（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：　　，□有　□無主張優先權

美國　　2001年09月26日　09/963,857　☑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

本發明大體上與電腦有關。特別地，它與產生偽隨機號碼有關。

2. 相關技術描述

許多形式的保全，例如資料編密碼，利用隨機號碼來增加破解密碼的困難。如此的編密和隨機號碼產生最常以電腦執行。然而，一電腦使用一有限集合的已知指令和已知的時序關係，因此由一電腦所產生的任何事物理論上不是隨機的。但是藉由依照正確類型的複雜演算法，即使當過去歷史的號碼順序已知時，一電腦可計算顯得隨機性且難以預測的一序列號碼。一偽隨機號碼產生器(PRNG)所以稱為偽隨機，是因為它藉由對相對小集合的輸入資料(其可能是或可能不是隨機的)反覆一些複雜的演算法來產生它的輸出，而不是藉由取樣一些真實地隨機的實際程序。保全應用中一PRNG的數值，是以根據先前來自PRNG的輸出號碼及/或對PRNG的輸入號碼的全部或部分歷史，決定特定輸出號碼的數值之困難為基礎。

一些PRNG使用一疊代的單向雜湊演算法，其取得一第一號碼，經由一演算法將它轉換成一第二號碼，然後使用第二號碼為演算法的一輸入以產生一第三號碼，其變成演算法的輸入以產生一第四號碼等。如果演算法夠複雜，從先前的號碼預測一號碼是非常困難的。然而，如果一不懷好意的攻擊者知道PRNG演算法，因為在PRNG的輸入和輸出

五、發明說明（ 3 ）

節。在其他實例中，未詳細地表示眾所週知的電路、結構、和技術以便不模糊了本發明。

本發明的各種具體實施例使用一數字順序器(例如一計數器或線性回饋移位暫存器)的輸出，當成對一疊代的雜湊演算之週期的部份輸入。為了增加雜湊結果的隨機性，數字順序器的輸出可能藉由對不可預測的時間週期停止它的運算變得更隨機。一具體實施例持續地執行雜湊演算，但當產生了一偽隨機號碼的請求時停止數字順序器，而在下一雜湊階段的開始再次啟動數字順序器。

一疊代的雜湊演算是重複地從輸入號碼產生輸出號碼的任何循環雜湊運算，使每一輸出號碼的至少一部份饋回當成輸入以產生下一輸出號碼。在一具體實施例中，使用了一種變更形式之眾所週知的安全雜湊演算法(SHA)。一標準的SHA定義在美國商務部，技術局，國家標準與技術學會1995年4月17日所出版的聯邦資訊處理標準公告180-1中。

圖1表示依照本發明一具體實施例的偽隨機號碼產生器的方塊圖。在圖1所說明的具體實施例中，偽隨機號碼產生器(PRNG)10包括一雜湊電路形式的雜湊器12。雜湊器12在IN-1和IN-2接收結合的輸入資料，對結合的輸入資料執行一雜湊演算，並在OUT以一偽隨機號碼(PRN)的形式產生輸出資料。在所說明的具體實施例中，一時鐘訊號CLK用來對雜湊器12的處理元件計時，而需要多個時鐘脈衝來產生每一PRN。在輸出所產生的PRN閂鎖到暫存器16內，它可

五、發明說明（ 4 ）

從暫存器16供請求一PRN的裝置或運算取得。在一具體實施例中，每一新的PRN蓋寫掉暫存器16中的資料，如此重複地變更可使用的PRN。

雜湊器12可能從二個來源接收輸入資料。在一具體實施例中，IN-1和IN-2代表同時地接收資料的平行位元群組。在另一具體實施例中，IN-1和IN-2代表在相同輸入位元於不同時間(例如透過未顯示的一多工器)所接收的不同輸入。在一些具體實施例中，IN-1和IN-2的每一個接收大號碼為循序地接收的一系列較小號碼。

來自雜湊器12的輸出資料之至少一部分透過回饋電路15饋回到輸入IN-2，以使用為一輸入來混雜下一PRN。在一具體實施例中，回饋電路15由從OUT到IN-2的直接連接所組成。在另一具體實施例，回饋電路15對資料執行一有效運算，例如但不限於，暫時儲存輸出資料且在需要時部分提供它。

為了增加雜湊器輸出的隨機性，輸入資料的另一來源從數字順序器(NS)14提供在輸入IN-1。NS 14如此命名是因為它輸出一序列號碼。即使重複的週期可能非常長，序列最後可能重複。在圖1所說明的具體實施例中，訊號NSCLK用來計時NS 14的處理元件。在一具體實施例中，NSCLK是可獨立於CLK由控制電路18停止和啟動之CLK的一導函數，因此當NS 14的輸出由一第一預定的事件(例如收到對一偽隨機號碼的請求)停止、和由一第二預定的事件(例如下一雜湊階段的開始)重新開始時，雜湊器12繼續執行。在

五、發明說明（ 5 ）

各種具體實施例中，獨立於雜湊器12停止和開始NS 14的能力，消除如果它們從一共通的時鐘來源操作時將存在NS 14和雜湊器12之間的同步。

在一具體實施例中，NS 14是一計數器，例如一64位元計數器，而NSCLK用來增量(或縮減)計數器。在另一具體實施例中，NS 14是一線性回饋移位暫存器(LFSR)，而NSCLK用來透過LFSR的元件推進那些位元。

