

申請日期	91.9.27
案 號	91122363
類 別	G06F15/16

A4

C4

(以上各欄由本局填註)

發 明 專 利 說 明 書 I223751 新 型		
一、發明 新 名稱	中 文	用以執行模組乘法之方法及裝置
	英 文	METHOD AND APPARATUS FOR PERFORMING MODULAR MULTIPLICATION
二、發明 人 創作人	姓 名	麥克 D. 洛霍 MICHAEL D. RUEHLE
	國 籍	美國 U.S.A.
	住、居所	美國加州聖地牙哥市唯那諾街 12022 號 12022 VERANO COURT, SAN DIEGO, CALIFORNIA 92128, U.S.A.
三、申請人	姓 名 (名 稱)	美商英特爾公司 INTEL CORPORATION
	國 籍	美國 U.S.A.
	住、居所 (事務所)	美國加州聖塔卡拉瓦市米遜大學路2200號 2200 MISSION COLLEGE BOULEVARD, SANTA CLARA, CALIFORNIA 95052, U.S.A.
	代 表 人 姓 名	湯姆士 C. 雷納德 THOMAS C. REYNOLDS

(由本局填寫)

承辦人代碼：
大類：
I P C 分類：

A6
B6

本案已向：

國（地區） 申請專利，申請日期： 案號： ，☐有 ☐無主張優先權

美國 2001年09月28日 09/965,916 ☒有☐無 主張優先權

有關微生物已寄存於： 寄存日期： ，寄存號碼：

裝
訂
線

五、發明說明 (1)

發明背景

發明領域

本發明一般而言係關於算術處理及密碼學的領域。更特定而言，本發明係關於一種用以執行模組乘法之方法及裝置。

相關技藝說明

模組取冪及相關的數學運算常用於像是密碼學的一些應用中。舉例而言，形式為 $X^E \bmod M$ 的模組取冪為 Rivest-Shamir-Adleman(RSA)加密系統中的主要運算，其中 X 、 E 及 M 皆為大的無符號整數(如 512 或 1024 位元)。模組取冪依此為一種利用類似大小的整數來重覆形式為 $A \times B \bmod M$ 之模組乘法之處理。一種執行模組乘法的方式為先運算 $A \times B$ ，然後減去所得到的乘積再模組 M 。執行這兩個獨立運算及偵測所得到的餘數所需要的時間及資源使得此技術對於大的整數無法適用。模組乘法亦可利用其它像是「蒙哥馬利乘法」的技術來執行，其中該乘法及模組減法運算係在一個數學轉換空間中的單一步驟內來執行。

習用的模組乘法器通常包含實施在硬體中的一線性收縮陣列或「串鏈」的處理元件(PE)，例如一特定應用積體電路(ASIC)，或一可程式邏輯裝置，例如一場域可程式閘極陣列(FPGA)。在習用的模組乘法器中，一給定的處理元件由處理資料來執行一模組乘法運算的一部份，然後在一給定的時脈循環中將其傳送到其相鄰或相接的PE中。在下一個時脈循環中，該原始的處理元件維持閒置，而相鄰的

五、發明說明(2)

處理元件即處理該接收的資料，並傳送該處理的資料回去，其後該原始處理元件可佔用另一個循環來運算。因此，在大多數習用的模組乘法器中，每個處理元件在每間隔一個時脈循環來進行有用的工作，而在剩餘的時間內為閒置。在一傳統的模組乘法器中，這些閒置循環可用來同時執行一額外的有限模組乘法運算，其中三個運算子中的兩個，B及M必須相同。

在這種模組乘法器中，一組循環要用來根據一熟知的平方及相乘的模組取冪技術來執行一相關的乘法運算。但是在所有的習用模組乘法器中，所需要的處理元件之總數係相關於該模組乘法運算子的大小及每個元件所處理的位元數目。舉例而言，一512位元模組乘法運算將需要至少128個4位元處理元件，藉此一1024位元的模組乘法運算將需要至少256個。模組乘法器基本上亦包含一固定數目的額外處理元件及/或額外的邏輯來執行模組乘法運算。因此，用來對於大尺寸的運算子執行運算之模組乘法器，例如運用在模組取冪為主的密碼系統者，其需要大量的空間及硬體的資源。

圖式簡單說明

本發明係藉由範例來說明，其並不限於所附圖面，其中類似的參考編號係用來代表類似的元件，其中：

圖1所示為根據本發明一具體實施例之範例性系統方塊圖；

圖2所示為根據本發明一第一具體實施例之模組乘法器

五、發明說明(3)

的高階方塊圖；

圖3所示為根據本發明一第二具體實施例之模組乘法器的高階方塊圖；

圖4所示為根據本發明一具體實施例之處理元件的高階方塊圖；

圖5所示為根據本發明一具體實施例之模組乘法運算到一模組乘法器之資料流程圖；

圖6所示為本發明一具體實施例之高階程序流程圖。

發明詳細說明

此處係揭示一種用以執行模組乘法之方法及裝置。在以下的詳細說明中，許多特定的細節，例如特定的電腦系統、模組乘法器、及處理元件架構或結構之提出係要提供對於本發明之更為完整的瞭解。但是其必須瞭解此處所述的這些及其它特定細節並非必要來用於實施本發明。類似地，雖然本說明的許多部份係利用「右」、「左」、「右手邊」、「左手邊」、「最右方」或「最左方」等用語來代表本發明的部份，這些用語係代表在圖面中所示的相對元件方向，其必須不能解釋為對於本發明的實體實施上的限制。在其它狀況下，熟知的結構、元件或連接已經省略，或並未在特定細節中來說明，藉以避免不必要地混淆本發明。

圖1所示為根據本發明一具體實施例之範例性資料處理系統100的方塊圖。在所示的具體實施例中，資料處理系統100包含一或多個處理器102，及耦合到一處理器系統匯流

五、發明說明 (4)

排106之晶片組104。處理器102其每個可包含任何適當的處理器架構，且對於一具體實施例包含一IntelTM架構，其用於例如在美國加州 Santa Clara之IntelTM公司提供的處理器之PentiumTM系列。本發明一具體實施例的晶片組104包含一「北橋接器」或記憶體控制器集線器(MCH)108，及一「南橋接器」或輸入/輸出(I/O)控制器集線器(ICH)110，其如所示地耦合在一起。MCH 108及ICH 110每個可包含任何適當的電路，而對於一具體實施例，其每個可形成為一獨立的積體電路晶片。其它具體實施例的晶片組104可包含任何適當的一或多個積體電路或分離裝置。

MCH 108可包含一適當的介面控制器，以提供任何適當的通訊鏈結到處理器系統匯流排106及/或任何適當的裝置或組件來通訊於MCH 108。一具體實施例的MCH 108提供每個介面之適當的仲裁、緩衝及連貫性管理。

MCH 108係耦合於處理器系統匯流排106，並提供一介面到處理器102在該處理器系統匯流排106上。處理器102在本發明的其它具體實施例中可結合於MCH 108或晶片組104來形成一單晶片。MCH 108根據本發明在一具體實施例亦提供一介面到一記憶體112、一繪圖控制器114及一處理器117，其每個係耦合到MCH 108中，如圖所示。記憶體112能夠儲存資料及/或在一處理器上的指令執行檔，例如資料處理系統100的處理器102或117，其可包含任何適當的記憶體，例如像是動態隨機存取記憶體(DRAM)。繪圖控制器114器控制在一適當顯示器116上的資訊顯示，例如像是一陰

五、發明說明(5)

極射線管(CRT)或液晶顯示器(LCD)，其耦合到繪圖控制器114。在所示的具體實施例中，MCH 108透過一加速的繪圖埠來介面於繪圖控制器114。但是，其將可瞭解到本發明可使用任何適當的繪圖匯流排或埠的標準來實施。一具體實施例的繪圖控制器114另可結合於MCH 108來形成一單晶片。

雖然處理器117已經在附圖中描述為一獨立、特定用途或「特定應用」積體電路晶片，在本發明的其它具體實施例中處理器117係實施為一可程式邏輯或閘極陣列裝置，例如一場域可程式閘極陣列(FPGA)，及做為一通用處理器(例如一或多個處理器112)，其可利用在一機器-可讀取媒體中所實施的可執行指令來程式化，以造成該通用處理器來執行本發明的方法。

