行政院國家科學委員會專題研究計畫　期中進度報告

具安全考量之可重組式大量資料流運算架構(1/3)

計畫類別：個別型計畫
計畫編號：NSC94-2213-E-009-114-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：國立交通大學資訊工程學系(所)

計畫主持人：鍾崇斌
共同主持人：單智君
計畫參與人員：蔣昆成、汪威定、陳逸麒、張華鼎、陳群旻、黃伯仁、喬偉豪

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 95 年 6 月 1 日

一、中英文摘要：

1.中文摘要

關鍵詞：計算機架構、可重組式計算、軟/硬體協同設計、加解密電路、硬體重組設定編譯器

隨著電子產業的重心由個人電腦轉移至消費性電子產品，系統單晶片成為目前晶片設計上最重要的課題。各式各樣的消費者需求使得消費性電子相較於傳統的個人電腦需要更多樣化的產品發展。可重組式計算提供兼具彈性與效能考量之解決方案，可以有效的縮短研發上的時程甚至可以在晶片生產完成之後仍然具有可修改運作功能的特性。因此，我們選定可攜式產品必備的加解密應用為我們設計的基礎，研究適合大規模資料運算的可重組式計算架構。本研究計畫預計以三年的時間，研究可重組式計算架構的軟/硬體整合環境，包括：

- 應用分析：分析加解密演算法與龐大資料運算的應用，以研究其加速的潛能與重組的流程
- 硬體設計：研究可重組式架構、運算單元、資料流網路與重組設定網路之設計。
- 軟體設計：研究支援硬體重組與軟/硬體程式分割之編譯器，並發展其整合設計環境。

在第一年的計畫執行期間，我們分析各個加解密演算法的運算結構與特性。根據這些特性，我們設計的一個可行的可重組式計算架構。更進一步地，使用 Verilog 硬體描述語言將此設計的概念實作為實際的電路。並利用 Synopsys 公司所提供的硬體合成工具轉換為實際的台積電 0.35um 半導體製程的基礎元件組合。為了比較實際的研究成效，我們亦設計一個以一般晶片設計流程所完成的客製化電路。根據實驗結果，我們所設計的可重組式計算架構，可以有效的減少執行相同運算的硬體效能成本。最後，我們將此研究成果彙整分析後投稿於今年三月二十一日至三月二十四日所舉辦的國際學術會議 ACM Symposium on Information, Computer and Communications Security (ASIACCS'06)，並於當次會議期間發表本論文研究成果。

2.計畫英文摘要

Key Words: Computer Architecture, Reconfigurable Computing, HW/SW co-design, Cryptographic Hardware, Hardware Configuration Compiler

According the trend of electric industry, instand of the personal computer products the consumer electronics becomes the main stream of the industry. As a result, system on a chip is the most important topic in the design of a product. The consumer electronic products need more diversifrom style to fit with various requirements of many kinds of customers compare with the personal computer products. The reconfigurable computing provides a flexible solution make a product to satisfy the elasticity and computing performance of a product. Indeed, the schedule of the product development is extremely reduced and the product remains adjustable even though it is completed with its production. For this reason, we choose the cryptographic application, the most essential function on portable devices, as the base design of ours.

We will research into the architectures of reconfigurable computing that are suitable for the computations of streaming data. In this project, we expect to research the integrated environment of reconfigurable computing in three years. The main researches are:

- Application analysis: analyze the applications of cryptographic and streaming data, explore the possibility of speedup and research the flow of reconfiguration.
- Hardware design: the design of the architecture of reconfigurable computing, the processing elements, the dataflow networks and the configuration network.
- Software design: the research of compiler that support reconfigurable computing and hardware/software partition; develop the integrated environment of application design.

In the first year of this research project, we analyze the computing structures and features of each cryptographic algorithm. According to the result of analysis, we design a workable reconfigurable architecture. Moreover, we use the Verilog hardware description language to implement this design concept into realistic circuit design. A tool provided by Synopsys Inc. is used to synthesize the design into a real circuit with TSMC 0.35um fabrication processes. In order to compare the effects of this project, we also designed a circuit using a tradition design flow called custom design. The experimental result indicates that the reconfigurable architecture has better cost effective performance compared with custom design. Finally, we collect the result of our simulation and publish a research paper in the conference ACM Symposium on Information, Computer and Communications Security (ASIACCS'06) held in March 21-24, 2006.