圖2表示依照本發明一具體實施例的線性回饋移位暫存器的概要。在所說明的線性回饋移位暫存器(LFSR) 20的具體實施例中，正反器21-0到21-7在輸出位元b0-b7上產生一八位元的號碼。號碼的數值可在目前數值透過正反器移位時，隨時鐘訊號CLK的每一脈衝改變，並由互斥或(XOR)閘22-24修改。每一XOR閘藉由以後續正反器其中之一的輸出對先前正反器的輸出執行一XOR運算，修改對一特定正反器的輸入。在所說明的具體實施例中，對正反器21-6的輸入由閘22透過以b7和b0的數值執行一XOR運算修改，對正反器21-5的輸入由閘23透過以b6和b5的數值執行一XOR運算修改，對正反器21-3的輸入由閘24透過以b4和b1的數值執行一XOR運算修改，而b3的數值饋回到正反器21-7的輸入沒有修改。其他具體實施例可能使用其他回饋安排。在一具體實施例中，多重正反器的輸出可能饋回到提供輸入到正反器21-7的一單一XOR閘。

由於上述回饋安排和XOR閘的效應，通常透過一移位暫存器可預期的位元之流動可轉換成一偽隨機號碼產生器。

五、發明說明（ 6 ）

然而，有限數目的位元和回饋安排的固定本質最後(以一相似於一計數器輸出一循環序列的輸出數值之方式)造成輸出數值的一循環序列。在這個應用中計數器和LFSR之間的一主要不同是，當較高位元相同時一計數器經過長的週期，因此減低在輸出所經歷的一些不可預測性。

在一具體實施例中，LFSR 20包括和產生所要數目的位元之PRN需要的一樣多之正反器，例如64個正反器以產生一64位元號碼。在另一具體實施例中，可能平行使用多重LFSRs，使它們的輸出結合以形成有所需位元數目的一號碼，例如使用八個8位元LFSRs來產生一64位元號碼。在又一具體實施例中，可能結合來自LFSR 20的一些連續輸出數值以形成有所需數目位元的一號碼，例如取來自一8位元LFSR的八個連續輸出數值並結合它們成為一64位元號碼。

圖3A，3B表示依照本發明一具體實施例在階段和週期之間的相對時序。圖3A展示所說明具體實施例一疊代的雜湊演算和一數字順序器的階段和週期。一階段包括在PRNG輸出產生一PRN所必需的那些運算，而一週期包括產生一數字順序器輸出數值所必需的那些運算。在一具體實施例中，一週期是一時鐘週期。在圖3A所說明具體實施例中，雜湊演算法需要80個時鐘週期來計算一雜湊數值，加上5個時鐘週期的耗用時間，每一階段總數是85個時鐘週期。所說明運算的用辭可通稱解釋為s：c，以s指示階段數目1-n，而c指示在每一階段當中的週期數目1-85。在每一階段之後，雜湊器輸出的至少一部分可能置入到一暫存器或其

五、發明說明（ 7 ）

他儲存裝置，以當成一PRN供需要一PRN的任何裝置或運算使用。在一具體實施例中，在每一階段的結束目前PRN由一新PRN代替，以便對一裝置或運算可使用的PRN反覆地改變。

在一些具體實施例中，在每一階段的開始來自先前階段的輸出之至少一部份輸入當成起始資料，如從週期1：85到週期2：1、從週期2：85到週期3：1等那些循迴箭號所示。這個輸入也顯示在圖1中的輸入IN-2。同時，NS 14可能正產生一序列的新號碼。在一具體實施例中，每一週期在數字順序器的輸出產生一新的號碼。在圖3A所說明的具體實施例中，這些週期顯示為C_0，C_1，C_2等。在每一混雜階段開始時，使用NS輸出的目前數值之至少一部份當成那個階段的起始數值之一部份，如圖3A中從右-到-左的箭號所示。這個輸入也顯示在圖1中的IN-1。在一具體實施例中，NS的輸出與雜湊器的輸出不相關聯(也就是，NS輸出的數值不依雜湊器輸出的數值而定)，相反地是雜湊器輸出的數值依NS輸出的數值而定。這個單向相關性增加根據雜湊器輸出的歷史得出NS輸出的困難。

當雜湊演算設定初值時，可能沒有先前的結果可當成輸入資料使用，因此來自任何來源的種子資料可用來設定階段1的初值。

圖3B表示圖3A具體實施例的一後續，在雜湊器已經到達它的第9階段、且NS已經產生超過760個輸出數值之後。在圖3B所說明的具體實施例中，在第10階段的第32週期接收

五、發明說明（ 8 ）

對一PRN的請求。這個請求可能來自需要提供一偽隨機號碼供它運算的任何來源。當接收到請求時，可能凍結NS的運算，以便它停止，在每一時鐘週期產生新的輸出數值。在一具體實施例中，NS的運算從下一雜湊階段最初的地方重新開始。參照圖1，停止和開始NS 14可能以控制電路18藉由停止和開始時鐘訊號NSCLK控制。因為對一PRN的請求之精確時序通常是不可預測的(至少相對於PRNG來說)，NS在哪一週期凍結也可能是不可預測的，而因此它保持凍結的週期數目可能同樣地是不可預測的。如此在混雜運算和NS輸出之間先前同步的運算可能由對一PRN的請求所中斷，而它們失去同步相差一不可預測數目的週期。失去同步甚至只相差一個週期，可能從雜湊器產生一完全不同集合的未來輸出。

