation	128 mW

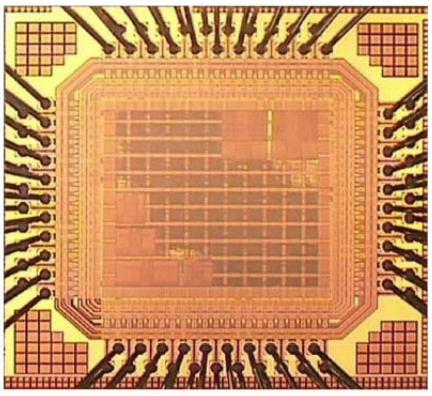
the data bus width can be set to 8, 16, or 32 bits; to provide the AES IP in a variety of applications, four “modes of operation” (ECB, CBC, CFB, and OFB) have been defined in the IP. A Key Schedule is employed to produce the set of Round Keys required for every data blocks and store in RAM before the encryption or decryption of input data. Thus, it may save some of the power dissipation. Compared with the widely used lookup-table architecture, the Euclid’s multiplicative inverse lookup-table architecture employed in the research may reduce the hardware overhead of the S-box and InvS-box by an amount of 36.45%.

(d). A data compression and decompression algorithm design and its related VLSI architecture designs and implementation

In this research, we propose a multilevel lossless data compression architecture that combines the PD-LZW algorithm and an approximated adaptive Huffman algorithm. In the first stage, PD-LZW algorithm is used for speeding up the compression rate by changing the data unit of compression from byte to byte stream; in the second stage, the approximated adaptive Huffman algorithm that uses an ordered list to simulate the tree-based adaptive Huffman algorithm is used, which also speeds up the compression and decompression rate. Besides, throughput in compression can be superior to our previous worked result by at most 25% by using scheduling and allocation algorithms, and the resulting hardware can also share 710-byte CAM memory, 11.25-byte registers and 29-byte ROM.



(a) TSMC 0.35 μm 2P4M process



(b) TSMC 0.18 μm 1P6M process

Process	TSMC 0.35 μm 2p4m	TSMC 0.18 μm 1p6m
Package type	LCC 84	LCC 84
Die area	2.9 mm × 2.9 mm	1.6 mm × 1.6 mm
Core areas	2.2 mm × 2.2 mm	1.2 mm × 1.2 mm
Data rate (bps)	266 M to 1.33 G	532M to 2.66 G
Operating Frequency	100 MHz	200 MHz
Power dissipation	394/333 mW	288/232 mW

3. Selected Projects

1. NSC project: The Development and Design of an Embedded Hardware Platform and its Integrated Design Environment (I) (NSC 92-2213-E-011-062).
2. NSC project: The Development and Design of an Embedded Hardware Platform and its Integrated Design Environment (II) (NSC 93-2213-E011-048).
3. NSC project: The Design and Implementation of a USB OTG Chip and USB Speaker (NSC 95-2221-E011-049)

4. Selected Publications

1. **Ming-Bo Lin**, Jang-Feng Lee, and Gene Eu Jan, "A lossless data compression and decompression algorithm and its hardware architecture," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, Vol. 14, No. 9, pp. 925-936, 2006.
2. **Ming-Bo Lin** and Yung-Yi Chang, "A new architecture of a two-stage lossless data compression and decompression algorithm," submitted to *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, (2007 March).