公告本

申請日期	91-9-27
案　　號	91122355
類　　別	G06F 7/50

A4
C4

（以上各欄由本局填註）

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中　文	於蒙哥馬利乘法器處理元件中之組件減少
	英　文	COMPONENT REDUCTION IN MONTGOMERY MULTIPLIER PROCESSING ELEMENT
二、發明創作人	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：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）	申請專利，申請日期：	案號：	
美國	2001年09月28日	09/966,044	☑有 □無 主張優先權

有關微生物已寄存於：　　寄存日期：　　，寄存號碼：

五、發明說明（ 1 ）

發明背景

1.發明領域

本發明一般而言關於電腦。特定而言，係關於用於蒙哥馬利乘法器中的處理元件。

2.相關技藝說明

有一些應用包含了公用金鑰資料加密/解密，像是Rivest-Shamir-Adleman (RSA)演算法，其利用的演算法係使用對於大的數目之乘法及模數減法之組合。特別是，該RSA演算法重覆地實施X Y mod Z的運算(即X乘以Y除Z的餘數)。當處理大的數目時(例如在RSA為主的資料安全性中常用的1024位元的數目)，此演算法包含至少兩個耗時的運算(一乘法及一除法)，及餘數的偵測。蒙哥馬利乘法器經常用來實施此演算法。蒙哥馬利乘法器使用一種轉換來在單一運算中執行X Y mod Z，其藉由轉換X、Y及Z成為其它數目，例如A、B及M，來執行一轉換的運算，並倒轉轉換該結果。利用長序列的乘法，如果該轉換的運算比實際運算的耗時較少，決定一最終答案的整體時間可顯著地低於利用蒙哥馬利乘法器者。

一些蒙哥馬利乘法器使用一線性的收縮陣列，即一串鏈的相同處理元件(PE)，其中每個PE在每個牽涉到的數目中處理其一部份(例如4個位元)。該串鏈包含足夠的PE來保持所牽涉到最大的數目，包含過渡的結果。過渡資訊在運算期間係在相鄰的PE之間於兩個方向上輸送。

在一習用的線性收縮陣列中，蒙哥馬利乘法器(LSAMM)

五、發明說明（ 2 ）

，其三個參數中的兩個(基本上為B及M)，即經由連接到每個PE之匯流排來預先載入到該PE中。對於導引多重位元匯流排到數百個PE所需要的連接會加入顯著的複雜度到該電路。一習用的LSAMM亦在每一個PE中加入一解碼電路，以解碼一多重位元進位運算。每個PE必須包含專屬於執行該匯流排介面及進位解碼運算之電路，所以匯流排運算及多重位元承載者所需要的整個電路可由將此額外邏輯乘以在該LSAMM中的PE數目來決定。因為蒙哥馬利乘法器經常實施在具有固定可用數量電路之場域可程式閘極陣列(FPGA)中，所有額外的邏輯會消耗許多閘極，其另可用來增加PE的數目，或可利用到其它功能。

至少一個參數的倍數必須在一蒙哥馬利乘法開始之前來載入到一習用的蒙哥馬利乘法器。在軟體中預先計算這些非常大的數目之倍數為一非常耗時的處理，其會減慢任何需要蒙哥馬利乘法的運算。

圖式之簡單說明

本發明最佳地是參考以下的說明，以及用來說明本發明之具體實施例的附屬圖式來加以瞭解。在圖式中：

圖1所示為根據本發明一具體實施例的系統。

圖2所示為根據本發明一具體實施例之蒙哥馬利乘法器。

圖3所示為根據本發明一具體實施例之處理元件的架構。

圖4A所示為根據本發明一具體實施例中，直接載入初始參數到該串鏈的處理元件中的迴轉邏輯。

圖4B所示為根據本發明一具體實施例中，間接載入初始

五、發明說明（ 3 ）

參數到該串鏈的處理元件中的迴轉邏輯。

圖5所示為根據本發明一具體實施例中使用迴轉邏輯來實施的一流程圖。

發明之詳細說明

為了充分認識本發明，在下面的詳細說明中提出許多的特定細節。在其他情況下，為了避免混淆本發明，不會詳細說明已熟知的電路，如比較器。

本發明可實施在硬體、軟體或韌體中。本發明亦可實施為儲存在一機器-可讀取的媒體上，其可由至少一個處理器讀取及執行，以執行此處所述的運算。一機器-可讀取的媒體可包含用於以機器(如電腦)可讀取的形式來儲存或傳送資訊的任何機制。舉例而言，一機器-可讀取媒體可包含唯讀記憶體(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)，及其它者。

本說明的許多部份係以名詞「右方」、「左方」、「右手邊」、「左手邊」、「最右側」或「最左側」來代表本發明的部份。這些名詞代表如圖中所示的相對方向，其必須不能解釋做為本發明之實體實施的限制。

不同的具體實施例使用一線性收縮陣列蒙哥馬利乘法器(LSAMM)設計來載入初始參數的位元到一特定的處理元件(PE)中，並傳遞那些位元通過一串聯連接的串鏈之PE，藉此排除將所有PE並聯連接所需要的一匯流排。將該PE連接

五、發明說明（ 4 ）

在一串聯的串鏈並不會防止位元群組在PE之間平行地轉移。在本發明的說明中，「傳遞」代表在一串鏈的PE中由PE到PE傳送位元的群組。「傳遞通過」一特定的PE包含以下任何一項，1) 開始傳遞(一群組的位元並未自一相鄰PE所接收，但可遞送到另一個相鄰的PE)，2) 結束傳遞(一群組的位元自一相鄰的PE接收，但並不遞送到另一個相鄰的PE)，及3) 繼續傳遞(一群組的位元自一相鄰的PE接收，且遞送到另一個相鄰的PE)。傳遞並不需要每個位元群組到達該串鏈中的每一個PE。

在一具體實施例中，該LSAMM亦執行該參數所有需要的倍數之預先計算，其使用與執行該蒙哥馬利乘法相同的電路。利用不同電路元件的多重用途可降低每個PE所需要的邏輯數量，當相較於一習用的LSAMM時。在一具體實施例中，蒙哥馬利乘法器係實施在一具有固定數目可用的邏輯之FPGA中。該電路的節省可用來在該FPGA中包含更多的PE。

圖1所示為根據本發明一具體實施例的系統。在圖1所示的具體實施例中，系統100包含一處理器(CPU) 110，其經由輸入/輸出(I/O)邏輯130及記憶體匯流排160耦合到LSAMM 150。在一具體實施例中，系統100亦包含一加速繪圖處理器(AGP) 120，及一耦合到I/O邏輯130之記憶體140，及耦合許多其它裝置(未示出)到I/O邏輯130之I/O匯流排170。在圖1之具體實施例中，該LSAMM 150包含一蒙哥馬利乘法器(MM)控制器180，其連接到記憶體匯流排160，允