處理器117根據本發明一具體實施例來用於加速大量運算的工作，例如模組取冪及/或模組乘法，其相關於加密系統的加密、解密或鑑認運算，例如RSA。因此，在一具體實施例中，處理器117包含一模組乘法器，其包含至少一第一及第二獨立的運算通道，及一介於該第一及第二獨立運算通道之間的耦合裝置，以回應用接收一第一控制信號來耦合該第一運算通道與該第二運算通道。處理器117可透過一熟知的處理器插座(未示出)，其透過耦合到MCH 108之PC-100或PC-133記憶體匯流排上的一雙重線上記憶體模組(DIMM)溝槽來耦合到資料處理系統100，或在本發明其它具體實施例中透過一擴充匯流排。

五、發明說明(6)

MCH 108亦耦合到ICH 110來經由一集線器介面來提供存取到ICH 110。ICH 110提供一介面到資料處理系統100的I/O裝置或週邊組件。ICH 110可包含任何適當的介面控制器來提供任何適當的通訊鏈結到MCH 108，及/或到任何適當的裝置或組件來通訊於ICH 110。一具體實施例的ICH 110可對於每個介面提供適當的緩衝及仲裁。

在所示的具體實施例中，ICH 110進一步提供一介面到一網路介面控制器118、一大量儲存裝置120，及到一鍵盤122、滑鼠124、軟式磁碟機126，以及額外的裝置透過一或多個標準串列128或序列130埠通過一超級I/O控制器132。網路介面控制器118或另外的數據機編碼解碼器(未示出)可用來耦合資料處理系統100到一適當的通訊網路，其可透過許多熟知的方法進行。大量儲存裝置120可包含任何適當的裝置或組件來儲存資料及/或指令，例如一磁帶或硬碟磁性儲存裝置，或一光學儲存裝置，像是光碟或數位多樣化碟片(DVD)唯讀記憶體(ROM)裝置。在本發明一具體實施例中，大量儲存裝置120包含一或多個硬碟機(HDD)。在所示的具體實施例中，ICH110亦提供一介面到一擴充匯流排橋接器134，以便於透過一擴充匯流排來附加額外的I/O裝置或週邊組件，例如一週邊組件內連接(PCI)、工業標準架構(ISA)或通用序列匯流排(USB)(未示出)。

本發明的具體實施例可包含軟體、資訊處理硬體、及許多處理運算，其進一步在此處說明。本發明的特徵及處理運算可實施為在一機器-可讀取媒體中的所包含的可執行

五、發明說明(7)

指令，像是記憶體112、大量儲存裝置120、耦合軟碟機126的可移除碟片媒體、一透過網路介面控制器118可用的一通訊網路，或類似者。

一機器-可讀取媒體可包含任何機制，其提供了一機器(例如資料處理系統100)可讀取形式的資訊(即儲存及/或傳送)。舉例而言，一機器-可讀取媒體包含但不限於：唯讀記憶體(ROM)；隨機存取記憶體(RAM)；磁碟儲存媒體；光學儲存媒體；快閃記憶裝置；電性、光學、聲音或其它形式的傳遞信號(如載波、紅外信號、數位信號等)；或類似者。該指令可用來使得像是程式化有指令的處理器102或處理器117之通用或特定用途處理器來執行本發明的方法或處理。另外，本發明的特徵或運算可由特定的硬體組件來執行，其中包含用以執行該運算之硬體接線邏輯，或藉由任何可程式資料處理組件及顧客化硬體組件之組合。

其必須瞭解到本發明可利用一具有比所示之範例性系統較多或較少數目的組件的資料處理系統100來實施。舉例而言，資料處理系統100在本發明的其它具體實施例中可包含許多種伺服器或客戶端電腦系統或裝置中的一種，例如工作站、個人電腦、「薄型客戶端」(即網路電腦NetPC)、網際網路家電、終端機、掌上型運算裝置、穩固的細胞式或個人通訊服務(PCS)電話、「薄型伺服器」(有時候稱之為裝置伺服器、應用伺服器或特殊伺服器)或類似者。在本發明一具體實施例中，資料處理系統100包含一伺服器電腦系統。在本發明另一具體實施例中，資料處理系統100

五、發明說明(8)

包含一用以執行安全插座層(SSL)連接或加密/解密運算之電子商務加速器網路裝置。

圖2所示為根據本發明一第一具體實施例之模組乘法器200的高階方塊圖；在所示的具體實施例中，模組乘法器200包含複數個處理元件，例如處理元件202、終端或「末端」邏輯204，及一耦合裝置，其根據本發明包含一第一多工器206及一第二多工器208。

當多種技術及硬體實施可用來實現模組乘法，所述的模組乘法器200具體實施例包含一蒙哥馬利乘法器，其建構成一處理元件的線性收縮陣列，其每個處理元件係處理一蒙哥馬利乘法運算的一些位元數目。例如，在圖2所示的具體實施例中每個處理元件一次運作一蒙哥馬利乘法運算的4個位元。通常，所需要的處理元件數目將等於數字N的數目，其係在該模組乘法中處理的運算子加上一些額外的處理元件來管理溢位的狀況，並保證適當的輸入係供應給該陣列的餘數，其中該「數字」的數目係等於該位元數目n，其為每個運算子除以該「根」，或每個處理元件所處理的位元數目。

因此，在習用的模組乘法器中，一512位元的乘法運算基本上需要132個4位元的處理元件，而一256位元的乘法需要68個4位元的處理元件。另外，一模組乘法運算可利用一個處理元件來完成，其具有功能為最後或「最左方」的處理元件加入到相關的末端邏輯中。舉例而言，末端邏輯可用來包含一「或」邏輯閘，以由下一個到最後一個處理元

五、發明說明(9)

件及一正反器來取得至少兩個進位位元信號，用以註冊該邏輯「或」閘極輸出，並透過一「S-in」中間結果輸入來將其提供給下一個到最後的處理元件。但是在所示的具體實施例中，所需要的處理元件之數目可降低到通常執行那些運算子之模組乘法運算所需要之實際處理的大小之一半。

在本發明的內容中，每個具有形式為 $A \times B \bmod M$ 之複數個模組乘法運算皆為「獨立」，如果其在三個運算子(即「A」、「B」及「M」)中至少兩個為不同。此外，一模組乘法器的運算通道係描述為「獨立」，如果其每個能夠同時執行複數個獨立模組乘法運算中至少一個運算。其亦必須瞭解到，雖然用語「A」、「B」及「M」係用於整個內容中來代表在一模組乘法運算中的參數，這些為通稱的設定，其可使用任何其它用語但並不背離本發明的精神及範圍。

在本發明一具體實施例中，該處理元件的線性收縮陣列包含複數個獨立的運算通道，其包含一第一運算通道及一第二運算通道，其能夠分別執行形式為 $A1 \times B1 \bmod M1$ 及 $A2 \times B2 \bmod M2$ 之獨立的第一及第二模組乘法運算。一或多個運算子可提供給該初始或「最右方」處理元件(在圖2中標示為PE-0)，並收縮地由右到左來傳遞通過該PE的線性陣列，以完成所述的模組乘法運算。其必須瞭解到，在此說明的內容中，該用語「運算子」可包含一或多個整個模組乘法運算子(例如「A」、「B」及/或「M」運算子)或其任何部份，例如數位或個別的二元化位元。

五、發明說明 (10)

在一具體實施例中，該模組乘法器先由傳遞每個運算子B1、B2、M1及M2來初始化，一次一個數字來通過該乘法器，直到每個運算子分佈到該線性收縮陣列的所有處理元件。在另一具體實施例中，每個參數B1、B2、M1及M2的倍數經過計算，然後儲存在該收縮陣列的一些或所有PE中。為了執行該模組乘法運算，一運算子A1係依序地傳送，一次一個數字，到達該線性收縮陣列的PE-0、PE-1、PE-2等，在交替的時脈循環中，來利用儲存的B1及M1的倍數來處理。在中間的時脈循環中，運算子A2係類似地傳送通過要利用儲存的B2及M2倍數來處理之處理元件的陣列。當A1及A2的所有數字已經傳送通過該串鏈的處理元件，該乘法運算即完成，而該運算結果R1及R2即儲存在整個處理元件陣列中。然後該結果R1及R2即可由左到右傳送回通過該處理元件陣列，並透過PE-0來接收。