從圖3B所說明的具體實施例繼續，當下一雜湊階段(階段11)開始，NS 14中的凍結數值提供到雜湊器12當成雜湊器的輸入資料之一部份。在那時，NS 14的運算可能恢復，而NS 14可能對每一時鐘週期再一次開始產生一新的輸出數值。在圖3B所說明的具體實施例中，當收到對一PRN的請求時NS 14在週期C_{796}凍結。當階段10完成時，週期C_{796}的凍結數值提供到雜湊器12當成輸入開始階段11，且NS 14在週期C_{797}開始產生新的號碼。

在圖3B所說明的範例中，如果未凍結NS 14，階段11將以週期C_{850}的數值開始。在C_{796}和C_{850}的數值之間的差異代表NS 14的54次疊代，且可能代表開始階段11的重大不同數

五、發明說明（ 9 ）

值。此外，造成不同的疊代之數目是隨機的，且可能只由每一階段時鐘週期的數目所限制。

在一電路具體實施例中，NS 14藉由停止它的時鐘(舉例來說，圖1中的NSCLK)凍結，而藉由重新開始它的時鐘重新開始。在雜湊器的一軟體具體實施例中，NS 14藉由停止一計數器或其他增量(或減縮)實體(不是硬體就是軟體)凍結，而藉由重新開始那個實體重新開始。

在一具體實施例中，在系統設定初值之後所請求的第一PRN未從凍結NS獲利，因為PRN是在凍結的第一次發生之前產生，但所有後續PRN請求確實從凍結NS獲利。對第一次請求的PRN的這個缺點，可藉由最初產生對一PRN的一或更多假請求避免，這將會暫時凍結NS並在後續的PRN數值中產生足夠的隨機性。

圖4表示依照本發明一具體實施例之圖1的特定具體實施例的方塊圖。在圖4的PRNG 40中，雜湊器42、NS 44、回饋電路45、暫存器46和控制電路48分別對應於圖1的雜湊器12、NS 14、回饋電路15、暫存器16和控制電路18，PRNG 40中在各種輸入、輸出和連接有特定數目的位元。在圖4的具體實施例中，只完全使用在各種地方產生的位元之一部分，使辨別邏輯的內部狀態更困難。如果只使用在一特定點的位元輸出之一部分，而其餘位元不揭露，判斷電路的任何部份之內部狀態是更困難的，因為只有部分資訊可用來幫助這樣的判斷。

在圖4的具體實施例中，雜湊器42接收並以512位元號碼

五、發明說明（ 10 ）

內部運作，但只輸出那些位元中的160個，其全部饋回到IN-2產生下一雜湊階段的輸入之一部分。160個位元中只有64個置入到暫存器46使用作為一PRN，且這64個位元是揭露在PRNG 40外部的僅有位元。在相同具體實施例中，NS 44內部產生70個位元，平行使用各種長度的7個LFSR，但只輸出那些位元中的32個。在一具體實施例中，NS 44輸出11個連續的32位元數值，以填滿雜湊器42在IN-1所接收的352個位元。當雜湊器42的160個位元減少到64個位元，且當NS 44的70個位元減少到32個位元時，各種技術可用來決定要使用可取得位元的哪一個。在一具體實施例中，使用了一群連續位元，而哪一些連續的位元之選取是一設計選擇。在另一具體實施例中，所選擇的位元是不連續的，且它們的順序可能在輸出以前重新排列。

圖5表示依照本發明一具體實施例的方法之流程圖。在圖5所說明的具體實施例之流程圖50中，在方塊51使用一PRN的目前數值、和數字順序器的目前輸出當做輸入資料開始一新的雜湊階段。在一具體實施例中，輸入資料包括雜湊器的完整160個位元先前輸出，包括組成那個輸出的一部份之PRN的64個位元。如果系統剛剛起始，這些號碼可能仍不存在而可能使用種子資料替代。判斷方塊52判斷是否已經收到對一PRN的請求。在一具體實施例中，一旦收到這樣的請求，對這個判斷方塊的答案持續是'是的'直到目前的雜湊階段完成。如果已經收到對一PRN的請求，方塊53停止數字順序器，以便它的輸出數值保持凍結，直到數

五、發明說明（ 11 ）

字順序器重新開始。如果還沒收到對一PRN的請求，數字順序器在方塊54繼續執行並產生一新的輸出數值。每一回經過方塊54可能產生數字順序器的一新的輸出數值，它變成目前數字順序器數值直到它改變為止。不論是否收到對一PRN的請求，雜湊階段的運作在方塊55繼續。在一具體實施例中，雜湊運作的時鐘和數字順序器的時鐘是相同的頻率。判斷方塊56判斷目前的雜湊階段是否已經完成。如果目前的雜湊階段還沒完成，控制返回到方塊52。如果雜湊階段已經完成，最新產生的PRN載入到一暫存器，在那裡它可供後續PRN請求取得。方塊58載入新的雜湊器輸出，包括新的PRN、和數字順序器的目前輸出數值到雜湊器的輸入。在雜湊器的輸入它們變成在方塊51開始的下一雜湊階段的起始數值。另外，數字順序器重新開始(或繼續執行)，以便它將會在下一雜湊階段的開始執行著。