五、發明說明（ 5 ）

許該LSAMM 150由該CPU 110及/或其它裝置定址做為一區塊的記憶體，但其它具體實施例將LSAMM 150以其它方式來耦合。LSAMM 150亦包含一串鏈的串聯連接的處理元件(PE) 190-x，其經由該串鏈的一末端連接到MM控制器180，所以一組參數(如A、B、M)可提供給該串鏈，而一結果(如R)可經由在該串鏈末端處的PE來自該串鏈接收。在圖1的具體實施例中，任何可寫入一組參數到LSAMM 150及自該LSAMM 150讀取一最終結果之裝置皆可使用LSAMM 150來執行一蒙哥馬利乘法。雖然該名稱「A」、「B」及「M」在整個說明書中用來代表在一蒙哥馬利乘法中的參數，這些為原始的命名。其可使用任何其它的名稱但不背離本發明的精神及範圍。

圖2所示為根據本發明一具體實施例之線性收縮陣列蒙哥馬利乘法器。在圖2所示的具體實施例中，使用一串鏈的串聯連接的PE來執行具有一組參數A、B、M之蒙哥馬利乘法，其中每個參數係散佈在PE中，每個PE一個數字。一數字係定義成由每個PE處理之每個參數的位元數目。在此整個說明書中所使用的範例具體實施例中，一數字為一4位元的16進位數目，而每個PE係每次以4位元的A及/或4位元的B及/或4位元的M來運算。在其它具體實施例中，可使用其它大小的數字，而每個PE的邏輯即依每個範例有所不同。

圖2所示的具體實施例中顯示一串鏈的數量N+3個PE，編號由190-0到190-(N+2)，並標示為PE-0到PE-(N+2)。在一具體實施例中，該LSAMM 150運作在1024位元的參數，而該

五、發明說明（ 6 ）

N的數值為256。在此具體實施例中的PE數目為259，包含256個PE來保持256個參數的16進位數字，而3個額外的PE則在處理期間容納過渡的結果。蒙哥馬利乘法器(MM)控制器180由一次一個數字透過PE-0傳送參數A、B、M到該串鏈中來控制該處理。MM 180亦傳送控制碼c及其它數值q到PE-0中來用於傳遞通過該串鏈的PE，其在稍後說明。

在一具體實施例中，該串鏈的PE係由順序地傳送每個參數B及M到左方來設定為一蒙哥馬利乘法，一次一個數字，由MM控制器180到PE-0、PE-1、PE-2等，直到每個參數係分佈在PE-0到PE-N之內。在一具體實施例中，每個參數B及M的倍數即在PE中計算，並儲存在PE中。為了執行實際的蒙哥馬利乘法，參數A即順序地一次一個數字地傳送到左方，由MM控制器180到PE-0、PE-1、PE-2等，以運作在該儲存的B及M之倍數。當A的所有數字已經傳送通過該串鏈的PE時，該乘法運算即完成，其結果R即存在於PE中。如果蒙哥馬利乘法完成，該結果R即傳送到右方通過該PE，並到MM控制器180中。在一具體實施例中，如果該結果R為下一個蒙哥馬利乘法之初始參數，如同常見於RSA運算中的例子，R的倍數即經過計算，並儲存在PE中，而不傳送到該MM控制器180中，而一新的參數A即如前述地傳遞通過該PE，以執行下一個蒙哥馬利乘法。

在所示的具體實施例中，參數A、B、M及結果R其每一個代表一大的數目，其分佈到該串鏈的PE中。控制碼c其每個足夠地小，以置於一單一PE中，而每個控制碼導引該PE

五、發明說明（ 7 ）

，其中其目前之位置係要執行目前在該PE中所包含之數值的運算。控制碼係傳送到具有相關參數的數字之向左通過該PE。對於每種運算，傳送通過該PE之控制碼的序列為預先決定的。在一具體實施例中，該預先決定的序列係儲存在MM控制器180中，並依需要提供給PE-0。在其它具體實施例中，該預定的序列係儲存在MM控制器180之外，並提供給MM控制器180來傳送到PE-0。

q的數值亦足夠小來符合於每個PE，並傳送通過左方的該PE，以及該相關參數的數字來進一步定義在每個PE中的運算。在一具體實施例中，蒙哥馬利乘法運算之q數值係在PE-0中決定，並傳送於其上，而其它運算的q數值為預定的序列，其儲存在或外部於MM控制器180，如同為該控制碼。

在該LSAMM 150的運算期間，每個PE在兩個方向中傳送資訊到相鄰的PE。在一具體實施例中，每個PE在一個時脈循環中執行一內部運算，如同由該PE的目前數值c、q及該數字A所指定，然後等待一時脈循環來傳送資訊到相鄰的PE，以自相鄰的PE接收資訊。在一具體實施例中，該偶數的PE在一偶數的時脈循環中的特定蒙哥馬利乘法中執行運算，並在該奇數時脈循環中等待來自相鄰的奇數PE之資訊，而該奇數的PE在該奇數時脈循環中的相同蒙哥馬利乘法中執行運算，並在該偶數時脈循環中等待來自相鄰的偶數PE之資訊。在一具體實施例中，這些運算及等待之交替的循環係在每一個其它的時脈循環由輸入所需

五、發明說明（ 8 ）

要的參數及控制碼之數字到PE-0中來產生，及在該中介的時脈循環上輸入零及一非運算控制碼到PE-0中。然後此非運算循環傳遞下到交叉有該運算循環之串鏈。藉此載入一1024位元數目到一串鏈的4位元PE在一具體實施例中採取512個時脈循環。

圖3所示為根據本發明一具體實施例之處理元件的架構。在圖3的所示具體實施例中，PE 190包含PE控制邏輯310、兩個儲存元件(B-RAM 312及M-RAM 314)、兩個位址暫存器(Q-暫存器324及A-暫存器322)、兩個加法器(S+B加法器330及S+B+M加法器340)、兩個多工器(第一多工器335及第二多工器355)、兩個進位暫存器(進位1暫存器332及進位2暫存器342)、一累積暫存器(S-暫存器345)，及一結果暫存器(R-暫存器360)。雖然說明一單一PE 190，在一具體實施例中，PE 190為在該串鏈中每一個PE 190-x之原型。在所示的具體實施例中，在圖3底部所示的連接為多個PE所共用，所示的連接到具有PE之右方介面到右方，及所示的連接到具有PE之左方介面到左方，並使得來自一PE的輸出連接到該相鄰PE之類似命名的輸入。例外為PE-0，其介面到在右方的MM控制器180，及PE(N+2)，其左方沒有PE，而在一具體實施例中，其耦合到一迴轉電路，以允許某些資料的迴轉。在一具體實施例中，所有的PE具有一共用的時脈輸入Clk。在其它具體實施例中，該時脈信號被緩衝，並分散在PE的群組之間，以避免信號載入問題。