二、研究內容：

1.前言

目前電子產業的趨勢，已經從個人電腦漸漸將重心轉移到消費性電子產品上。為了迎合世界上各式各樣的消費者需求與屬性上的差異，消費性電子相較於傳統的個人電腦需要更多樣化的產品發展而非一致性的少樣多量。另一方面，消費性電子產品更進一步走向體積小功能精巧且省電的可攜式產品(Portable Device)特性，利用電池供應產品運作時所需要的電能供應。在這樣的消費性電子的蓬勃發展，系統單晶片(System-on-a-Chip, SoC)便隨之成為電子產業的主流發展。歸功於半導體技術的發展，系統單晶片最主要的優點即是將系統中所需要的各種零組件透過新一代的半導體技術整合在單一製程的單一晶片上。顯而易見的這樣的發展可以讓以往需要多個晶片才能整合設計完成的產品，輕易的實現在僅僅數平方公分的面積上，這樣的發展可以達成消費性電子的體積小與省電的的需求。然而，對於消費者的多樣化需求卻因為半導體標準化的流程而無法快速的達到這些需求。以目前的晶片設計與半導體製作的時間，一個新的產品往往需要半年到一年半的研發生產。也就是當研發人員或市場規劃人員眼見消費者的新需求，必須經過半年至一年半才有辦法將這個產品生產完成。

眼見消費者的需求與供應商提供所需產品有半年以上甚至一年半的差距，我們認為可重組式運算(Reconfigurable Computing)技術可以有效的縮短研發上的時程甚至可以在晶片生產完成之後仍然具有可修改運作功能的特性。在消費性電子產品上，可重組式運算架構配合系統單晶片的技術可以成為未來產品設計上的主流。除此之外，個人電子產品相對地擁有更多的個人化資料甚至隱私資料，對於資訊保密的要求也更高。例如，當兩位使用者想要使用個人數位助理(PDA)想要透過 GPRS 甚至 CDMA 互相交換私人資料，由於這個資料需要透過公共網路傳輸我們必須確保在傳輸的過程不會遭受惡意的使用者竊取解讀這些資料。本計畫首先針對三個目前最為廣泛使用的加解密演算法：DES, AES, 與 RSA 分析其運算的特性，並設計相對應的運算單元及可重組式架構。我們將以三年的時間，探討加解密演算法與可重組式計算的結合以提供適合消費性電子產品的系統架構。

2.文獻探討

在可重組式計算的技術中，以傳統的 FPGA(Field Programmable Gate Array)架構最具代表性[1-2]，其架構是以 CLB (Configurable Logic Block)為基礎的運算單元，每個 CLB 的運算能力為單一位元的運算，此架構的優點經由適當的重組這些 CLB 便可以執行任意的運算型態。由於每個 CLB 僅能執行單一位元的運算，在實際的應用上這些 CLB 透過複雜的連結網路相互連接才有能力執行較大位元數的運算。因此，由於這些連結網路所形成的龐大繞線體積造成了 FPGA 在效能上的限制與使用效率的降低。同時，每一個 CLB 必須擁有其個別的重組設定（Configuration），大量的重組資料與重組時間亦限制其應用的變化性。目前，FPGA 多應用於發展產品原形，極少使用於 SoC 的產品。

先進的高效能可重組式架構，如:GARP[3], PRISC[4], Raw[5], PipeRench[6]等，其設計針對通用性質(General Purpose)且高效能的分散式運算。此種架構之可重組式計算，運用軟/硬體的分割技術將程式切割為多個獨立的運算程序，並將這些運算程序分派於各個高效能的運算單元。這些高複雜性的運算單元相當於精簡指令的微處理器(Micro Processor)，相對地，為了同時服務這些運算單元的大量資料需求，其記憶體階層的設計與高頻寬的匯流排需求使得硬體電路無法整合於系統單晶片之上。因此，雖然其運算單元擁有相對更高位元組的運算能力，其運用龐大的晶片面積來提升高效能