在該模組乘法器的運算期間，一給定的處理元件在每個「時脈」或該時脈來源(未示出)的脈衝上，由該線性收縮陣列中其立即(即前/右及下/左)的相鄰PE之兩者來接收資料或提供資料。每個PE具有一適當的控制信號，並在一時脈循環期間具有一第一運算子A1的數字，藉以執行在該第一運算通道內一模組乘法運算之一部份，然後具有其它的控制信號，及一第二運算子A2的數字，以在下一個時脈循環期間來執行另一個模組乘法運算的一部份。在一具體實施例中，偶數的PE在奇數的時脈循環中執行一第一模組乘法的運算，並在一偶數時脈循環中執行一第二模組乘法中

五、發明說明 (11)

的運算，而在奇數的PE在偶數的時脈循環中執行一第一模組乘法及在一奇數時脈循環中執行一第二模組乘法中的運算。所應用的運算子及/控制信號，及該運算通道為「啟動」或運算中，因此係交替於一應用的時脈及/或控制信號。

在圖2所示的具體實施例中，除了利用該第一及第二獨立運算通道來執行兩個不同的模組乘法運算，該運算通道係根據本發明結合來形成一單一「虛擬」運算串鏈，藉由輸送該處理元件的線性收縮陣列的末端回到該陣列的開始處。該第二運算通道因此可做為該第一的延續，其有效地加倍了該線性收縮陣列的長度，而犧牲了可用的乘法通道中的一個。但是其必須瞭解到，在本發明其它具體實施例中，所得到的有效線性收縮陣列長度可大於或小於該原始長度的兩倍。舉例而言，本發明的具體實施例可以實施為其中一具有超過兩個獨立的運算通道之線性收縮陣列可用來產生一較長的有效陣列長度。類似地，可實施一具體實施例中並非所有的線性收縮陣列的處理元件皆用到，或包含在所提供的回授迴路內，而造成一較短的有效陣列長度。

在圖2所示的具體實施例中，該耦合裝置的第一多工器206及第二多工器208其每個可基於一接收到的控制信號來運作，Mux Select 210。在一具體實施例中，Mux Select 210在一邏輯「1」及一邏輯「0」之間交替。因此，該第一或「最右方」處理元件的輸入耦合到該第二多工器208的輸出，其交替地具有一通道1資料源212耦合到第二多工器208的第一輸入，及該陣列的最後或最左方處理元件的一輸出

五、發明說明 (12)

耦合到第二多工器208的第二輸入。類似地，利用Mux Select 210，該最後或「最左方」處理元件的輸入耦合到該耦合裝置的第一多工器206的一輸出，其交替地具有末端邏輯204的一輸出或該第一或「最右方」PE的輸出，即PE-0。

因此，一回授路徑提供在使用本發明之耦合裝置的所示之線性收縮陣列的第一及最後處理元件之間。所得到的回授運算通道之使用使得一n-位元模組乘法運算之第一部份係使用該第一獨立運算通道來執行，而該n-位元模組乘法運算的第二部份使用該第二獨立的運算通道來執行，其中該第一及第二運算通道係使用執行n/2位元模組乘法通常所需要的處理元件數目來建構。在一具體實施例中，所述的模組乘法運算之第一部份係在一第一時段期間執行，而所述的模組乘法運算之第二部份係在一第二時段期間來執行，其中該第一時段及第二時段有重疊。

因此，圖2所示的該靜態模組乘法器具體實施例可用來執行一n-位元的模組乘法運算，其使用具有通常足以執行一n/2位元模組乘法運算之處理元件數目的線性收縮陣列。因此為了此說明的目的，所示的陣列或串鏈之處理元件將有左至右由編號0到N/2+2來代表，由第一個處理元件開始，其中N等於在該模組乘法中所處理的運算子中數字的數目。所以例如一1024位元的模組乘法運算，其通常需要259個4位元處理元件加上末端邏輯(即 $1024 / 4 = N = 256 + 3$ ，額外的PE = 259)其另將需要131個4位元的處理元件($N = 256 / 2 = 128 + 3 = 131$)。在本發明一具體實施例中，

五、發明說明 (13)

存在有一限制為其需要在該回授串鏈中的處理元件數目為奇數，所以由該第一運算通道末端所回授回的資料可到達該第二運算通道的開始，並碰到該陣列的處理元件之另外閒置的運算循環，而非忙碌循環。在另一具體實施例中，其在一陣列中需要偶數個處理元件，在該陣列內可包含奇數個額外的處理元件(如一額外的處理元件)，但在該回授迴路本身之外。該額外的處理元件可加入到該末端邏輯，或另放置在該回授迴路的左側，或另可在該回授迴路的右側，其在該第二多工器208之前。

其必須瞭解到所使用的處理元件數目、每個元件處理的位元數目及所示的模組取冪器的大小為任意的，並可在其它具體實施例中變化。在本發明一具體實施例中，一專屬的512位元的蒙哥馬利乘法器，其通常實施成一雙通道的131-PE串鏈，其另可實施為一靜態的單通道回授67-PE串鏈。在本發明另一具體實施例中，一雙通道512位元的蒙哥馬利乘法器以131-PE串鏈實施，其可做成額外可選擇地能夠執行1024位元的蒙哥馬利乘法，其立用具有相同數目的處理元件之單通到回授串鏈。因此，本發明的具體實施例通常允許模組乘法及取冪運算來利用比先前所需要的要少的硬體資源來執行。

圖3所示為根據本發明一第二具體實施例之模組乘法器300的高階方塊圖。圖3的模組乘法器300實質上類似於圖2所示的模組乘法器200，其包含複數個處理元件，例如處理元件302、終端或「末端」邏輯304，及包含一第一多工器

五、發明說明 (14)

306及一第二多工器308的一耦合裝置來接收一通道1資料源312，及一第一控制信號，Mux Select 1 310，如根據本發明之圖2中所述。但是，模組乘法器300包含額外的邏輯，其可允許處理元件的線性收縮陣列來選擇性地在至少兩個模式之間切換：一第一雙通道模式，其中該線性收縮陣列的第一及第二獨立運算通道可彼此獨立地運算，並運作為兩個獨立的n-位元模組乘法器，及一第二單一回授通道模式，其中該第一及第二運算通道係在耦合在一起運作，以運作為一單一2n-位元的模組乘法器。

更特定而言，圖3的具體實施例之模組乘法器300之耦合裝置包含一第三多工器314及一第四多工器316，以接收一邏輯「1」信號、一通道2資料源320及一額外的控制信號，Mux Select 2 318，且選擇性地耦合處理元件的模組乘法器300的線性收縮陣列之第一及第二運算通道，以回應於Mux Select 2控制信號318的狀態。在所示的具體實施例中，當該Mux Select 2 318控制信號在一第一，即邏輯「0」狀態中，前述相對於圖2之回授路徑即中斷，而模組乘法器300的第一及第二獨立運算通道即獨立地運作，交替在關於該通道1 312及通道2 320資料源之兩個獨立的模組乘法運算之間。相反地，當該Mux Select 2 318控制信號在一第二，即邏輯「1」狀態，前述的回授邏輯即完成，而該第一及第二運算通道即如前述的結合來運作為一單一模組乘法運算串鏈。其必須立即瞭解到，許多其它的實施可達到類似的結果，其可視為本發明的其它具體實施例，且皆在本發明

五、發明說明 (15)

的精神及範圍內。

圖4所示為根據本發明一具體實施例之處理元件的高階方塊圖。在圖4所示的具體實施例中，一處理元件400，例如圖2的PE 202或圖3的PE 302，其包含兩個儲存元件(B-RAM 412及M-RAM 414)，及包含PE控制邏輯410的處理邏輯，兩個位址暫存器(Q-暫存器424及A-暫存器422)，兩個加法器(S+B加法器430及S+B+M加法器440)，兩個多工器(第一多工器435及第二多工器455)，兩個進位暫存器(Carry-1-暫存器432及Carry-2-暫存器442)，一累積暫存器(S-暫存器445)，一通道選擇暫存器450，及一結果暫存器(R-暫存器460)。雖然所示為單一的PE 400，在一具體實施例中，PE 400為一給定的模組乘法器運算串鏈的每一個處理元件之通稱。