在一具體實施例中，Clk、Carry-In-1、Carry-Out-1、

五、發明說明（ 9 ）

Carry-In-2、Carry-Out-2及所有內部的連接來傳遞那些信號，其每個包含一個位元，而Cntl-In及Cntl-Out包含容納不同控制碼所需要的位元數目。圖3所示的所有剩餘連接包含由每個PE所處理的位元數目，例如對於所示的具體實施例為每個4位元。在一具體實施例中，每個PE亦依需要包含其它輸入及輸出，例如一重置輸入(未示出)。

在一具體實施例中，圖3的不同邏輯元件執行以下的運算：控制邏輯310閂鎖自該PE接收的一控制碼到右方，其使用該控制碼來在一目前的時脈循環期間控制本PE之邏輯元件，然後傳送該控制碼到左方的該PE。儲存元件B-RAM 312係用來儲存在該PE串鏈中所儲存的每個B的倍數的一個數字，而使用儲存元件M-RAM 314來儲存在該PE串鏈中所儲存的每個M的倍數的一個數字。A-暫存器322及Q-暫存器324保持該位址，其分別選擇在B-RAM 312及M-RAM 314內所想要的位置，(同時用於讀取及寫入)，且亦傳送這些位址到左方的該PE。S+B加法器330係用來加入一選擇的位置之內容在B-RAM 312到在該PE中的S-暫存器之內容到左方，其包含任何透過在該PE中S+B加法器之Carry-In-1的輸入接收的任何進位位元到右方。Carry-1-暫存器332閂鎖來自S+B加法器330之任何進位位元，並在下一個時脈循環期間提供它做為一進位位元到在左方的該PE中的S+B加法器。當選擇第一多工器335之左手邊輸入時，S+B+M加法器340加入該S+B加法器330之輸出到M-RAM 314中一選擇位置之內容中。當選擇第一多工器335之右手邊輸入時，S+B+M加法器

五、發明說明（ 10 ）

340加入S-暫存器345的內容到M-RAM 314中該選擇位置之內容。任何接收的進位位元係由該PE提供到該右方通過該Carry-In-2輸入，而任何產生的進位位元在下一個時脈循環中係閂鎖到該Carry-2-暫存器342來由該PE使用到該左方。該S+B+M加法器340的輸出即閂鎖到S-暫存器345中，其做為過渡結果的一累積暫存器。該S-暫存器345的輸出係分散到每個B-RAM 312、M-RAM 314、第一多工器335、第二多工器355及該S-Out輸出。R-暫存器360閂鎖S-暫存器345之輸出，如果選擇第二多工器355之右手邊輸入，否則閂鎖在該PE中R-暫存器的內容到該左方。

在圖3的具體實施例中，Clk係用來閂鎖資料到該控制邏輯中，及到該Q-、A-、S-、R-、Carry-1-及Carry-2-暫存器中，及在B-及M-RAMS中時脈寫作運算，而兩個加法器、兩個多工器、及在B-及M-RAMS中的讀取運算為組合性，即在一輸入處的任何改變即無關於時脈狀態而傳遞通過到該控制元件的輸出。在其它具體實施例中，該B-及M-RAM使用一時脈的輸入來讀取以及寫入運算。在一具體實施例中，選擇了時脈速率，所以在PE 190中最差狀況的組合延遲係小於一時脈循環。來自Clk輸入到其它電路元件之特定連接未示於圖3，以避免使得圖面覆蓋太複雜。

控制邏輯310包含控制PE 190之運算所需要的邏輯，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310包含一解碼器電路來轉換該控制碼到必要的控制信號。在其它具體實施例中，該控制碼可簡單地閂鎖，其中該

五、發明說明（ 11 ）

控制碼的每個位元指定一特殊的控制信號。在一具體實施例中，該控制碼指定運算包含但不限於：選擇第一多工器335的兩個輸出中的一個，選擇第二多工器355的兩個輸入之一，寫入到B-RAM 312、寫入到M-RAM 324，重置該A、Q、S及R暫存器中一或多個，並約束該時脈信號到許多邏輯元件。

因為一蒙哥馬利乘法以B及M的倍數運算，一具體實施例預先計算在PE內的倍數，使用一蒙哥馬利乘法所使用的相同邏輯。在圖3所示的具體實施例中，該儲存元件包含隨機存取記憶體(RAM)、標示為B-RAM及M-RAM來代表所儲存的參數。另一個具體實施例使用一種記憶體技術，而非RAM，用於儲存元件B-RAM 312及M-RAM 314。共同地，所有在PE串鏈中的B-RAM 312提供儲存空間給(0 x B), (1 x B), (2 x B)等的數值。每個PE之B-RAM 312提供每個B的倍數之一個數字之儲存空間。在一具體實施例中，其中每個PE運算在一16進位數字，B-RAM 312包含16個4位元的儲存位置來保持相對應的(0 x B)到(15 x B)之數字，而M-RAM 314包含16個4位元儲存位置來保持(0 x M)到(15 x M)之相對應的數字。在一具體實施例中，其中每個PE處理除了4之外的位元數目，在每個RAM中的位置數目即依此來改變，以定址及儲存所需要的倍數的數目。

該PE 190的邏輯可用於許多種方式，根據當時所要執行的運算。在一具體實施例中，該PE執行以下每一項，其在以下的段落中更為詳細地說明：

五、發明說明（ 12 ）

1) 載入初始參數到B-RAM及/或M-RAM。

2) 預先計算B的倍數，並儲存在B-RAM中。

3) 預先計算M的倍數，並儲存在M-RAMS中。

4) 執行一蒙哥馬利乘法。

載入初始參數到B-RAM及/或M-RAMS

在一LSAMM中，每個蒙哥馬利乘法以該PE中的初始參數B及M開始。在一些條件下，該蒙哥馬利乘法的結果為下一個蒙哥馬利乘法之初始參數，所以初始參數不需要載入。在一具體實施例中，在一乘法S-暫存器345的末端處包含該累積的結果之數字，然後載入到B-RAM 312(或M-RAM 314)中，其位在由A-暫存器322(或Q-暫存器324)所指定的位址處，如同下一個蒙哥馬利乘法之初始參數的一個數字。