圖6表示依照本發明一具體實施例的系統。在圖6所說明的具體實施例中，一系統60包括一處理器61，經由一輸入-輸出(I/O)匯流排65和一I/O控制器63連接到一PRNG 10。I/O控制器可能也連接到一主記憶體62和一加速圖形處理器(AGP) 64。也可能連接其他裝置(未顯示)到系統。中央處理器61可能執行軟體以操作PRNG 10。能夠在I/O匯流排65上存取PRNG 10的任何裝置可能請求一PRN和從PRNG 10讀取目前的PRN。

在各種具體實施例中，對一PRN的呼叫之精確時序中的變異性引入額外的隨機性、或渾沌性(超過沒有這個變異性

五、發明說明（ 12 ）

的一相似PRNG之運作)到PRNG 10的運作內。舉例來說，如果這樣的一呼叫的時序改變剛好超過一秒鐘，而一時鐘週期是15十億分之一秒(ns)長，對一PRN的請求可能在NS 14的六千七百萬週期之中的任何一個到達。因為六千七百萬是大約2^{26}，這代表26個位元的一渾沌性或隨機性。當進行二個呼叫時，二個NS時鐘凍結代表來自NS 14(六千七百萬)^{2}個可能數值，或52個位元的渾沌性。對一PRN的每一額外呼叫產生一額外26個位元的渾沌性。在一些點，來自NS的渾沌性之總數將超過可能的混雜順序的數目。這讓使用的特定雜湊演算法接近可得的隨機性之最大量，而進一步的呼叫可能不增加PRNG輸出中隨機性的量。在此時，以苦力方式判斷PRN可能是一不懷好意的攻擊者判斷它的數值之最有效方法。在一資料編密環境中，這可能代表嘗試一解密鍵中號碼的每一種可能組合看看結果是否是可理解的。

修改的保全雜湊演算法

在各種具體實施例中，一修改的保全雜湊演算法(SHA)使用在雜湊器中。在一使用圖4中描述的位元數量之具體實施例中，修改的SHA以下列方式操作：

一512位元輸入(來自雜湊器42的先前輸出之160個位元和來自NS 44之352個位元)由雜湊器42使用當成輸入資料。修改的SHA演算法中的主要迴路有四組二十個運作形式的總共80個順序操作(t=0到79)。非線性SHA運作如下：

$f_t(B, C, D) = (B \wedge C) \vee (\sim B \wedge D)$ (對 t=0 到 19)

五、發明說明（ 13 ）

$f_t(B, C, D) = B \text{ xor } C \text{ xor } D$ (對 t=20-39)

$f_t(B, C, D) = (B \wedge C) \text{ v } (B \wedge D) \text{v} (C \wedge D)$ (對 t=40-59)

$f_t(B, C, D) = B \text{ xor } C \text{ xor } D$ (對 t=60-79)

其中t=運作的數目，^=邏輯及，v=邏輯或，~=邏輯補數和xor=互斥或。

演算法中使用了四個常數K和五個變數A、B、C、D和E，他們的數值以十六進位表示法顯示：

K_t =5A827999 (對 t=0-19)

K_t =6ED9EBA1 (對 t=20-39)

K_t =8F1BBCDC (對 t=40-59)

K_t =CA62C1D6 (對 t=60-79)

變數的起始數值為：

A_0 = 67452301

B_0 = EFCDAB89

C_0 = 98BADCFE

D_0 = 10325476

E_0 = C3D2E1F0

輸入資料從十六個32位元字組(M_0-M_{15})使用下列演算法轉換成八十個32位元字組(W_0-W_{79})：

$W_t = M_t$ (對 t = 0-15)

$W_t = (W_{t-3} \text{ xor } W_{t-8} \text{ xor } W_{t-14} \text{ xor } W_{t-16}) <<< 1$ (對t = 16-79)，其中<<<1=向左移位一個位元。

演算法的主要迴路看起來像這樣：

對t=0到79，

五、發明說明（ 14 ）

$$TEMP = (A <<< 5) + F_t(B,C,D) + E_t + W_t + K_t$$

$$E = D$$

$$D = C$$

$$C = B <<< 30$$

$$B = A$$

$$A = TEMP$$

在80個迴圈之後，修改的SHA演算法之輸出是由ABCDE所代表的160-位元字串。在一具體實施例中，這個字串的64位元部分存在暫存器46中當成目前的PRN，而整個160位元饋回到雜湊器42的輸入，作為下一雜湊階段的起始輸入資料的一部份。如先前描述，那些位元可能在存檔及/或饋回之前重新排列。