在所示的具體實施例中，除了在一線性收縮陣列中該第一或「最右方」處理元件及最後或「最左方」處理元件，在圖4底部所示的連接為多個PE所共用，所示的右方連接為介面於該右方的PE，而所示的左方連接係介面於該左方的PE，來自一PE的輸出即連接到相鄰PE的類似命名的輸入。一線性收縮陣列的該第一及最後處理元件，(如分別為圖2及3中的PE-0及PE- $N/2 + 2$)係共享該共用的連接，其示於該顯示的處理元件400之底部，具有其處理串鏈的剩餘PE。類似的，在左方的第一PE的連接介面於其左方的PE，而在右方的最後PE連接即介面於其右方的PE，如上所述。但是這些處理元件的其餘連接可隨其它的PE來改變。例如在

五、發明說明 (16)

該範例性處理元件的右方所示的連接(即 Cntl-In、Q-In、A-In、S-Out、Carry-In-1、Carry-In-2、Chnl-In及R-Out)，其交替地同時介面於一控制器及其它的資料源(未示出)，及該第一處理元件的最後處理元件之左方所示的連接。類似地，在該範例性處理元件左方所示的連接(即 Cntl-Out、Q-Out、A-Out、S-In、Carry-Out-1、Carry-Out-2、Chnl-Out及R-In)交替地介面於末端邏輯(未示出)，及根據本發明一具體實施例的最後處理元件之第一處理元件右方所示的連接。

在一具體實施例中，Clk，Carry-In-1，Carry-Out-1，Carry-In-2，Carry-Out-2，Chnl-In，Chnl-Out，及所有內部連接來傳遞那些信號，其每個包含一個位元，而Cntl-In及Cntl-Out包含辨識每個複數個控制碼所需要的位元數目。圖4所示的所有剩餘連接包含由每個PE所處理的位元數目，例如每個所示的具體實施例為4個位元。在本發明一具體實施例中，每個PE 400可視需要亦可包含其它輸入及輸出，例如一種輸入(未示出)。

在一具體實施例中，圖4的多個邏輯元件執行以下的運算：控制邏輯410鎖存器來自右方的PE所接收的一控制碼，使用該控制碼來在目前的時脈循環期間控制本PE的邏輯元件，然後傳送該控制碼到左方的PE。儲存元件B-RAM 412係用來儲存每個B的倍數之一個數字，其係儲存在該PE串鏈中，而儲存元件M-RAM 414係用來儲存每個M的倍數的一個數字，其係儲存在該PE串鏈中。A-暫存器422及Q-

五、發明說明 (17)

暫存器424分別保持在B-RAM 412及M-RAM 414中選擇所要的位置之位址(同時對於讀取及寫入)，並傳送這些位址給左方的PE。S + B加法器430係用來加入在B-RAM 412中一選擇位置的內容到左方的PE中該S-暫存器之內容，其包含透過該Carry-In-1接收的任何進位位元，來自右方的PE中的S+B加法器之輸入。Carry-1-暫存器432鎖存器來自S+B加法器430之任何進位位元，並在下一個時脈循環期間將其做為一進位位元來提供給在左方PE中的S+B加法器。

當選擇該第一多工器435之左手邊輸入時，S+B+M加法器440加入該S+B加法器430的輸出到M-RAM 414中所選擇位置的內容中。當選擇該第一多工器435的右手邊輸入時，S+B+M加法器440加入S-暫存器445的內容到M-RAM 414中該選擇的位置之內容。任何接收的進位位元即由右方的PE提供通過該Carry-In-2輸入，而任何產生的進位位元即由該PE使用來鎖存到Carry-2-暫存器442到下一個時脈循環中的目前PE之左方。該S+B+M加法器440的輸出即鎖存到S-暫存器445中，其做為過渡結果的一累積暫存器。該S-暫存器445的輸出即分佈到每個B-RAM 412, M-RAM 414、第一多工器435，及該S-Out輸入來由右方的PE使用。R-暫存器460鎖存該S-暫存器445的輸出，如果選擇第二多工器455的右手邊輸入，而另外鎖存在左方的PE中的R-暫存器之內容。通道選擇暫存器450係耦合到B-RAM 412及M-RAM 414兩者的一位址位元，以選擇在兩個儲存元件中一第一位址庫或一第二位址庫。在每個庫中，A-暫存器422

五、發明說明 (18)

及Q-暫存器424選擇特定的位置，如前所述。在一具體實施例中，該通道選擇數值由右到左傳遞通過該處理元件的通道選擇暫存器450，以及在A及Q暫存器中的數值。在一具體實施例中，該通道選擇數值為該控制碼的一部份。

在圖4的具體實施例中，Clk用來鎖存資料到該控制邏輯，到該Q-、A-、S-、R-、Carry-1-及Carry-2-，及通道選擇暫存器中，並來計時在B-及M-RAM中的寫入運作，而在B及M-RAM中的兩個加法器、兩個多工器及該讀取運作為組合式，即在一輸入端的任何改變會傳遞通過到該邏輯元件的輸出，而無關於時脈狀態。在其它具體實施例中，該B及M-RAM使用一計時的輸入來用於讀取以及寫入運作。在一具體實施例中，時脈速率的選擇使得在PE 210中最差狀況的延遲可小於一個時脈循環。來自該Clk輸入到其它電路元件之特定連接在圖4中並未顯示，以避免使得圖面覆蓋太複雜。

控制邏輯410包含控制PE 400的運作所需要的邏輯，其基於通過Cntl-In所接收的控制碼。在一具體實施例中，控制邏輯410包含一解碼器電路，以轉換該控制碼到必要的控制信號。在其它具體實施例中，該控制碼僅為鎖存，其中該控制碼的每個位元指定一特定的控制信號。在一具體實施例中，該控制碼指定了包含但不限於以下列出的運作：選擇第一多工器435中兩個輸入中的一個，選擇第二多工器455中兩個輸入中的一個，寫入到B-RAM 412，寫入到M-RAM 424，重置一或多個的A、Q、S及R暫存器，並禁

五、發明說明 (19)

止該時脈信號到不同的邏輯元件。

因為蒙哥馬利乘法係利用B及M的倍數來運算，一具體實施例在PE內預先計算該倍數，使用了用於該蒙哥馬利乘法之相同的邏輯。在圖4所示的具體實施例中，該儲存元件包含隨機存取記憶體(RAM)、標示的B-RAM及M-RAM來代表儲存的參數。即使該用語‘B-RAM’及‘MRAM’在整個內容中皆使用，在一些具體實施例中，係使用RAM之外的儲存元件形式。總而言之，在PE串鏈中所有的B-RAM 412提供了 $(0 \times B1)$ 、 $(1 \times B1)$ 、 $(2 \times B1)$ 等數值的儲存空間的第一庫，及 $(0 \times B2)$ 、 $(1 \times B2)$ 、 $(2 \times B2)$ 等數值的儲存空間的第二庫。在一具體實施例中，其中每個PE係運作在一16進位的數字，B-RAM 412包含32個4位元的儲存位置，16個位置來保持 $(0 \times B1)$ 到 $(15 \times B1)$ 的數字，而其它16個位置來保持 $(0 \times B2)$ 到 $(15 \times B2)$ 的數字。類似地在相同的具體實施例中，M-RAM 414包含32個4位元的儲存位置，以保持 $(0 \times M1)$ 到 $(15 \times M1)$ 及 $(0 \times M2)$ 到 $(15 \times M2)$ 之相對應的數字。在一具體實施例中，其中每個PE處理一些位元，而非4個位元，在每個RAM中的位置數目即依此而改變，以對於每組參數來定址及儲存所需要的倍數的數目。

在一些具體實施例中，一給定參數的單一數值永遠用於兩種蒙哥馬利乘法中。在這些具體實施例中，該相對應的儲存元件提供了唯獨該參數的單一數值之倍數的儲存，而來自通道選擇暫存器450到該儲存元件之連接即可消除，所以兩個蒙哥馬利乘法皆自相同的運算子倍數庫來讀取。在

五、發明說明 (20)

這種具體實施例中，M-RAM 414包含16個位置來儲存(0 x M)到(15 x M)之倍數，而通道選擇暫存器450並不控制一位址輸入線到M-RAM 414。設計來保持兩個獨立的M數值之具體實施例亦可用於具有單一數值的M來使得M1及M2相同的應用中。

在一具體實施例中，當PE 400在兩個同步蒙哥馬利乘法運算期間的每一個時脈循環上交替於該第一及第二通道之間，該信號Cntl-In為一頻率為Clk一半的方波，所以該通道選擇暫存器450的輸出會在交替的時脈循環中於高及低之間振盪。此動作在每個時脈循環中交替於B-RAM 412及M-RAM 414中第一及第二儲存位置庫之間。其必須立即瞭解到圖2及3所示之不同的單一輸入及輸出其每個可映射到關於圖4之處理元件400所述的一或多個輸入及輸出。