在其它條件下，初始參數並未包含在PE中，所以該初始參數即由一外部來源來供應。在一具體實施例中，一初始參數輸入到該串鏈的末端，並傳遞通過該PE的S-暫存器，直到每個數字在其適當的PE之S-暫存器中，藉此該數字寫入到該相對應的RAM中。請參考圖3，藉由歸零B-RAM 312及M-RAM 314之輸出，並選擇第一多工器335的左手邊輸入，加法器330及340將未改變地傳送通過在S-In處的數值，將其載入到S-暫存器345，由此該數值可在S-Out處使用，藉此使得一數值傳遞通過S-暫存器。但是，因為該S-暫存器設計來傳送資料由左到右，在一具體實施例中，該參數開始傳遞通過S-暫存器，其由PE-(N+2)開始。在一具體實施例中，MM控制器180具有一獨立的輸出到PE-(N+2)之S-In

五、發明說明（ 13 ）

，並輸入該內部參數的數字到PE-(N+2)中。在其它具體實施例中，MM控制器180輸入該初始參數的數字到PE-0的位址暫存器中，並由右到左傳遞該數字通過該PE的串鏈。然後一迴轉電路迴路該PE-(N+2)的位址暫存器輸出回到PE-(N+2)之S-In輸入，由其該數字由左到右傳遞通過該S-暫存器，如前所述。該迴轉運算及電路之具體實施例係在以下的段落中說明。

圖4A所示為根據本發明一具體實施例中，直接載入初始參數到該串鏈的處理元件中的迴轉邏輯。圖4B所示為根據本發明一具體實施例中，間接載入初始參數到該串鏈的處理元件中的迴轉邏輯。圖5所示為根據本發明一具體實施例中使用迴轉邏輯來實施的一流程圖。圖5的流程圖500係相對於圖4A、4B之迴轉邏輯來說明，並進一步參考到圖3之PE。在流程圖500之方塊510中，一初始參數的數字為來自MM控制器180之輸出。在使用圖4A的一具體實施例中，該初始參數的數字係直接提供給迴轉多工器425，並略過方塊520。在使用圖4B的電路之另一個具體實施例中，該初始參數的數字即輸出到PE-0的A-暫存器322，藉此將它們在方塊520中傳遞通過該串鏈的PE之A-暫存器，直到到達PE-(N+2)。來自PE-(N+2)之A-暫存器322，該初始數值的數字即提供給迴轉多工器425。在一具體實施例中，使用該Q-暫存器，而非A-暫存器，以由PE-0到PE-(N+2)傳遞該初始參數的數字。在圖4A及4B之具體實施例中，該初始數值的數字係迴轉回通過迴轉多工器425到PE-(N+2)之S-In輸入，如方塊530

五、發明說明（ 14 ）

。在方塊540中，該初始參數的數字係傳遞通過該S-暫存器，直到每個數字依前述的方法到達其適當的PE。

當載入初始參數時，該信號LoopSel選擇該迴轉多工器之右手邊輸入，所以該初始參數的數字即輸入到S-In。如果一初始參數並不載入到該串鏈的PE，該信號LoopSel選擇該迴轉多工器425之左手邊輸入，其輸入零到S-In中。在一具體實施例中，該信號LoopSel由MM控制器180所提供。在其它具體實施例中，該信號LoopSel由額外的迴轉邏輯(未示出)產生，其係回應於一控制碼或一序列的控制碼，其僅有該迴轉邏輯可辨識。

在另一具體實施例中，迴轉多工器425係連接到一內部PE(例如藉由連接到PE-N而非PE-(N+2)之迴轉多工器425)，將連接到該PE的S-Out輸出的迴轉多工器425之左手邊輸入到左方。此具體實施例允許載入初始參數，而不需要傳送資料通過位在該串鏈末端處的額外PE，其通常並不保持該初始參數的任何部份。

<u>預先計算B的倍數，並儲存在B-RAM中</u>

在圖3所示的具體實施例中，計算每個B的倍數的一數字，並儲存那些數字在B-RAM 312中，藉由在每個PE中執行以下的步驟：

1) 清除B-RAM 312中的位置0之內容為0，其藉由寫入所有皆為零的資料到位置0。在一具體實施例中，此運算係由零化該A-暫存器322之內容來執行，以選擇位置0，並零化該S-暫存器345之內容來提供資料寫入到位置0。

五、發明說明（ 15 ）

2) 載入正確的B數字到S-暫存器345中，其透過先前在「載入初始參數到B-RAM及/或M-RAM中」的章節中所描述的處理。

3) 清除該Q暫存器，設定M-RAM為「寫入」，並由S-暫存器345寫入B的數字到M-RAM 314的位置0中。M-RAM 314為此數字暫時的保持地方，且可在該預先計算步驟的結束時來清除。

4) 設定M-RAM 314為「讀取」，並留下Q-暫存器324被清除來連續地自M-RAM 314讀取B的數字。設定B-RAM 312為「寫入」，清除該S-暫存器345，並設定該A-暫存器322為「0」。

5) 選擇該多工器335的右手邊輸入，所以該S+B+M加法器340將來自M-RAM 314的B之數字與S-暫存器345中目前的數字相加，並儲存該總和成為在S-暫存器345中新的數值，其包含在Carry-In-2處所接收的任何相關進位位元之影響(任何由此加法所產生的進位位元即閂鎖到Carry-2-Reg 342中，由左方的該PE使用)。

6) 增加在A-暫存器322中的數值，利用在S-暫存器345中的每個新數值，所以在S-暫存器345中的變化數值即儲存到B-RAM 312中連續的位置0、1、2、3等。在增加通過所有的B倍數之後，在B-RAM 312中的結果為該位置0包含一數字0 x B = 0，位置1包含相同的數字 1 x B，位置2包含相同的數字2 x B，位置3包含相同的數字3 x B等。當此處理施加到PE 0到N時，即完成該預先計算及B之倍數的儲存。

五、發明說明（ 16 ）

預先計算M的倍數，並儲存在M-RAM中

在圖3所示的具體實施例中，計算每個M的倍數的一數字，並儲存那些數字在M-RAM 314中，藉由在每個PE中執行以下的步驟：

1) 藉由寫入零到每個位置來清除M-RAM的內容。在一具體實施例中，此係藉由零化該S-暫存器345的內容來執行，並重覆地寫入該零數值到該M-RAM中，而增加Q-暫存器324之內容。

2) 載入正確的M數字到S-暫存器345中，其透過先前在「載入初始參數到B-RAM及/或M-RAM中」的章節中所描述的處理。

3) 清除該Q暫存器，並由S-暫存器345寫入M的數字到M-RAM 314的位置0中。位置0為此數字暫時的保持地方，且可在該預先計算步驟的結束時來清除。

4) 選擇該多工器335的右手邊輸入，所以該S+B+M加法器340將加入來自M-RAM 314之數字到S-暫存器345中目前的數字，並儲存該總和成為在S-暫存器345中新的數值，其包含在Carry-In-2處所接收的任何相關進位位元之影響(任何由此加法所產生的進位位元即閂鎖到Carry-2-Reg 342中，由左方的該PE使用)。依此方式，在S-暫存器345中的數值將利用每個加法來連續地改變通過M, 2M, 3M等相同的數字。