平行運算，無法適用於消費性電子的精巧省電的產品特性。

在現今的 SoC 應用上，消費性電子產品在資料傳輸上的保密性具有舉足輕重的地位。這些產品透過網路傳輸達到訊息交換、網路交易等加值應用。為了防止個人資料在開放的網路環境遭受惡意的竊取或盜用個人身份，必須應用加解密的演算法提供資料傳輸上的保密性。目前，SoC 應用為了加速這類的加解密演算法，必須整合獨立的加解密加速電路。然而，使用者的使用特性是大部分的時間上使用非機密的應用，如：收發 e-mail、觀看網頁等，造成獨立的加解密加速電路的閒置形成資源浪費。我們利用重組式邏輯電路，在 SoC 產品進行資料傳輸時，提供快速的硬體進行加解密運算。此外，當使用者不需要傳遞機密資料時，可重組式邏輯可以重設為其他應用，如：Video Display、MPEG-4、MP3 Audio Encode/Decode 等，同時亦可提供大量資料運算的加速。

近年來嵌入式系統與消費性電子產品的迅速發展，快速的產品汰換與高執行效能的要求即為成功的產品的基本條件。在研發時程與效能需求的雙重壓力下，可重組式計算的觀念益顯重要。可重組式計算利用其可重設的處理單元(Processing Element, PE)與可重設的資料流網路，快速的切換不同的應用於相同的可重組式邏輯上。可重組式計算對於系統單晶片應用具備下列優點：

- 縮短產品研發時程，
- 多樣性應用，與
- 適用於大規模運算之加速。

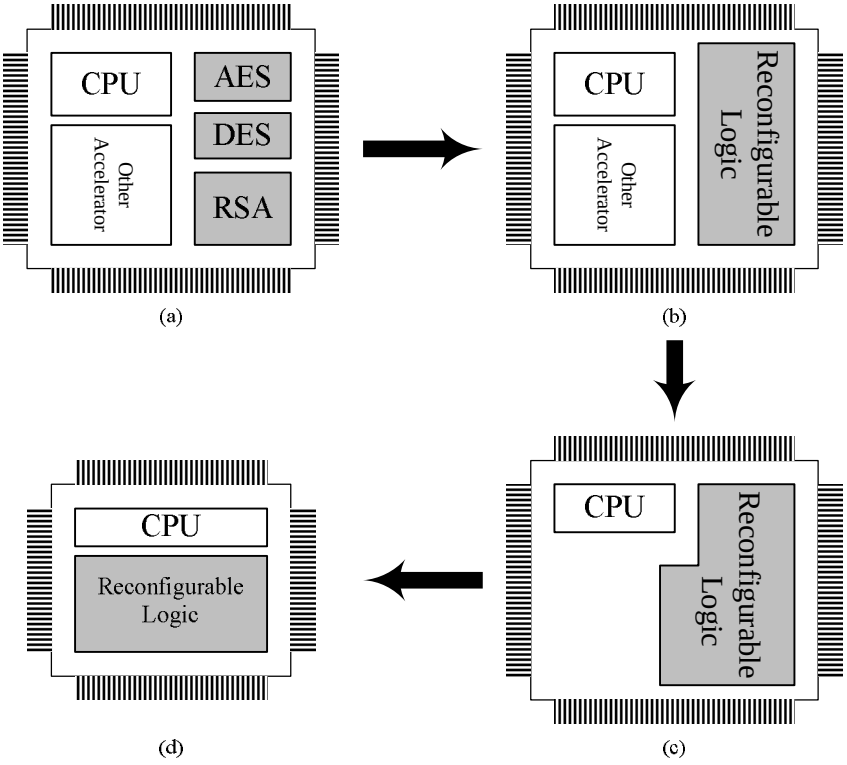
目前，可重組式計算架構已成功的應用於實現即時影音播放、combinatorial search[8]、與 stream processing 等多項應用中。