圖5所示為根據本發明一具體實施例之模組乘法運算到一模組乘法器之資料流程圖。當配合用於標準密碼位元長度的一單一模組乘法運算時，其需要數百個處理元件及數千個時脈循環來完成，僅包含7個處理元件之簡化的模組乘法乘法器已示於圖5，藉以避免使得所示圖面的覆蓋太過於複雜。在圖5所示的表格中，陰影區域顯示當註冊資料時的循環，其係在一處理元件、末端邏輯、或在「通道1」輸入暫存器輸入該第一處理元件(即PE-0)時。較暗的陰影顯示註冊在該虛擬(雙重長度)串鏈的下半部中資料，而較淡的陰影顯示註冊在上半部中的資料。此外，在每個表格單元或元素內的數目代表該串鏈位置，其為一處理元件在每個

五、發明說明 (21)

循環中可有效服務者，因此例如在循環8中，所述的模組乘法運算到達PE-6，而在循環9中來自PE-6的資料環繞到實質上為PE-0，但功能做為下一個處理元件PE-7。

圖6所示為根據本發明之方法的一具體實施例的高階程序流程圖，用以對於複數個運算子來執行一模組乘法運算，其立用包含一第一獨立運算通道及一第二獨立運算通道的一模組乘法器。圖6所示的處理即開始(方塊600)，然後接收到複數個運算子及像是圖2的Mux Select信號210及圖3的Mux Select 1信號310之第一控制信號(方塊602)。接下來，該第一及第二獨立運算通道利用根據本發明之耦合裝置來耦合在一起(方塊604)。然後，使用該第一運算通道來執行一模組乘法運算的第一部份(方塊606)，並在所示的處理終止(方塊610)之前來使用該第二運算通道執行該模組乘法運算的第二部份(方塊608)。

在前述的說明中，本發明已經參考其特定的範例性具體實施例來說明。但是，其將可瞭解到所述的範例性具體實施例之變化或修正，以及本發明的其它具體實施例皆可在不背離如在所附申請專利範圍中所定義的本發明之廣義精神及範圍之下來實施。因此該說明書及圖面係要視為一說明性而非限制性的意義。

四、中文發明摘要 (發明之名稱：用以執行模組乘法之方法及裝置)

本發明揭示一種用以執行模組乘法之方法及裝置。根據本發明一具體實施例的裝置包含一模組乘法器，其具有複數個獨立的運算通道，其中該複數個獨立的運算通道包含一第一運算通道及一第二運算通道，及介於該第一運算通道及該第二運算通道之間的一耦合裝置，以接收一控制信號，並回應於一接收該控制信號來耦合該第一運算通道到該第二運算通道。

英文發明摘要 (發明之名稱：METHOD AND APPARATUS FOR PERFORMING MODULAR MULTIPLICATION)

A method and apparatus for performing modular multiplication is disclosed. An apparatus in accordance with one embodiment of the present invention includes a modular multiplier including a plurality of independent computation channels, where the plurality of independent computation channels includes a first computation channel and a second computation channel, and a coupling device interposed between the first computation channel and the second computation channel to receive a control signal and to couple the first computation channel to the second computation channel in response to a receipt of the control signal.

五、發明說明 (22)

圖式元件符號說明

- 100 資料處理系統
- 102 處理器
- 104 晶片組
- 106 處理器系統匯流排
- 108 「北橋接器」或記憶體控制器集線器(MCH)
- 110 「南橋接器」或輸入/輸出(I/O)控制器集線器(ICH)
- 112 記憶體
- 114 繪圖控制器
- 116 顯示器
- 117 處理器
- 118 網路介面控制器
- 120 大量儲存裝置
- 122 鍵盤
- 124 滑鼠
- 126 軟式磁碟機
- 128 標準串列
- 130 序列埠
- 132 超級 I/O 控制器
- 134 擴充匯流排橋接器
- 200 模組乘法器
- 202 處理元件
- 204 終端或「末端」邏輯
- 206 多工器

修正本有無誤？
93年5月
是否准予修正？

裝
訂
線

五、發明說明 (23)

- 208 多工器
- 210 Mux select
- 212 資料源
- 300 模組乘法器
- 302 處理元件
- 304 終端或「末端」邏輯
- 306 多工器
- 308 多工器
- 310 Mux Select 1
- 312 通道 1 資料源
- 314 多工器
- 316 多工器
- 318 Mux Select 2
- 320 通道 2 資料源
- 400 處理元件
- 410 控制邏輯
- 412 B-RAM
- 414 M-RAM
- 422 A-暫存器
- 424 Q-暫存器
- 430 加法器
- 432 Carry-1-暫存器
- 435 多工器
- 440 加法器

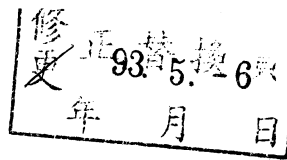
442	Carry-2-暫存器
445	S-暫存器
450	通道選擇暫存器
455	多工器
460	結果暫存器

請交員明示
年 月 日所提之

装

訂

線



六、申請專利範圍

1. 一種用以執行模組乘法之裝置，包括：

一模組乘法器，其包含複數個獨立的運算通道，該複數個獨立運算通道包含一第一運算通道及一第二運算通道；及

一耦合裝置，其介於該第一運算通道及該第二運算通道之間，以接收一第一控制信號，並回應於接收該第一控制信號來耦合該第一運算通道到該第二運算通道。

2. 如申請專利範圍第1項之裝置，其中該模組乘法器包含一處理元件的線性收縮陣列，該處理元件的線性收縮陣列包含該複數個獨立的運算通道。
3. 如申請專利範圍第1項之裝置，其中該耦合裝置包含一耦合裝置，其用來接收一第二控制信號，並回應於該第二控制信號的狀態來選擇性地耦合該第一運算通道到該第二運算通道。
4. 如申請專利範圍第3項之裝置，該裝置具有對應於該第二控制信號之一第一狀態之一第一運作模式，其中該第一運算通道在運作上獨立於該第二運算通道，及對應於該第二控制信號之第二狀態之一第二運作模式，其中該第一運算通道在運作上透過該耦合裝置來耦合到該第二運算通道。
5. 如申請專利範圍第4項之裝置，其中該第一運算通道及該第二運算通道在該第一運作模式中運作為兩個 n -位元的模組乘法器，而在該第二運作模式中做為一單一 $2n$ -位元的模組乘法器，其中 n 為一整數。

六、申請專利範圍

6. 如申請專利範圍第5項之裝置，其中n為512。
7. 如申請專利範圍第1項之裝置，其中該模組乘法器包含一蒙哥馬利乘法器。
8. 如申請專利範圍第1項之裝置，其中該一耦合裝置包含：
：一第一多工器，其耦合在該第一運算通道的一輸出與該第二運算通道的一輸入之間；及一第二多工器，其耦合在該第二運算通道的一輸出與該第一運算通道的一輸入之間。
9. 一種處理器，包括：
 一模組乘法器，其包含複數個獨立的運算通道，該複數個獨立運算通道包含一第一運算通道及一第二運算通道；及
 一耦合裝置，其介於該第一運算通道及該第二運算通道之間，以接收一第一控制信號，並回應於接收該第一控制信號來耦合該第一運算通道到該第二運算通道。
10. 如申請專利範圍第9項之處理器，其中該模組乘法器包含一處理元件的線性收縮陣列，該陣列包含該複數個獨立的運算通道。
11. 如申請專利範圍第9項之處理器，其中該耦合裝置包含一耦合裝置，其用來接收一第二控制信號，並回應於該第二控制信號的狀態來選擇性地耦合該第一運算通道到該第二運算通道。
12. 如申請專利範圍第11項之處理器，該處理器具有：對應於該第二控制信號之第一狀態之一第一運作模式，其中