5) 在一遞增的計數器及零之間交替該Q-暫存器324之內容：1、0、2、0、3、0等。當該Q-暫存器保持一零時，放

五、發明說明（ 17 ）

置M-RAM 314在一讀取狀態來由位置0讀出M的數值。當該Q-暫存器保持該遞增的計數器數值之一時，放置M-RAM在一寫入狀態，以由S-暫存器345寫入該累積的數值到該位置中。依此方式，該M的數字將由M-RAM 314中的位置0讀取，並加入到S-暫存器345中該累積的數值，其包含任何接收的進位位元之影響。然後該總和將寫入到M-RAM 314中的一位置，其利用每次寫入運算來遞增。在M-RAM 314中的結果為位置1包含M的一數字，位置2包含2M的相同數字，位置3包含3M的相同數字等。

6) 零化該S-暫存器345及該Q-暫存器324，並寫入S-暫存器345的零內容到M-RAM 314的位置0中。當該處理已經應用到PE 0到N時，即完成預先計算及儲存M的倍數。

在用於實施前述運算的具體實施例中，該A-暫存器322及Q-暫存器324之內容即經由一控制碼來清除為零。在另一具體實施例中，該A-暫存器322及Q-暫存器324之內容即由傳遞該零數值通過該PE串鏈來設定為零，如同在A-及Q-暫存器中的其它數值。

執行一蒙哥馬利乘法

在圖3所示的具體實施例中，每個PE依以下方式來在一蒙哥馬利乘法中執行：該A-暫存器322閂鎖A的一數字來選擇在B-RAM 312中的B之倍數的數字，該Q-暫存器324閂所一q值來選擇在M-RAM 324中M的倍數之數字，而控制邏輯310閂鎖一控制碼來在目前的時脈循環期間控制PE 190的邏輯元件。所有三個數值由該PE接收到右方，並在以下的時脈

五、發明說明（ 18 ）

循環中傳送到左方的該PE。使用該S+B加法器330，B-RAM 312之選擇的位置即加入到在左方之該PE中S-暫存器之目前內容。進位位元使用該Carry-In-1輸入及該Carry-Out-1輸出來由右到左傳遞，所以目前PE的S+B加法器330配合其它PE的S+B加法器來動作，以加入一選擇的B之倍數的數值到在該S暫存器中一過渡結果之向右移位(一個位元)的數值。依照類似的方式，該S+B+M加法器340使用在Carry-In-2及Carry-Out-2處的傳遞進位位元來配合於其它PE的S+B+M加法器來執行一較大的加法。其選擇第一多工器335的左手邊輸入，所以該S+B加法器330的輸出即加入到在M-RAM 314之選擇的位置中M的倍數。該總和閂鎖到S-暫存器345中做為新的過渡結果，完成由目前時脈循環的控制碼所定義的運算。如前所述，接著為等待來自相鄰PE之資訊的時脈循環，然後剛描述的處理即依需要重覆許多次來傳遞所有A的數字通過PE。當所有A的數字已經傳遞通過PE時，在S-暫存器345中的數值為該蒙哥馬利乘法之結果的一數字。當所有A的數字已經傳遞通過所有的PE，該蒙哥馬利乘法即完成。

如果該結果係要做為在一系列連續的蒙哥馬利乘法中新的初始參數，則該S-暫存器345之內容即載入到B-RAM 312中做為B的數字，而倍數即如先前在「預先計算B的倍數及儲存在B-RAM中」的段落中所述來計算。如果該結果為最終結果，該結果即移位通過在右方的PE，直到所有結果的數字已經移位到MM控制器180中，由此該結果可用於該系

五、發明說明（ 19 ）

統中的其它裝置。在一具體實施例中，該S-暫存器345的內容係透過在每一個PE中多工器355的右手邊輸入來載入到R-暫存器360中，然後所有R-暫存器360的內容即傳送通過在右方的彼此來進入MM控制器180，藉由在每一個PE中選擇該多工器355的左方輸入。在另一具體實施例中，R-暫存器360及第二多工器355並未包含在PE中，而該結果即使用S-In及S-Out連接經由每一個PE的S-暫存器來傳送到右方，其中如同原始參數的相同方式即如「載入初始參數到該B-RAM及/或M-RAM中」所述來載入。

前述的說明係要解釋而非限制。本技藝專業人士將可進行變化。那些變化係要包含在本發明內，其僅受限於所附申請專利範圍的精神及範圍之內。

A5
B5

四、中文發明摘要（發明之名稱：　於蒙哥馬利乘法器處理元件中之組件減少　）

本發明揭示一種蒙哥馬利乘法器電路，其具有一串鏈的處理元件，藉由傳遞一初始參數通過用於其它目的之暫存器來在每個處理元件中使用較少的電路邏輯。在每個處理元件中的累積暫存器係用來傳遞該初始參數通過該串鏈。在一具體實施例中，該初始參數首先傳遞通過位址暫存器，直到其到達該串鏈的末端，然後在相反方向上通過該累積暫存器來繞回。在一具體實施例中，用於蒙哥馬利乘法中至少一參數的倍數係使用執行該蒙哥馬利乘法中所使用的相同邏輯元件來在該蒙哥馬利乘法器的處理元件中預先計算。

英文發明摘要（發明之名稱：　COMPONENT REDUCTION IN MONTGOMERY MULTIPLIER PROCESSING ELEMENT　）

A Montgomery multiplier circuit with a chain of processing elements uses less circuit logic in each processing element by propagating an initial parameter through registers used for other purposes. An accumulation register in each processing element is used to propagate the initial parameter through the chain. In one embodiment the initial parameter is first propagated through address registers until it reaches the end of the chain, and is then looped back through the accumulation registers in the reverse direction. In one embodiment, multiples of at least one parameter used in a Montgomery multiplication are pre-calculated in the processing elements of the Montgomery multiplier using the same logic elements used in performing the Montgomery multiplication.