上述說明使用一修改的SHA演算法描述本發明一具體實施例，但可能使用其他演算法而不脫離本發明的精神。

本發明可能實施在一電路中或實施為一種方法。本發明也可能實施為儲存在一電腦可讀的媒體上之指令，其可由至少一處理器讀取和執行，以執行此處描述的運作。一電腦可讀的媒體可包括用來以可由一機器(舉例來說，一電腦)讀取的形式儲存或傳送資訊的任何機制。舉例來說，一電腦可讀的媒體可包括唯讀記憶體(ROM)；隨機存取記憶體(RAM)；磁性磁碟儲存媒體；光學儲存媒體；閃光記憶體裝置；電子、光學、聽覺的或其他形式的傳播訊號(舉例來說，載波、紅外線訊號、數位訊號等)和其他的。

前面的描述目的是說明而非限制。熟知該項技藝人士將

A5
B5

四、中文發明摘要（發明之名稱：基於雜湊之偽隨機號碼產生器）

一種有增加的隨機性之偽隨機號碼產生器(PRNG)。在每一雜湊階段中，一疊代的以雜湊為基礎的PRNG混雜在一數字順序器(例如一計數器或線性回饋移位暫存器)的輸出中。為了增進數字順序器輸出的不可預測性，它可能在相對不可預測的時間週期暫停。當數字順序器的輸出之時序是不可預測時，經過的時間不能用來確實地預測對於一雜湊演算之數字順序器的輸出相。不可預測的時間週期可能與何時接收一偽隨機號碼的請求有關。

英文發明摘要（發明之名稱：HASH-BASED PSEUDO-RANDOM NUMBER GENERATOR）

A pseudo-random number generator (PRNG) with increased randomness. An iterative hash-based PRNG hashes in the output of a numerical sequencer, such as a counter or linear feedback shift register, in each hash stage. To improve the unpredictability of the numerical sequencer output, it may be paused for relatively unpredictable time periods. When the timing of the output of the numerical sequencer is unpredictable, elapsed time cannot be used to reliably predict what the output of the numerical sequencer will be with relation to the hash operation. The unpredictable time period may be related to when a request for a pseudo-random number is received.

公告本

I237214

申請日期	91-9-19
案　　號	091121485
類　　別	G09C1/00, G06F7/58

（以上各欄由本局填註）

92年1月15日 修正補充

A4
C4

中文說明書替換頁(92年1月)

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中　文	基於雜湊之偽隨機號碼產生器
	英　文	HASH-BASED PSEUDO-RANDOM NUMBER GENERATOR
二、發明 ~~創作~~ 人	姓　名	邁可　D.　洛爾 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, CALIFORNIA92128, 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

五、發明說明（ 2 ）

之間不變的關係，他可能可以預測所有的未來輸出。

減少這危險的一傳統方法是在每一階段也在數值中混雜一自行變動的計數器。這增加預測一特定號碼、和藉以破解密碼的困難，但一計數器的輸出可預測地是線性的。有了足夠的資源，一專注的攻擊者可結合計數器的可預測性以已經-知道特性的演算法，判斷一特定的偽隨機號碼將會是什麼，而因此給不懷好意的一方機會解密一編密過的訊息。

圖式簡單說明

本發明透過參照下列說明和用來例示本發明具體實施例之伴隨的圖式可最好地瞭解。在那些圖式中：

圖1表示依照本發明一具體實施例的偽隨機號碼產生器的方塊圖。

圖2表示依照本發明一具體實施例一線性回饋移位暫存器的概要。

圖3A、3B表示依照本發明一具體實施例在階段和週期之間相對的時序。

圖4展示依照本發明一具體實施例，圖1的特定具體實施例之方塊圖。

圖5展示依照本發明一具體實施例的方法之流程圖。

圖6展示依照本發明一具體實施例的系統。

發明詳述

在下列說明中，陳述許多特定細節以提供本發明的徹底瞭解。然而，一般瞭解可以實行本發明而沒有這些特定細

五、發明說明（ 15 ）

會想到變化。打算包含那些變更在本發明中，本發明只由所附申請專利範圍之精神和範疇限制。

元件符號說明

10	偽隨機號碼產生器(PRNG)
12	雜湊器
14	數字順序器
15	回饋電路
16	暫存器
18	控制電路
20	線性回饋移位暫存器(LFSR)
21-0...21-7	正反器
22, 23, 24	互斥或(XOR)閘
40	偽隨機號碼產生器
42	雜湊器
44	數字順序器
45	回饋電路
46	暫存器
48	控制電路
60	系統
61	處理器
62	主記憶體
63	輸入/輸出控制器
64	加速圖形處理器(AGP)
65	輸入/輸出(I/O)匯流排

四、中文發明摘要（發明之名稱：基於雜湊之偽隨機號碼產生器）

一種有增加的隨機性之偽隨機號碼產生器(PRNG)。在每一雜湊階段中，一疊代的以雜湊為基礎的PRNG混雜在一數字順序器(例如一計數器或線性回饋移位暫存器)的輸出中。為了增進數字順序器輸出的不可預測性，它可能在相對不可預測的時間週期暫停。當數字順序器的輸出之時序是不可預測時，經過的時間不能用來確實地預測對於一雜湊演算之數字順序器的輸出。不可預測的時間週期可能與何時接收一偽隨機號碼的請求有關。

英文發明摘要（發明之名稱：HASH-BASED PSEUDO-RANDOM NUMBER GENERATOR）

A pseudo-random number generator (PRNG) with increased randomness. An iterative hash-based PRNG hashes in the output of a numerical sequencer, such as a counter or linear feedback shift register, in each hash stage. To improve the unpredictability of the numerical sequencer output, it may be paused for relatively unpredictable time periods. When the timing of the output of the numerical sequencer is unpredictable, elapsed time cannot be used to reliably predict what the output of the numerical sequencer will be with relation to the hash operation. The unpredictable time period may be related to when a request for a pseudo-random number is received.