六、申請專利範圍

該第一運算通道在運作上獨立於該第二運算通道；及對應於該第二控制信號之第二狀態的一第二運作模式，其中該第一運算通道在運作上透過該耦合裝置來耦合到該第二運算通道。

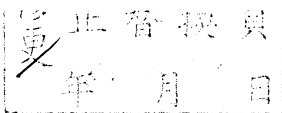
13. 如申請專利範圍第12項之處理器，其中該第一運算通道及該第二運算通道在該第一運作模式中運作為兩個 n -位元的模組乘法器，而在該第二運作模式中做為一單一 $2n$ -位元的模組乘法器，其中 n 為一整數。
14. 如申請專利範圍第13項之處理器，其中 n 為512。
15. 如申請專利範圍第9項之處理器，其中該模組乘法器包含一蒙哥馬利乘法器。
16. 如申請專利範圍第9項之處理器，其中該耦合裝置包含：
一第一多工器，其耦合在該第一運算通道的一輸出與該第二運算通道的一輸入之間；及一第二多工器，其耦合在該第二運算通道的一輸出與該第一運算通道的一輸入之間。
17. 一種用以執行模組乘法之系統，包括：
一記憶體，用以儲存資料及指令；
一第一處理器，其耦合到該記憶體來處理資料及執行指令；
一第二處理器，其耦合到該記憶體，該第二處理器包含：
一模組乘法器，其包含複數個獨立的運算通道，該複數個獨立運算通道包含一第一運算通道及一第二運

六、申請專利範圍

算通道；及

一耦合裝置，其介於該第一運算通道及該第二運算通道之間，以接收一第一控制信號，並回應於接收該第一控制信號來耦合該第一運算通道到該第二運算通道。

18. 如申請專利範圍第17項之系統，其中該模組乘法器包含一處理元件的線性收縮陣列，該元件的線性收縮陣列包含該複數個獨立的運算通道。
19. 如申請專利範圍第17項之系統，其中該耦合裝置包含一耦合裝置，其用來接收一第二控制信號，並回應於該第二控制信號的狀態來選擇性地耦合該第一運算通道到該第二運算通道。
20. 如申請專利範圍第19項之系統，該第二處理器具有：對應於該第二控制信號之第一狀態的一第一運作模式，其中該第一運算通道在運作上獨立於該第二運算通道；及對應於該第二控制信號之第二狀態的一第二運作模式，其中該第一運算通道在運作上透過該耦合裝置來耦合到該第二運算通道。
21. 如申請專利範圍第20項之系統，其中該第一運算通道及該第二運算通道在該第一運作模式中運作為兩個 n -位元的模組乘法器，而在該第二運作模式中做為一單一 $2n$ -位元的模組乘法器，其中 n 為一整數。
22. 如申請專利範圍第17項之系統，其中該耦合裝置包含：一第一多工器，其耦合在該第一運算通道的一輸出與該第二運算通道的一輸入之間，及一第二多工器，其耦合



六、申請專利範圍

在該第二運算通道的一輸出與該第一運算通道的一輸入之間。

23. 一種用以執行模組乘法之方法，包括：

接收一第一控制信號及複數個運算子；及

利用包含複數個獨立的運算通道之模組乘法器來對於該複數個運算子執行一模組乘法運算，該複數個獨立的運算通道包含一第一運算通道及一第二運算通道，其中執行該模組乘法運算包含：

回應於接收該第一控制信號來耦合該第一運算通道與該第二運算通道；

利用該第一運算通道來執行該模組乘法運算之第一部份；及

利用該第二運算通道來執行該模組乘法運算之第二部份。

24. 如申請專利範圍第23項之方法，其中執行一模組乘法運算包含利用包含一處理元件的線性收縮陣列之模組乘法器來對於該複數個運算子執行一模組乘法運算，該處理元件的線性收縮陣列包含該複數個獨立的運算通道。

25. 如申請專利範圍第23項之方法，其中：

執行該模組乘法運算的第一部份包含提供該複數個運算子到該第一運算通道，及利用該第一運算通道來處理該複數個運算子來產生一中間結果；

耦合該第一運算通道及該第二運算通道包含提供該中間結果到該第二運算通道；及

六、申請專利範圍

執行該模組乘法運算的一第二部份包含利用該第二運算通道來處理該中間結果。

26.如申請專利範圍第23項之方法，該方法進一步包含接收一第二控制信號，其中耦合該第一運算通道與該第二運算通道包含回應於接收該第二控制信號來選擇性地耦合該第一運算通道與該第二運算通道。

27.一種機器可讀取媒體，其中包含有複數個機器可執行的指令，其在當由一機器執行時，使得該機器來執行一方法，其包含：

接收一第一控制信號及複數個運算子；及

利用包含複數個獨立的運算通道之模組乘法器來對於該複數個運算子執行一模組乘法運算，該複數個獨立的運算通道包含一第一運算通道及一第二運算通道，其中執行該模組乘法運算包含：

回應於接收該第一控制信號來耦合該第一運算通道與該第二運算通道；

利用該第一運算通道來執行該模組乘法運算之一第一部份；及

利用該第二運算通道來執行該模組乘法運算之一第二部份。

28.如申請專利範圍第27項之機器可讀取媒體，其中執行一模組乘法運算包含利用包含一處理元件的線性收縮陣列之模組乘法器來對於該複數個運算子執行一模組乘法運算，該處理元件的線性收縮陣列包含該複數個獨立

六、申請專利範圍

的運算通道。

29. 如申請專利範圍第27項之機器可讀取媒體，其中：

執行該模組乘法運算之一第一部份包含提供該複數個運算子到該第一運算通道，及利用該第一運算通道來處理該複數個運算子來產生一中間結果；

耦合該第一運算通道及該第二運算通道包含提供該中間結果到該第二運算通道；及

執行該模組乘法運算之一第二部份包含利用該第二運算通道來執行該中間結果。

30. 如申請專利範圍第27項之機器可讀取媒體，該方法進一步包含接收一第二控制信號，其中耦合該第一運算通道與該第二運算通道包含回應於接收該第二控制信號來選擇性地耦合該第一運算通道與該第二運算通道。

31. 一種用以執行模組乘法之方法，包括：

在一收縮陣列乘法器的一第一末端處自該收縮陣列乘法器的一第二末端接收一資料值，及在該第二末端自該第一末端接收一資料值。

32. 如申請專利範圍第31項之方法，其中在一收縮陣列乘法器的一第一末端處自該收縮陣列乘法器之一第二末端接收一資料值包含：

在一多工器的一第一輸入自該收縮陣列乘法器的一第二末端接收一資料值；

在該多工器的一第二輸入處接收一通道資料輸入信號；及

六、申請專利範圍

透過該多工器的一輸出來提供來自該收縮陣列乘法器的第二末端之資料值或該運算資料輸入信號到一收縮陣列乘法器的該第一末端。

33. 如申請專利範圍第31項之方法，進一步包含：

在一時脈信號的交替循環期間處理運作在一給定問題上的處理元件中的資料。

裝

訂

線

正替換圖
33

第 091122363 號專利申請案
中文圖式替換本(93年5月)