3.研究方法

加解密演算法可分成兩大類，一為對稱演算法，另一個為非對稱性演算法，對稱性密碼學的概念早已使用的好幾千年，它擁有很多方式，從簡單的代換到複雜的建構方式，這類的演算法通常加密端與解密端會使用同一把金鑰(Key)，雙方都利用這把金鑰進行動作，這類的演算法通常非常快速，但是卻容易受攻擊，主要就是因為雙方都使用相同的金鑰，如果金鑰落入壞人的手中，那麼就會馬上徹底地危及使用該密鑰加密的資料的安全性。現有較常使用的對稱演算法有 DES (Data Encryption Standard), AES (Advanced Encryption Standard)。相較於對稱性演算法，非對稱性演算法沒有這樣的問題，一般非對稱演算法都會有兩把金鑰，一為公鑰，另一為私鑰，只要利用其中一把公鑰做加密運算，就只能用另外一把私鑰做解密運算。一般來說其中私鑰由一個人秘密保管，不需分享，因此可以避免安全性的考量，而另外一把公鑰就儘量讓大家知道，也就是因為加密解密的使用的金鑰不一樣，因此稱這類的演算法為非對稱加密演算法。這類演算法最負盛名的為 RSA 系統[9]。

我們提出的可重組式計算的架構適量提高運算單元的運算資料位元數，減少繞線佔晶片面積的比例並縮短重組時間，提高可重組式架構應用於系統單晶片的可行性。我們將運算單元的資料位元數，由 CLB 的單一位元提高八位元或三十二位元的運算能力，並定義所需的運算功能，如：加法、位元互換…等運算。經過運算能力的提升，原本在 CLB 間為了執行相同的運算所產生的區域資料網路，成為運算單元的內部網路。相對地，因為資料流網路用於傳遞運算單元間的資料，大量減少的繞線的需求。同時，在單一運算單元中，多個位元的運算僅共用相同的重組設定，而非個別位元運算使用獨立的重組設定。在此情況下，不僅減少了可重組式邏輯所需的重組設定記憶體及重組所需的時間，更進一步地減少了編譯後的程式大小。

本計畫運用可重組式計算之技術，將 DES、AES、RSA 等加解密演算法合併為單一的可重組式邏輯，以達到縮減晶片面積與減少耗電量。更進一步地，將該可重組式邏輯延伸到大量運算的應用並考量軟硬體分工的協同設計以擴充 SoC 的功能性。如圖一所示，其中(a)為目前的 SoC 晶片架構，對於個別的應用必須設計獨立的加速電路。首先，我們針對加解密的運算設計可重組式邏輯電路。如(b)所示，經過特化過程後可重組式邏輯可輕易的取代原本加解密的三種不同運算。同時，因為其運算的特性屬於大資料量運算，透過適度的修改後，可重組式邏輯亦能擔任其他運算加速的工作。如(c)所示，可重組式架構經過修改雖然增加了部分的面積，但是其優點是可以完全取代其他的運算加速電路。最後，如(d)所示，可重組式邏輯取代其他加速電路，因此晶片中的其他電路可以節省，進一步縮小 SoC 晶片面積並減少耗電量。