六、申請專利範圍

1. 一種產生偽隨機號碼之裝置，包含：

一雜湊電路，以接收一目前雜湊階段的第一和第二輸入數值，和根據第一和第二輸入數值從目前雜湊階段產生一輸出數值；

連接到雜湊電路的一數字順序器，以在目前雜湊階段期間產生一序列號碼，和提供序列號碼的目前一個之至少一部分當成一後續雜湊階段的第一輸入數值；

連接到雜湊電路的一回饋電路，以提供輸出數值的至少一部分，其當成後續雜湊階段的第二輸入數值；及

連接到數字順序器的一控制電路，以在一第一預定事件的發生時停止序列號碼的產生，和在一第二預定事件的發生時恢復序列號碼的產生。

2. 如申請專利範圍第1項之裝置，其中：

雜湊電路是要在目前雜湊階段的開始接收第一和第二輸入數值。

3. 如申請專利範圍第1項之裝置，其中：

第一預定的事件包括接收對一偽隨機號碼的請求。

4. 如申請專利範圍第1項之裝置，其中：

第二預定的事件包括後續雜湊階段的一部份。

5. 如申請專利範圍第1項之裝置，其中：

第二預定的事件包括後續雜湊階段的開始。

6. 如申請專利範圍第1項之裝置，其中：

數字順序器包括一計數器。

7. 如申請專利範圍第1項之裝置，其中：

A8
B8
C8
D8

六、申請專利範圍

數字順序器包括一線性回饋移位暫存器。

8. 如申請專利範圍第1項之裝置，其中：

序列號碼的目前一個之該至少一部分，包括序列號碼的目前一個之預定的位元。

9. 如申請專利範圍第1項之裝置，其中：

輸出數值的該至少一部分，包括輸出數值之預定的位元。

10. 一種產生偽隨機號碼之系統，包含：

一處理器；

連接到處理器的一記憶體；及

連接到處理器的一偽隨機號碼產生器，且包括：

一雜湊電路，以接收一目前雜湊階段的第一和第二輸入數值，和根據第一和第二輸入數值從目前雜湊階段產生一輸出數值；

連接到雜湊電路的一數字順序器，以在目前雜湊階段期間產生一序列號碼，和提供序列號碼的目前一個之至少一部分當成一後續雜湊階段的第一輸入數值；

連接到雜湊電路的一回饋電路，以提供輸出數值的至少一部分，其當成後續雜湊階段的第二輸入數值；及

連接到數字順序器的一控制電路，以在一第一預定事件的發生時停止序列號碼的產生，和在一第二預定事件的發生時恢復序列號碼的產生。

11. 如申請專利範圍第10項之系統，其中：

雜湊電路是要在目前雜湊階段的開始接收第一和第

六、申請專利範圍

二輸入數值。

12. 如申請專利範圍第10項之系統，其中：

第一預定的事件包括接收對一偽隨機號碼的請求。

13. 如申請專利範圍第10項之系統，其中：

第二預定的事件包括後續雜湊階段的一部份。

14. 如申請專利範圍第10項之系統，其中：

第二預定的事件包括後續雜湊階段的開始。

15. 如申請專利範圍第10項之系統，其中：

數字順序器包括一計數器。

16. 如申請專利範圍第10項之系統，其中：

數字順序器包括一線性回饋移位暫存器。

17. 如申請專利範圍第10項之系統，其中：

序列號碼的目前一個之該至少一部分，包括序列號碼的目前一個之預定的位元。

18. 如申請專利範圍第10項之系統，其中：

輸出數值的該至少一部分，包括輸出數值之預定的位元。

19. 一種產生偽隨機號碼之方法，包含：

在一先前雜湊階段、一目前雜湊階段、和一後續雜湊階段的每一階段期間產生一連串數值；

接收那些數值中之一當成一第一雜湊輸入；

從先前雜湊階段接收一雜湊輸出當成一第二雜湊輸入；

在一目前雜湊階段期間混雜第一和第二雜湊輸入以

六、申請專利範圍

產生一目前雜湊輸出；

如果第一預定的事件在目前雜湊階段期間發生，當一第一預定的事件發生時停止產生，而當一第二預定的事件發生時重新開始產生；及

如果第一預定的事件未在目前雜湊階段期間發生，在目前雜湊階段期間持續產生。

20. 如申請專利範圍第19項之方法，其中：

第一預定的事件包括接收對一偽隨機號碼的請求。

21. 如申請專利範圍第19項之方法，其中：

第二預定的事件包括後續雜湊階段的開始。

22. 一種電腦可讀取的媒體，其上儲存有指令，當指令由至少一處理器執行時，引起該至少一處理器執行運作，包含：

在一先前雜湊階段、一目前雜湊階段、和一後續雜湊階段的每一階段期間產生一連串數值；

接收那些數值中之一當成一第一雜湊輸入；

從先前雜湊階段接收一雜湊輸出當成一第二雜湊輸入；

在一目前雜湊階段期間混雜第一和第二雜湊輸入以產生一目前雜湊輸出；

如果一第一預定的事件在目前雜湊階段期間發生，當第一預定的事件發生時停止產生，而當一第二預定的事件發生時重新開始產生；及

如果第一預定的事件未在目前雜湊階段期間發生，持

A8
B8
C8
D8

六、申請專利範圍

續產生。

23. 如申請專利範圍第22項之媒體，其中：

第一預定的事件包括對一偽隨機號碼的請求。

24. 如申請專利範圍第22項之媒體，其中：

第二預定的事件包括一後續雜湊階段的開始。

第 091121485 號專利申請案
中文圖式替換本(93 年 3 月)

