計算機組

林銘波教授

美國馬里蘭大學博士

研究領域：資訊工程、超大型積體電路設計

關 鍵 字：VLSI、ASIC、SoC/SoPC、嵌入式系統設計

網　　頁：http://homepage.ntust.edu.tw/mblin/

電子郵件：mblin@et.ntust.edu.tw

電　　話：02-27376415

一、研究主題與目標

目前的主要研究方向主要分成三大部分：

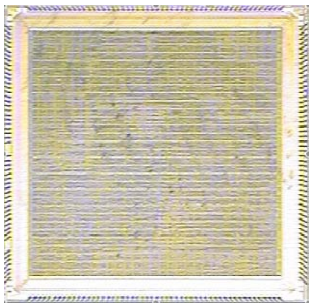
1. SoC 平台技術 IP 設計與發展：設計與研發 SoC 平台相關 IP，例如 ARM v4/v5 與 R6502 相容 IP。
2. FPGA SoC 平台(SoPC)/嵌入式系統應用設計與發展：使用 FPGA SoC 平台或是嵌入式系統設計與研發應用系統。此系統之特性為結合軟體與硬體整合設計，以求得最佳之系統性能及成本。
3. 專用 ASIC 設計：資料壓縮/解壓縮、Viterbi 解碼器、RSA 加解密 IC、AES 加解密 IC、ECC 加解密 IC、IEEE 1394 資料連結層 IP 、高速 USB 周邊控制器 IP。

二、最近研究題目

1、ARM v4 ISA 相容微處理器智產產生器

本研究設計一個與 ARM v4 ISA 相容的微處理器智產極其相關的周邊裝置界面。在本設計中包括相容於 ARM V4 指令集之微處理器，並以相容於 AMBA 2.0 匯流排標準控制器將常用周邊整合為一嵌入式系統發展平台。周邊則包括記憶體介面、中斷控制器、提供 4 組通道之 DMA 控制器、支援 32 個可規劃輸出入埠 (General Purpose Input Output, GPIO)、標準 UART、4 組 PWM 通道以及 32

位元計時器等。



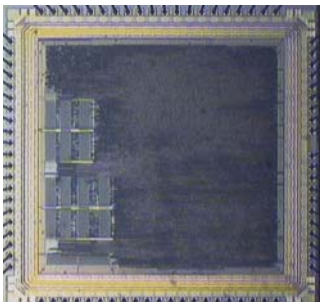
製程	TSMC 0.35μm 2P4M
包裝種類	CQFP 208
晶片面積	5. 434×5.434 mm^2
核心面積	4.704×4368 mm^2
閘數量	94, 131
消耗功率	179~191 mW

2、可調式橢圓曲線加解密智產

本研究設計兩種可調式橢圓曲線加解密智產，其中一種為參數化可調式架構，另一種為可調式架構。參數化的硬體架構具規則性，只需輸入參數，即可利用高階程式產生出任意金鑰長度的軟智產；可調式架構，則以最大金鑰長度為基準設計軟智產，其硬體架構較不具規則性，但是因為係針對單一金鑰長度設計而成，因而效能較佳。兩種智產架構皆在投影座標下，進行蒙哥馬利橢圓曲線純量積運算，並且採用多項式基底表示法來表示純量積運算中的有限場元素。

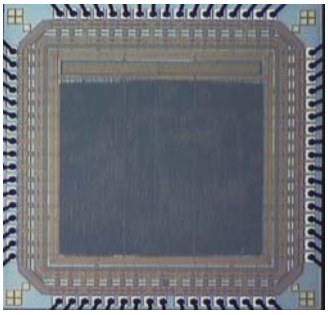
下圖為以硬體最大金鑰長度為 256 位元的可調式加解密晶片。該晶片具有與微處理器相容的控制介面，資料匯流排寬度有 8 位元、16 位元以及 32 位元三種設定模式，提供使用者搭配各種微處理器介面使用。

製程	TSMC 0.35μm 2P4M
包裝種類	84-pin CLCC
晶片面積	3. 633×3.633 mm^2
核心面積	2.723×2.723 mm^2
閘數量	61,406
消耗功率	716 mW