圖一、利用可重組式計算架構擴展應用並減少晶片面積

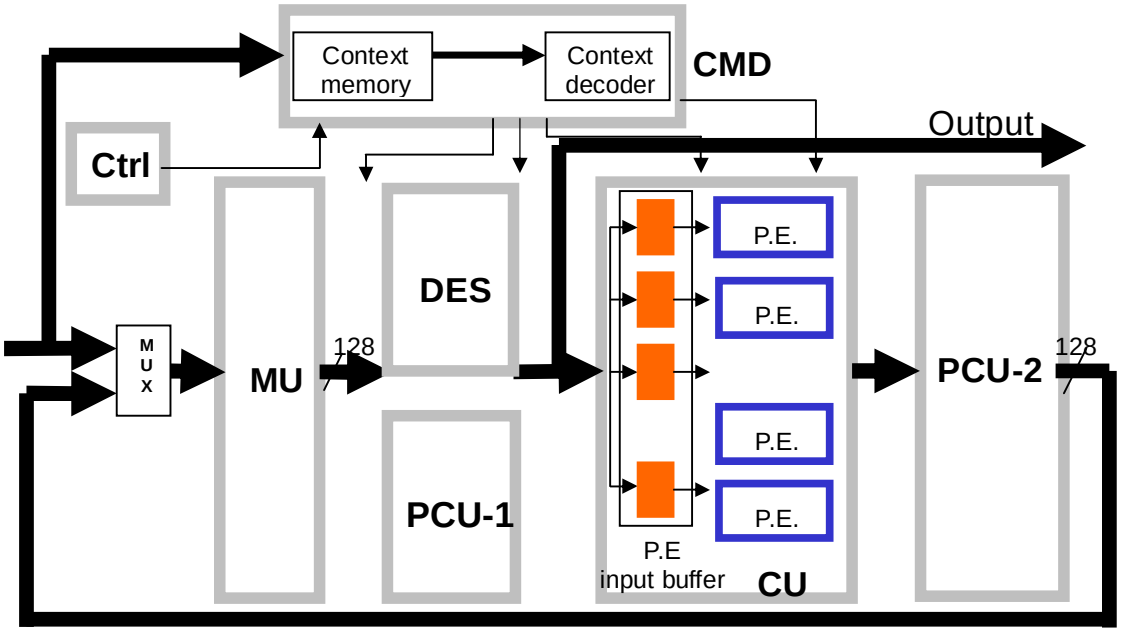
本計畫對可重組式計算的設計上，以下列為主要目標：

- 設計可重組式架構，研發多用途的 SoC 晶片。
- 研發軟硬/體協同工作的設計流程，以縮短研發時程並建立快速發展的 SoC 架構。
- 針對加解密演算法，特化 PE 的功能以加速執行效率。
- 利用特化後 PE 的結構，應用於一般上大資料量運算之加速。
- 動態調整效能與降低執行應用所需的耗電量。
- 減少時間與空間的乘積量。

4. 研究成果與討論

在第一年的計畫執行過程中，我們首先針對加解密演算法進行運算結構的統計與分析。如圖二所示，我們提出一個可重組式計算的架構整合了運算處理單元陣列、位元交換與重置單元、記憶體

控制單元與重組控制單元。我們將基本的運算單元運算能力設定為八個位元，各個運算單元透過縱向的網路連結可以擴充為更大位元字組的運算單元，以配合執行 RSA-1024 演算法中所需要的 1024 位元加減法運算的需求。針對對稱性的加解密運算，我們特化的兩個位元交換與重置單元(PCU-1, PCU-2)，對於各種的位元交換順序可以輕易的經由重組設定的變換來達成需求的運算。而 DES 單元則是特別針對 Data Encryption Standard 演算法所設計出來的單元，它可以簡化 DES 演算法的重組設定複雜度，更可以適度的加速整體的運算效能。記憶體控制單元(MU)則是負責於中央處理器溝通並取得所需要加密或解密的的資料與金鑰，並在運算過程中提供暫存資料的存放空間。而重組內容記憶體與解碼器(CMD)則是負責接收由中央處理器所傳送過來的重組資料並在適當的時機切換各個單元的運作功能，藉以完成中央處理器所交付的工作。



圖二、應用於加解密應用之可重組式計算架構

依據上述我們所提出的可重組式架構，我們使用 Verilog 硬體描述語言將實際的電路予以實作並配合台積電公司的 0.35um 半導體製程與 Synopsys 公司的電路合成軟體將本架構轉換為 Cell-Based 設計進一步分析評估其運作效能與可行性。另一方面，為了檢視我們所提出的架構相較於現今客製化設計流程所設計完成的產品間的執行效能與晶片空間上的優劣之處。我們仿造現有的加解密電路設計出在相同的電路並在相同的製程技術下評比。以晶片面積與執行時間的乘積為比較標準之下，我們的可重組架構只需客製化流程所設計出的產品百分之七十八的硬體成本便可以達到相同的執行效能。最後，我們將此研究成果彙整分析後投稿於今年三月二十一日至三月二十四日所舉辦的國際學術會議 ACM Symposium on Information, Computer and Communications Security (ASIACCS'06)，並於當次會議期間發表本論文研究成果[10]。

5. 計畫成果自評

本計畫預計在為期三年的計畫期間內，針對可重組式計算架構應用在消費性電子的產品之安全機制上的可行性進行研究。重要研究議題有：(1)加解密演算法的分析，包括 DES, AES, RSA、(2)軟/