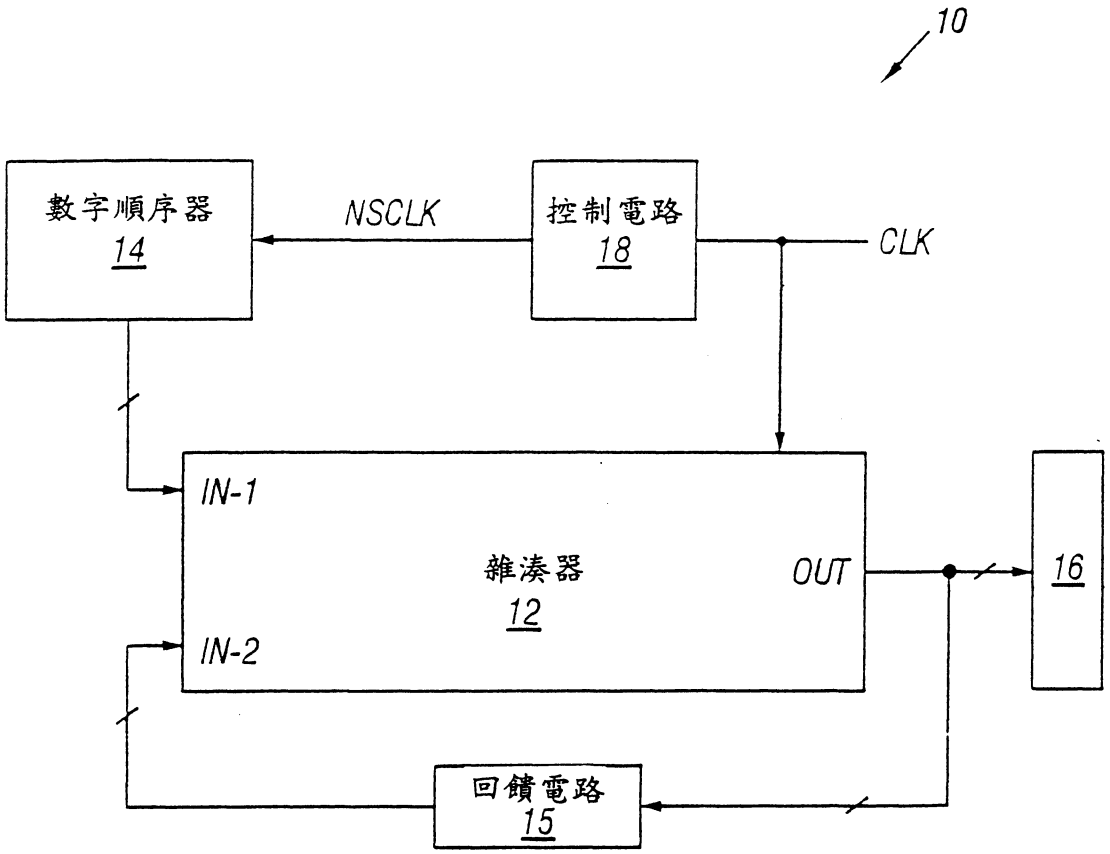

圖 1

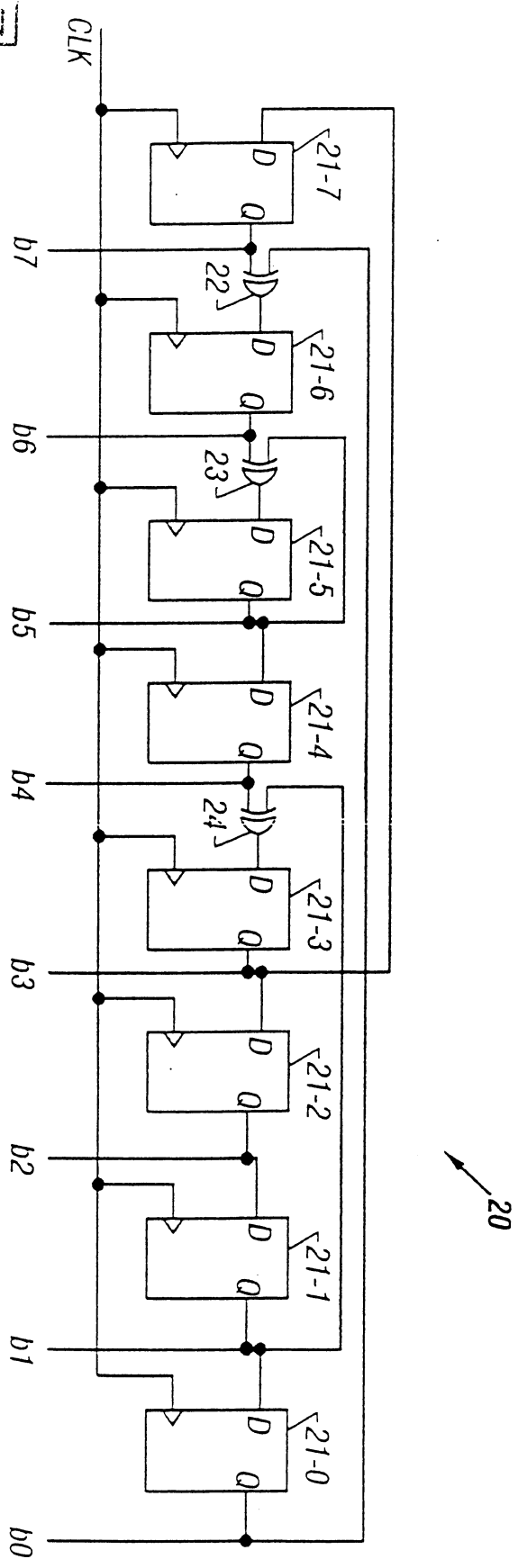