五、發明說明（ 20 ）

元件符號說明

110	處理器(CPU)
130	輸入/輸出(I/O)邏輯
140	記憶體
160	記憶體匯流排
180	蒙哥馬利乘法器(MM)控制器
310	控制邏輯
330	加法器
335	多工器
425	迴轉多工器
AGP	加速繪圖處理器
FPGA	場域可程式閘極陣列
LSAMM	線性收縮陣列蒙哥馬利乘法器
MM	蒙哥馬利乘法器
PE	處理元件
RAM	隨機存取記憶體
ROM	唯讀記憶體

六、申請專利範圍

1. 一種供於蒙哥馬利乘法器處理元件中組件減少之裝置，包括：

一在線性收縮陣列蒙哥馬利乘法器中的一第一處理元件，該第一處理元件包含：

一第一儲存元件；及

一第一累積暫存器，其耦合於一相鄰第二處理元件的一第二累積暫存器，以傳遞一第一初始參數通過該第一及第二累積暫存器，該第一累積暫存器進一步耦合到該第一儲存元件來載入該第一初始參數的一部份到該第一儲存元件中。

2. 如申請專利範圍第1項之裝置，其中：

該第一累積暫存器進一步載入該第一初始參數的第一組倍數的一部份到該第一儲存元件中。

3. 如申請專利範圍第1項之裝置，其中：

該第一處理元件進一步包含耦合到該第一累積暫存器之一第二儲存元件，以儲存傳遞通過該第一及第二累積暫存器之一第二初始參數的一部份。

4. 如申請專利範圍第3項之裝置，其中：

該第一累積暫存器進一步載入該第二初始參數的第二組倍數的一部份到該第二儲存元件中。

5. 如申請專利範圍第1項之裝置，其中：

該第一處理元件進一步包含耦合到該第一儲存元件之一第一位址暫存器，以定址在該第一儲存元件中的位置，並耦合到在該第二處理元件中的一第二位址暫存

六、申請專利範圍

器，以傳遞該第一初始參數到該第一及第二位址暫存器，其係在傳遞該第一初始參數通過該第一及第二累積暫存器之前。

6. 如申請專利範圍第5項之裝置，其中：

該第一初始參數係要傳遞通過該第一及第二位址暫存器，其係與傳遞通過該第一及第二累積暫存器為相反的方向。

7. 如申請專利範圍第1項之裝置，其中：

該第一累積暫存器係進一步在一蒙哥馬利乘法期間來累積過渡的結果。

8. 一種供於蒙哥馬利乘法器處理元件中組件減少之系統，包括：

一處理器；

一耦合到該處理器之記憶體；及

一耦合該處理器之一線性收縮陣列蒙哥馬利乘法器，並包含：

一組串聯連接的處理元件，其具有累積暫存器來傳遞一初始參數通過該累積暫存器，並在開始一蒙哥馬利乘法之前儲存來自該累積暫存器之該初始參數到該處理元件中的儲存元件，其中該累積暫存器係要在蒙哥馬利乘法期間保持該過渡結果。

9. 如申請專利範圍第8項之系統，其中：

該組串聯連接的處理元件進一步包含耦合到該儲存元件之位址暫存器，以定址在該儲存元件中的位置，而且

六、申請專利範圍

該位址暫存器進一步傳遞該初始參數通過該位址暫存器，其係在傳遞該初始參數通過該累積暫存器之前。

10. 如申請專利範圍第9項之系統，其中：

該位址暫存器進一步傳遞該初始參數通過該位址暫存器，其係與傳遞該初始參數通過該累積暫存器為相反的方向。

11. 一種供於蒙哥馬利乘法器處理元件中組件減少之裝置，包括：

一在一線性收縮陣列蒙哥馬利乘法器中的第一處理元件，該第一處理元件包含：

一第一儲存元件；

一耦合到該第一儲存元件之加法器，以計算一第一初始參數的倍數之一部份；及

一耦合到該加法器及該第一儲存元件之累積暫存器來載入該第一初始參數的倍數之一部份到該第一儲存元件中；

其中該第一儲存元件、該加法器及該累積暫存器係進一步對於該第一初始參數的倍數的該部份來執行一蒙哥馬利乘法。

12. 如申請專利範圍第11項之裝置，其中：

該第一處理元件進一步包含耦合到該加法器及該累積暫存器之一第二儲存元件；及

該加法器係要計算一第二初始參數的倍數之一部份，而該累積暫存器係要載入該第二初始參數的倍數的該部

六、申請專利範圍

份到該第二儲存元件中。

13. 如申請專利範圍第12項之裝置，進一步包含：

在該線性收縮陣列蒙哥馬利乘法器中一第二處理元件；

其中該累積暫存器係進一步在由該加法器計算之前傳遞該第一初始參數通過該第一及第二處理元件。

14. 如申請專利範圍第13項之裝置，其中：

該第一處理元件進一步包含一位址暫存器來定址在該第一儲存元件內的位置，並在傳遞通過該累積暫存器之前傳遞該第一初始參數通過該第一及第二處理元件。

15. 如申請專利範圍第14項之裝置，其中：

該傳遞通過該位址暫存器係在相反於傳遞通過該累積暫存器的方向上。

16. 如申請專利範圍第14項之裝置，進一步包含：

耦合到該位址暫存器及該累積暫存器之邏輯，用以迴路該第一初始參數由該位址暫存器到該累積暫存器。

17. 一種供於蒙哥馬利乘法器處理元件中組件減少之方法，包括：

載入一初始參數到一線性收縮陣列蒙哥馬利乘法器的一組處理元件中，藉由：

傳遞該初始參數通過該處理元件；及

載入該初始參數到在該處理元件中的儲存元件。

18. 如申請專利範圍第17項之方法，其中：

傳遞該初始參數包含傳遞該初始參數通過在該處理元件中的累積暫存器。

六、申請專利範圍

19. 如申請專利範圍第18項之方法，進一步包含：

傳遞該初始參數通過在該處理元件中的位址暫存器，其方向係相反於傳遞通過該累積暫存器；及

於該傳遞該初始參數通過該累積暫存器之前，迴轉在一特定處理元件處的該初始參數。

20. 一種具有指令儲存其上之電腦可讀取記錄媒體，其當由一組一或多個處理器執行時，即造成該組處理器來執行運算，其包含：

載入一初始參數及控制碼到一線性收縮陣列蒙哥馬利乘法器來造成在該線性收縮陣列蒙哥馬利乘法器中的處理元件，以傳遞該初始參數通過該處理元件，並載入在該處理元件中儲存元件之初始參數。

21. 如申請專利範圍第20項之媒體，其中：

傳遞該初始參數包含傳遞該初始參數通過在該處理元件中的累積暫存器。

22. 如申請專利範圍第21項之媒體，其中：

傳遞該初始參數進一步包含傳遞該初始參數通過在該處理元件中的位址暫存器，其係與傳遞通過該累積暫存器之相反的方向上，並在傳遞通過該累積暫存器之前迴轉在一特定處理元件處的該初始參數。