硬體協同工作的設計方法；(3)可重組式架構設計，包括資料流網路設計、重組設定網路的設計、微處理器與可重組邏輯間介面的設計；(4)運算單元之硬體設計與實作，針對加解密演算法對運算單元特化；(5)延伸至大量運算應用的運算單元之設計與實作；(6)低耗能的設計。在第一年的計畫執行期間，我們不僅針對加解密演算法進行分析並設計出初步可行的硬體架構。對此架構進行的設計成效進行成果的分析，我們發現以可重組式架構所設計之硬體可以有效的提高的成本效能亦即用較少的硬體成本便可以達到相同的執行效能。比較研究的內容與原計畫的相符程度，在此一年的時間內我們依據這個計畫所設定的項目逐步完成設定的目標，相符程度幾乎趨近於百分之百。除此之外，我們將此研究成果彙整分析後投稿於國際性學術會議並獲得刊登於該會議論文集中，達成的預期的研究目標。

本計畫針對消費性電子產品的應用提出可重組式計算之架構，執行該應用對於加速產品的研發速度、提高產品多樣性、降低研發成本與提升產業競爭力具有積極的幫助。消費性產品為了因應消費者的快速汰舊換新的習性，必須於短時間內發展各式各樣的產品，以迎合消費者的需求。可重組式計算可以針對相同類型的應用提供單一的系統單晶片，廠商可以透過軟/硬體整合的環境，快速地特化新型產品而避免重新研發專用硬體電路的曠日廢時。不僅可以加速新產品所需的研發時程，同時亦可針對不同的客戶客製化其個性化的商品。此外，廠商對於開發新產品必須承受產品失敗的風險，而這些風險無形的也成為業界最大的負擔，所有失敗的產品無形的都成為其他產品的成本負擔。業界平均的研發概況約十個產品只會有一個產品成功，換句話說，大約一個成功的產品約需十倍的研發成本。然而，透過可重組式計算的架構，廠商無須針對新產品開發新的 SoC 晶片，可以將可重組式架構透過軟體的修改其重組設定，而產生新型產品。這些快速且低成本的 SoC 解決方案，可以大幅提昇產業的競爭力。

參考資料

[1] M. Platzner, “Reconfigurable accelerators for combinatorial problems,” IEEE Computer, Vol. 33, No. 4, pp. 58-60, 2001.

[2] M. McLoone and J. McCanny, “High performance single-chip FPGA Rijndael algorithm implementations,” in Proc. CHES, 2001, pp. 68–80.

[3] J. Hauser, and J. Wawrzynek, “Garp: A MIPS Processor with a Reconfigurable Coprocessor,” Proc. IEEE Symp. Field-Programmable Custom Computing Machines, 1997.

[4] Andr’e DeHon: Reconfigurable Architectures for General-Purpose Computing, A.I. Technical Report No. 1586, Massachusetts Institute of Technology. 1996

[5] M. B. Taylor, “The Raw Processor: A Scalable 32 bit Fabric for General Purpose and Embedded Computing,” Proceedings of 13th Hotchips Workshop, August 21, 2001

[6] S. C. Goldstein, et. al., “PipeRench: A Reconfigurable Architecture and Compiler,” IEEE Computer , 2000

[7] W. Tsu et al., “HSRA: High-Speed, Hierarchical Synchronous Reconfigurable Array,” Proceedings of 7th International Symposium on Field-Programmable Gate Arrays, 1999.

[8] E. Caspi, et. al., “Stream computation organized for reconfigurable execution (SCORE): Introduction and Tutorial,” Proceeding of 10th Int’l Conf. Field-Programmable Logic and Applications, 2000

[9] SRIVATHS RAVI and ANAND RAGHUNATHAN NEC Laboratories America PAUL KOCHER Cryptography Research and SUNIL HATTANGADY Texas Instruments Inc.” Security in Embedded Systems: Design Challenges” 2004

[10] Keun-Cheng Chiang, Zhi-Wei Chen, and Jean Jyh-Jiun Shann, “Design and Implementation of a Reconfigurable Hardware for Serure Embedded Systems”, ACM Symposium on Information, Computer and Communications Security (ASIACCS’06)