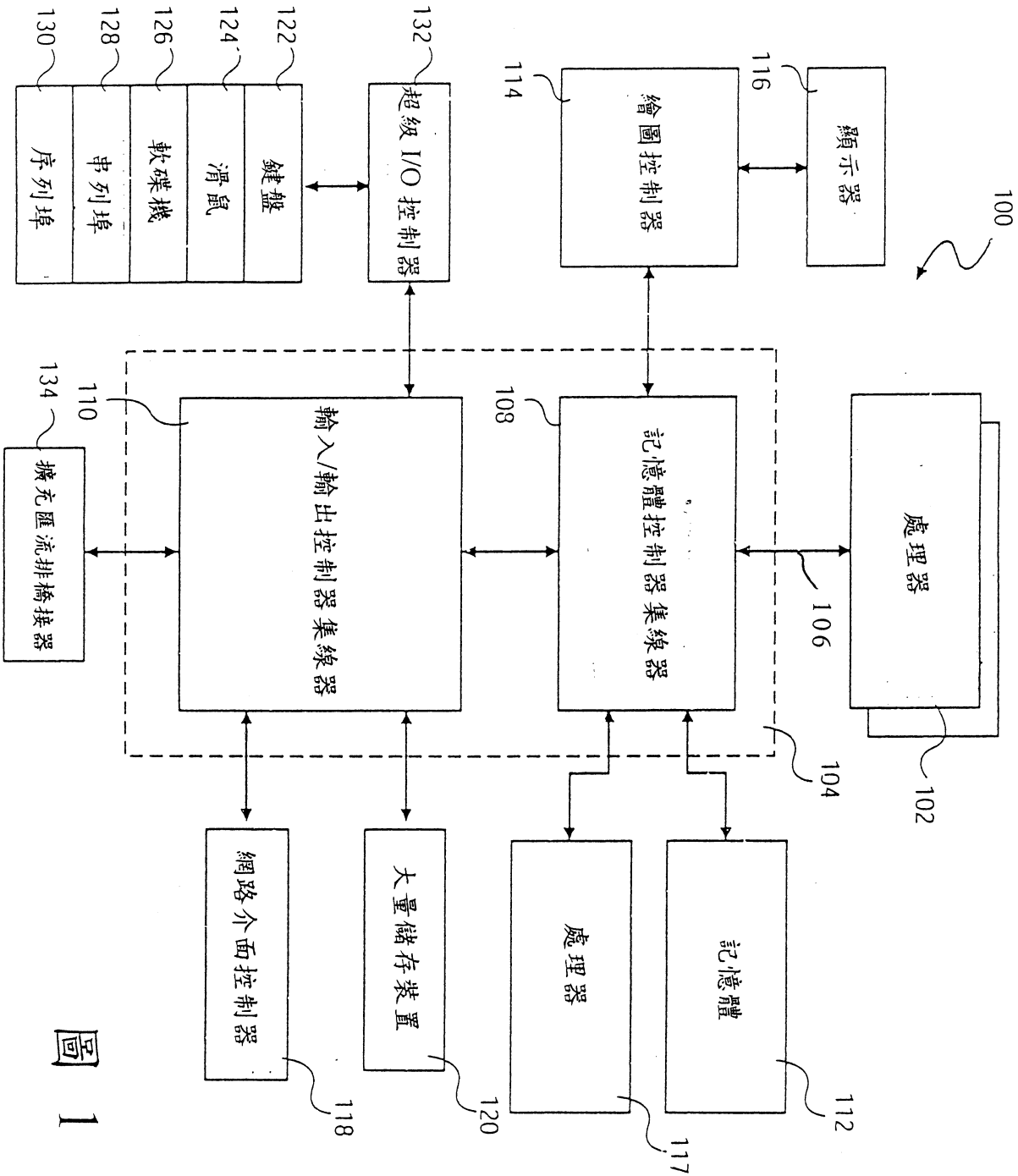


圖 1

修正替换頁
及
年 月 日

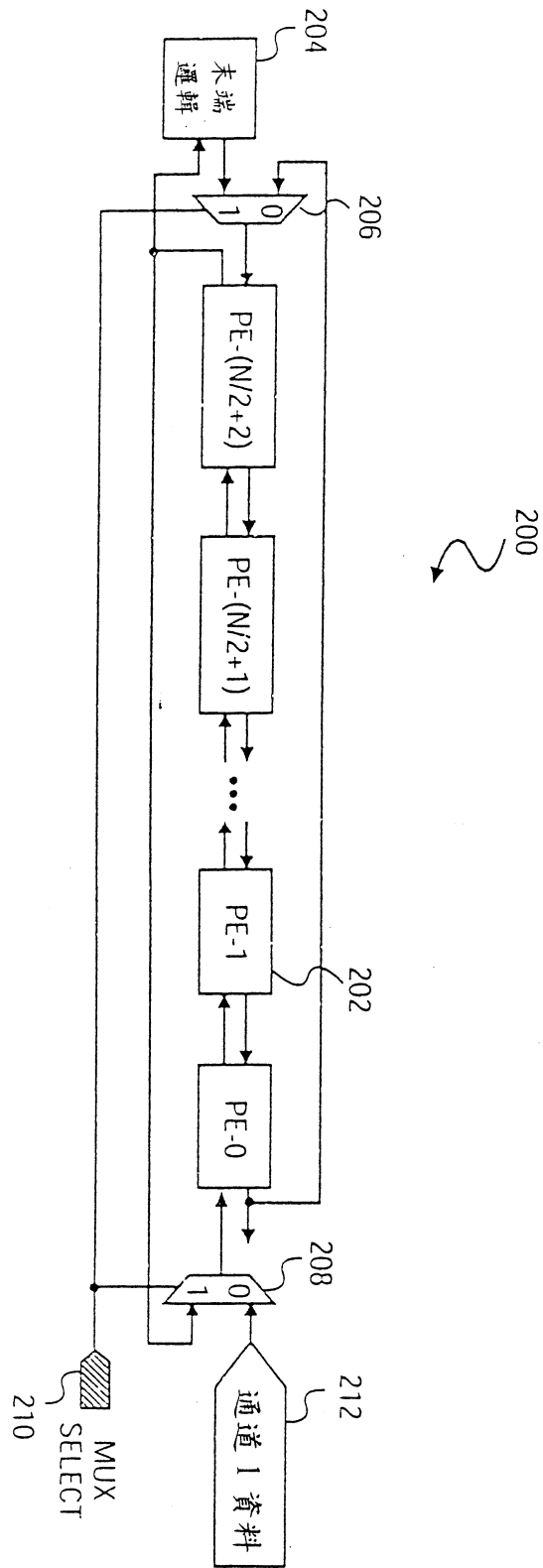


圖 2

98.11.6 研 究 所
研 究 所 研 究 員
研 究 所 研 究 員

修正替換頁
年 月 日

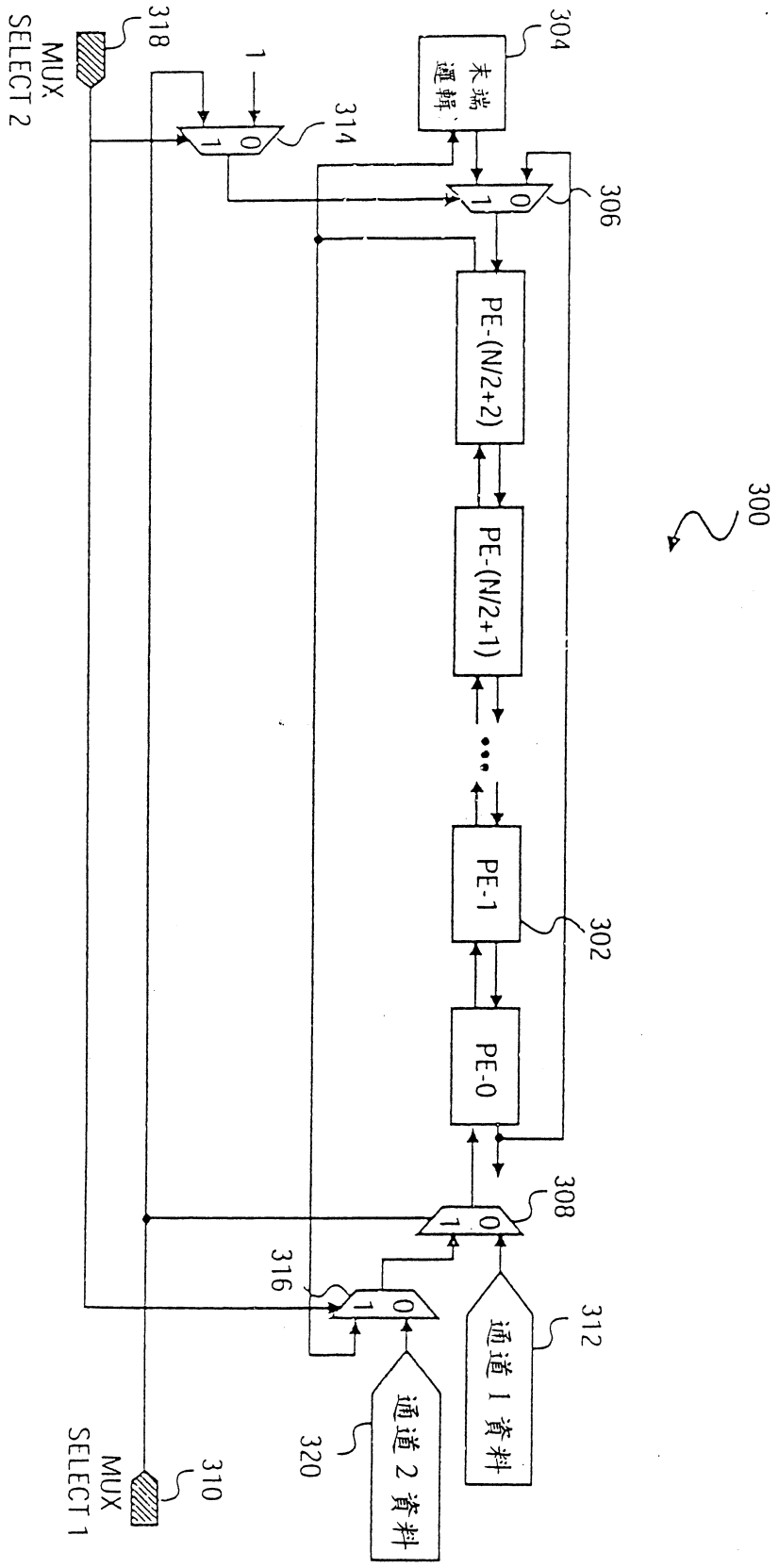


圖 3

83.5.6
日所提之

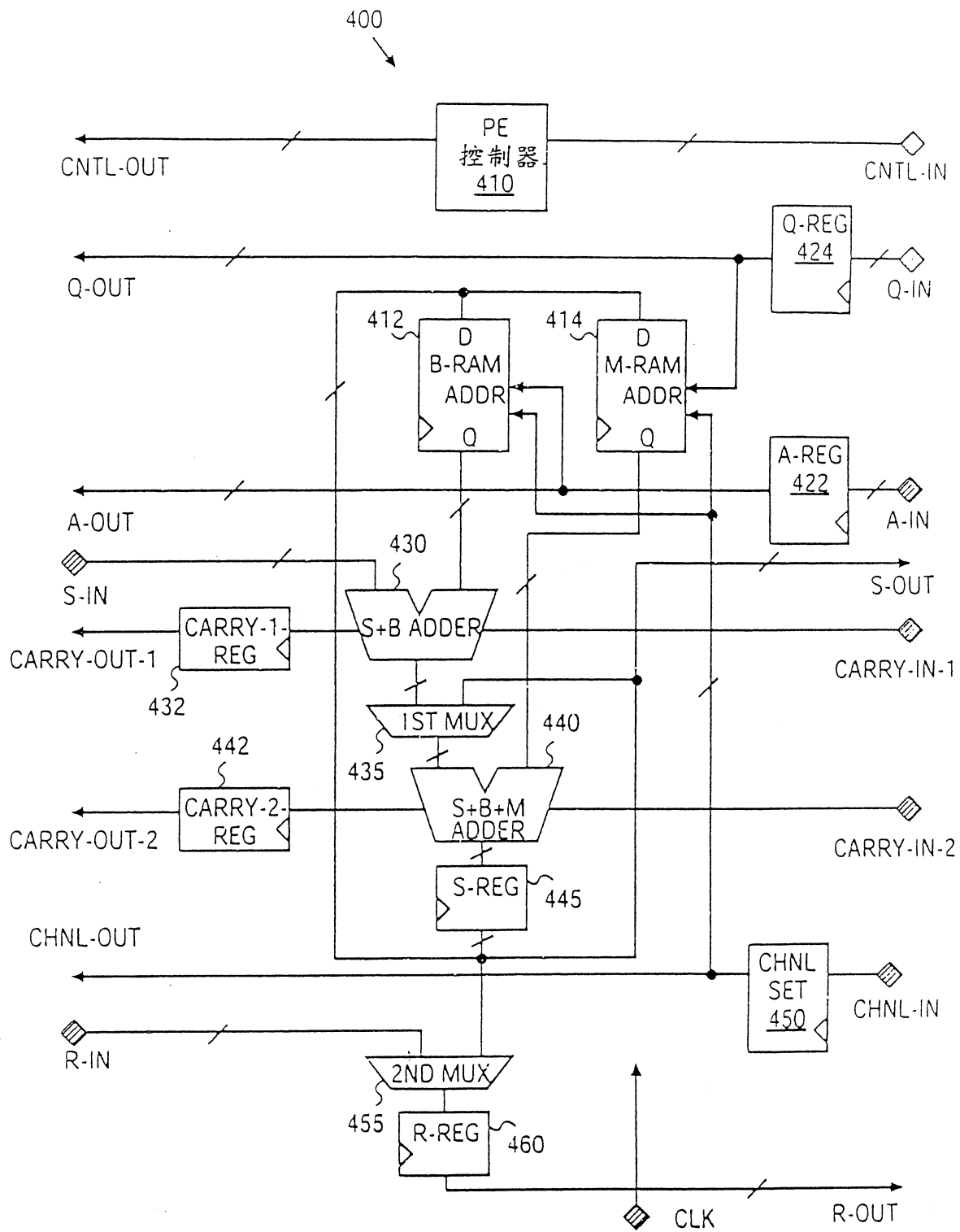


圖 4



循環	MUX SELECT	末端 邏輯	PE-6	PE-5	PE-4	PE-3	PE-2	PE-1	PE-0	輸入 暫存器
1	0								0	
2	1							1		
3	0						2		0	
4	1					3		1		