23. 如申請專利範圍第20項之媒體，進一步包含：

載入控制碼到該線性收縮陣列蒙哥馬利乘法器中，以造成該處理元件來預先計算在該處理元件中該初始參數的倍數，並儲存該倍數在該儲存元件中。

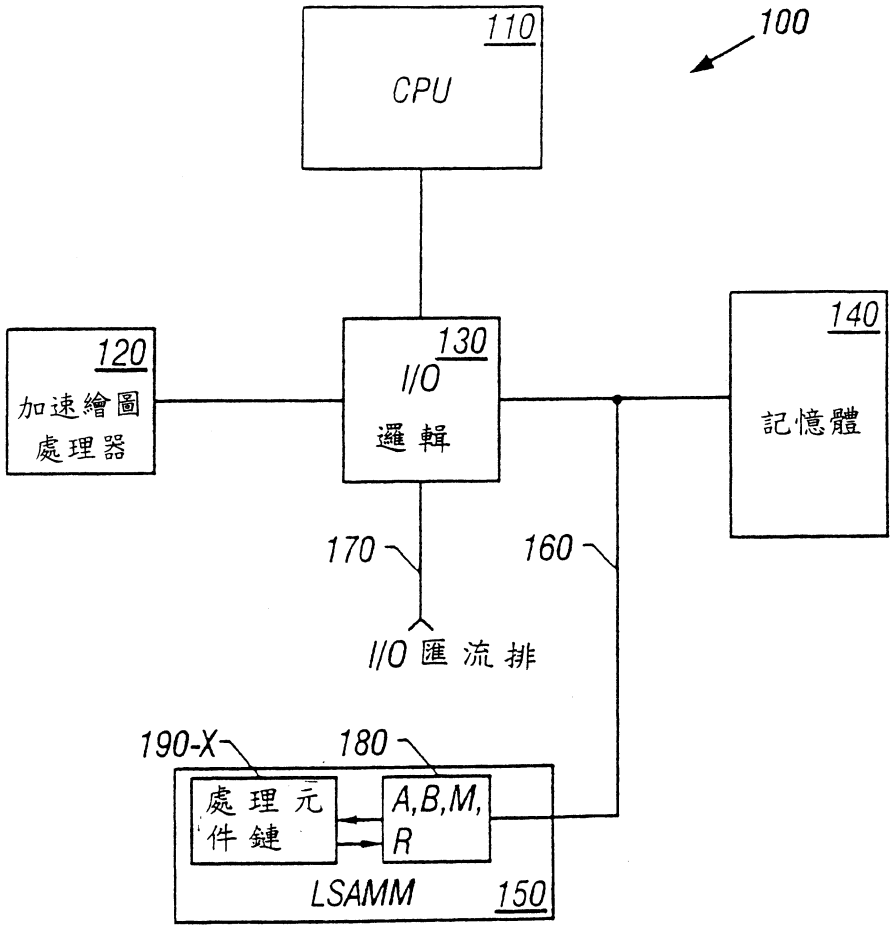
100
110
CPU
120
加速繪圖
處理器
130
I/O
邏輯
140
記憶體
170
160
I/O 匯流排
190-X
180
處理元
件鏈
A,B,M,
R
LSAMM
150

圖 1

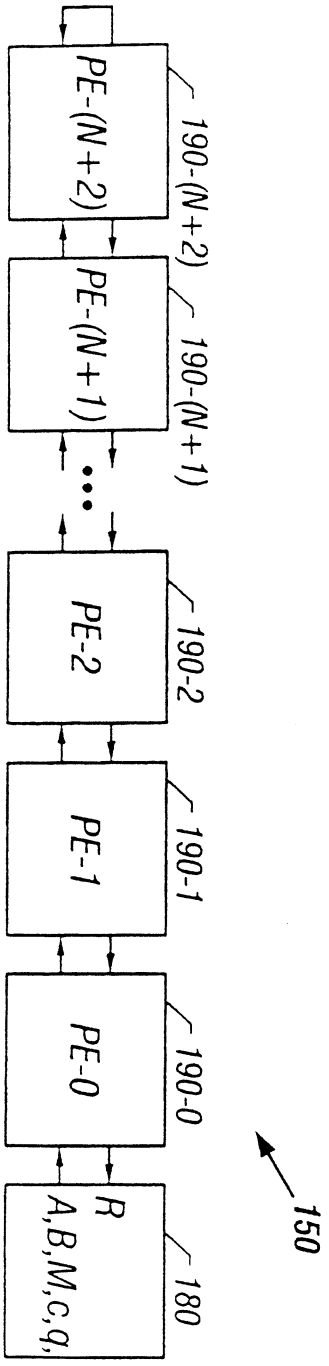

圖 2

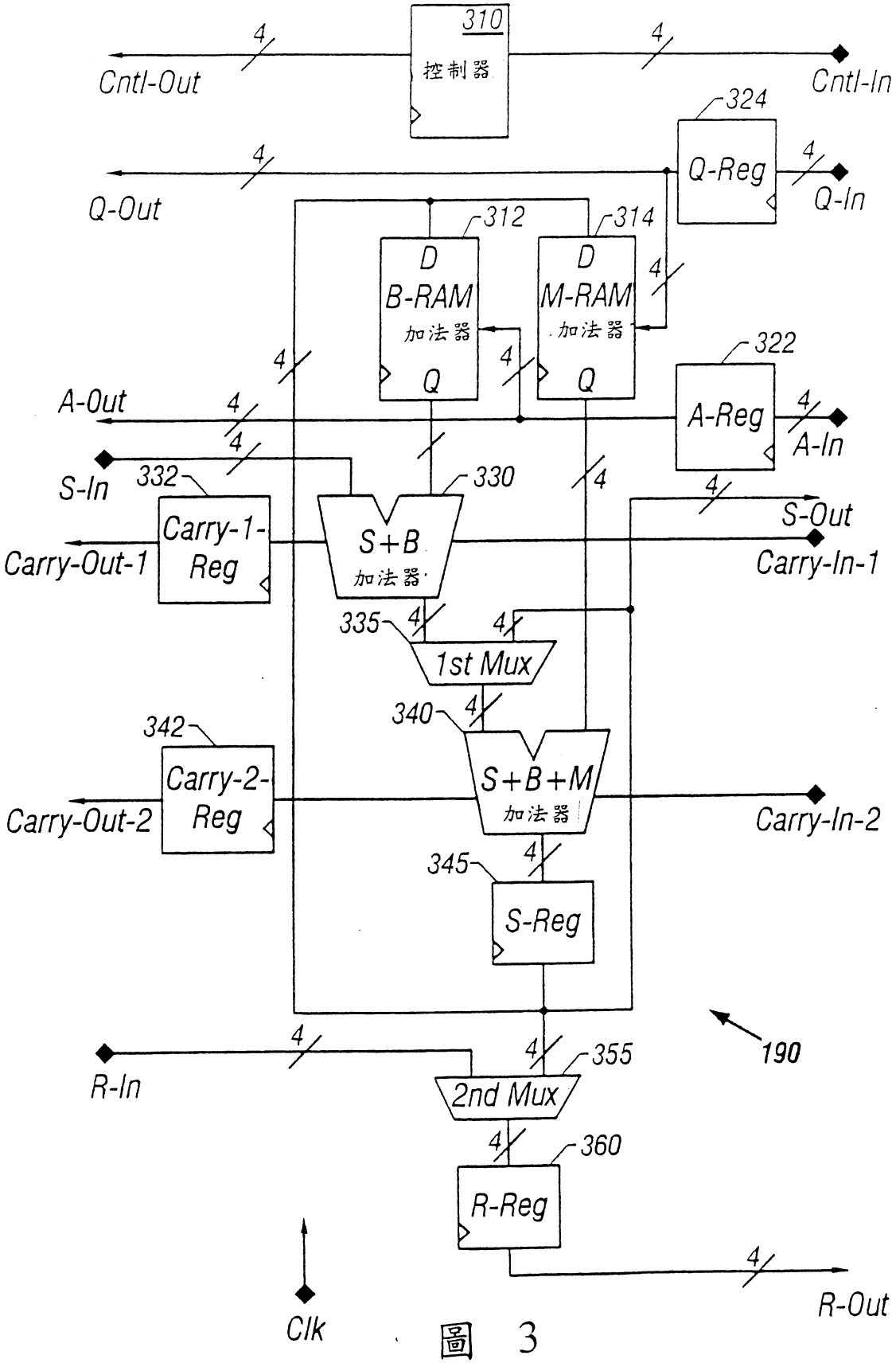
310
控制器
Cntl-Out
Cntl-In
4
324
Q-Reg
Q-Out
Q-In
312
314
D
B-RAM
加法器
Q
D
M-RAM
加法器
Q
322
A-Reg
A-Out
A-In
S-In
332
330
Carry-1-
Reg
S+B
加法器
S-Out
Carry-Out-1
Carry-In-1
335
1st Mux
340
342
Carry-2-
Reg
S+B+M
加法器
Carry-Out-2
Carry-In-2
345
S-Reg
190
R-In
355
2nd Mux
360
R-Reg
R-Out
Clk