3、AES 內建 CBC 模式加密與解密智產

在本研究中提出了一個具有管線(pipeline)架構的 AES plus CBC 加解密軟智產。依據 AES 演算法，此加解密晶片的每一筆輸入資料為 128 位元，金鑰長度則可以選擇為 128 位元、192 位元、或是 256 位元。晶片的使用者介面相容於微處理機的資料匯流排，可操作於 8 位元、16 位元以及 32 位元三種模式，並且內建了 ECB、CBC、CFB 以及 OFB 四種操作模式，供使用者彈性的依據實際情況選擇適合的操作模式。在本晶片的設計中，對於每一筆資料輸入所需的子金鑰使用金鑰擴展程序在加解密前事先產生，然後儲存於 RAM 中，並不需反覆計算相同的子金鑰，因此可以降低功率的消耗。在位元組替代轉換部分，利用歐幾里得演算法建立一個新的乘法反元素替換表，取代原本的 S-box 與 InvS-box，如此約可以減少 36.45%的面積。

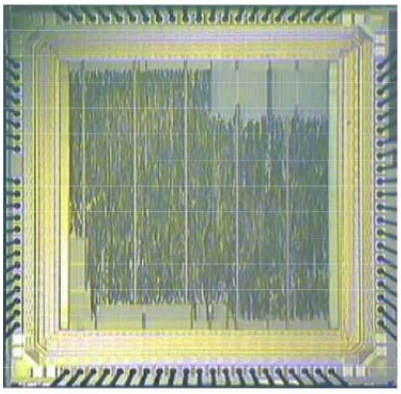


製程	TSMC 0.25 μm
包裝種類	68-PIN CLCC
晶片面積	2,550 μm × 2,550 μm
核心面積	1,672 μm × 1,672 μm
閘數量	76,610
資料速率	1.2 Gbps
工作頻率	156.25 MHz
消耗功率	128 mW

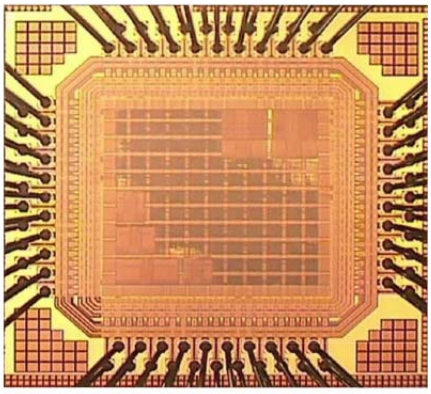
4、資料壓縮與解壓縮演算法與 VLSI 架構設計

在本研究中，我們論採用二階層無失真資料壓縮/解壓縮演算法，它結合了 PD-LZW 演算法及近似動態霍夫曼演算法。第一層的 PD-LZW 演算法將輸入資料處理單位由 LZW 演算法的字元改為字串，使壓縮與解壓縮速度可以獲得大幅提升。並將字典使用靜態記憶體取代大部分 CAM 的架構，並在之後加入一級 FIFO 以補償因為尋找匹配字串所花費的時間；第二層使用的近似動態霍夫曼演算法，採用兩個靜態記憶體來實現符號出現機率的排序串列以代替動態霍夫曼演算法的樹狀架構，也使得壓縮與解壓縮速度可利用管線加快。將壓縮與解壓縮硬

體架構資源共用後，共使用 112 位元組的 CAM、1048 位元組的 SRAM 與 29 位元組的 ROM。



(a) TSMC 0.35 μm 2P4M process



(b) TSMC 0.18 μm 1P6M process

製程	TSMC 0.35 μm 2p4m	TSMC 0.18 μm 1p6m
包裝種類	LCC 84	LCC 84
晶片面積	2.9 mm × 2.9 mm	1.6 mm × 1.6 mm
核心面積	2.2 mm × 2.2 mm	1.2 mm × 1.2 mm
資料速率(bps)	266 M to 1.33 G	532M to 2.66 G
工作頻率	100 MHz	200 MHz
消耗功率	394/333 mW	288/232 mW

三、主要的研究成果與所執行的計劃

1. 國科會研究計畫，*嵌入式系統硬體平台開發與整體發展環境設計*(Ⅰ)(I) (NSC 92-2213-E-011-062)。
2. 國科會研究計，*嵌入式系統硬體平台開發與整體發展環境設計* (NSC 93-2213-E011-048)。
3. 國科會研究計，USB OTG 晶片設計與 USB 播放系統設計與實作（Ⅰ)(NSC 95-2221-E011-049)

四、重要的研究成果相關論文發表

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).