5	0						2		0	
6	1				4		2	1	0	
7	0			5		3		1		
8	1		6		4		2		0	
9	0			5		3		1	0	
10	1		6		4		2	1	0	
11	0			5		3		1	0	
12	1		6		4		2	1	0	
13	0			5		3		1	0	
14	1		6		4		2	1	0	
15	0		6		4		2	1	0	
16	1		6		4		2	1	0	
17	0		6		4		2	1	0	
18	1		6		4		2	1	0	
19	0		6		4		2	1	0	
20	1		6		4		2	1	0	

圖 5

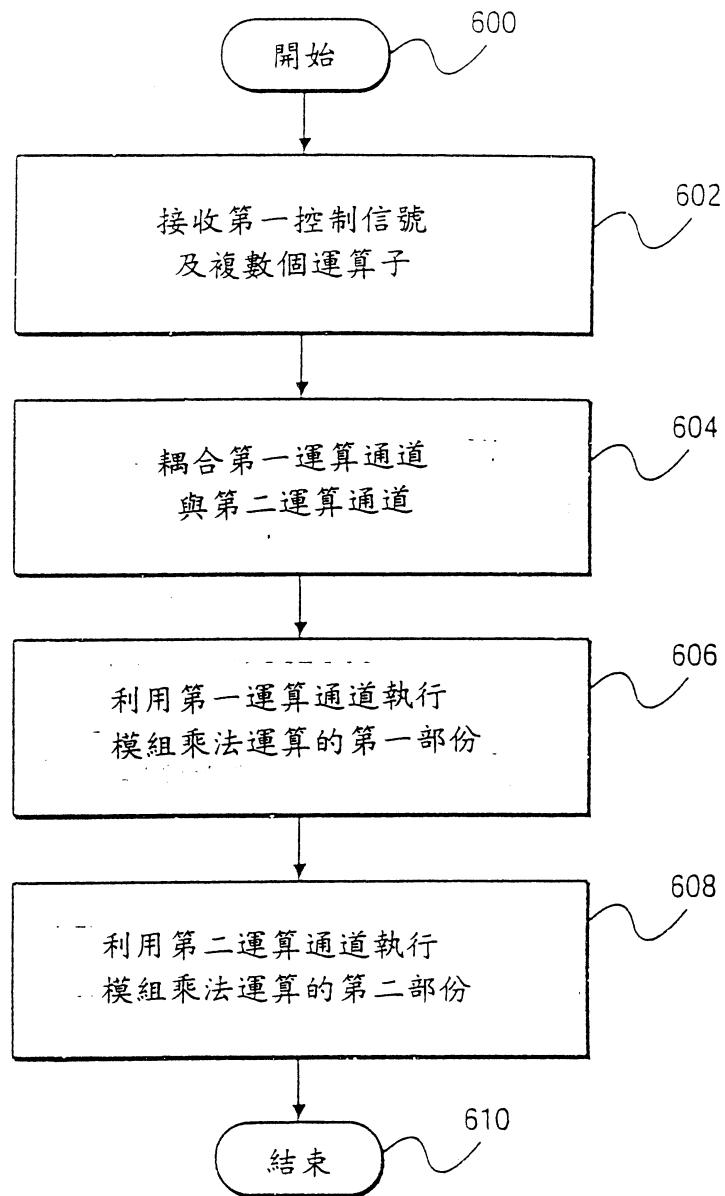
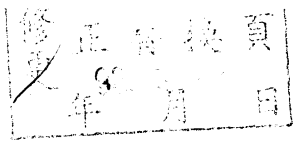


圖 6