圖 3

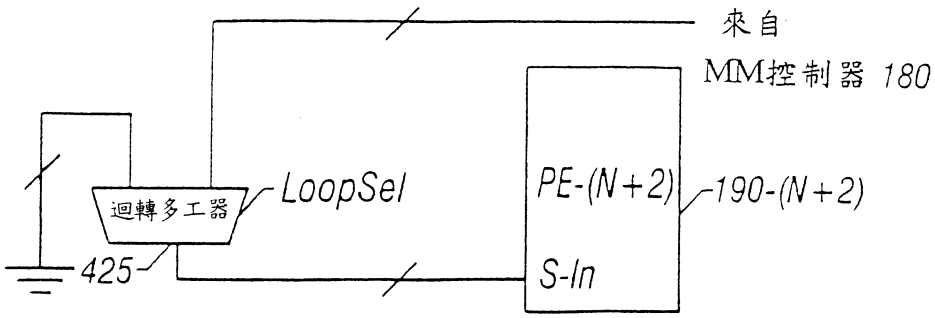
來自
MM控制器 180
迴轉多工器
LoopSel
425
PE-(N+2)
S-In
190-(N+2)

圖 4A

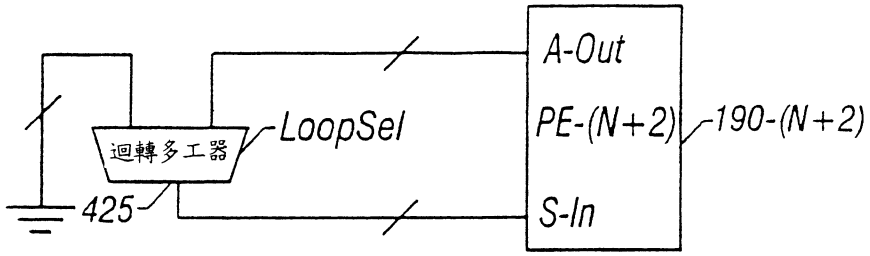
A-Out
迴轉多工器
LoopSel
PE-(N+2)
425
S-In
190-(N+2)

圖 4B

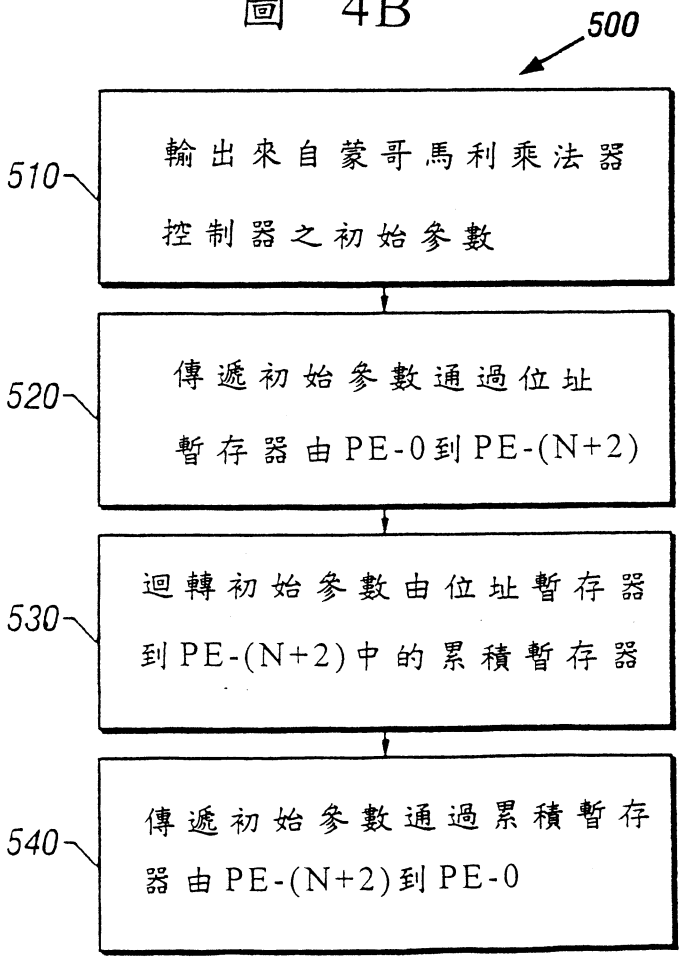
500
510
輸出來自蒙哥馬利乘法器控制器之初始參數
520
傳遞初始參數通過位址暫存器由PE-0到PE-(N+2)
530
迴轉初始參數由位址暫存器到PE-(N+2)中的累積暫存器
540
傳遞初始參數通過累積暫存器由PE-(N+2)到PE-0

圖 5