圖 2

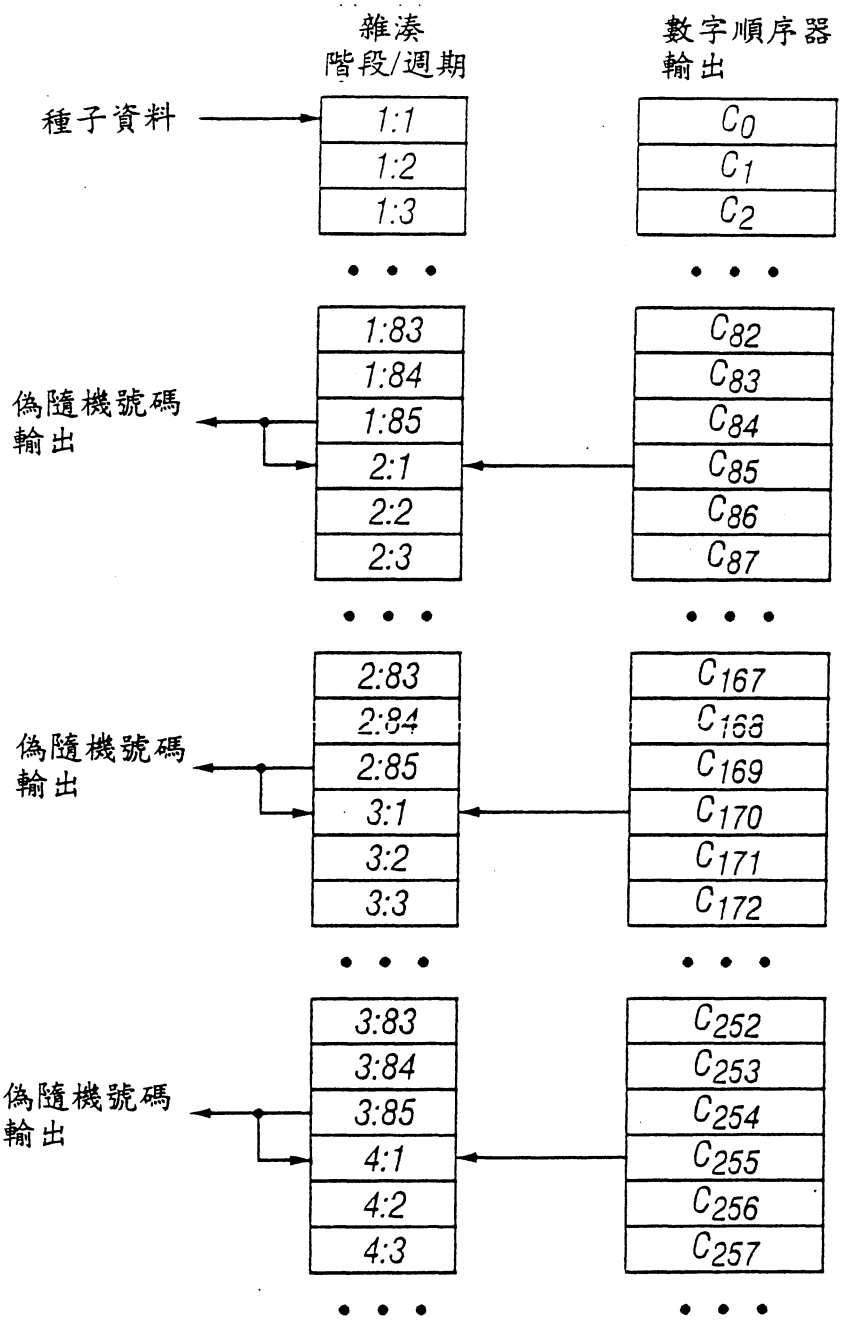

圖 3A

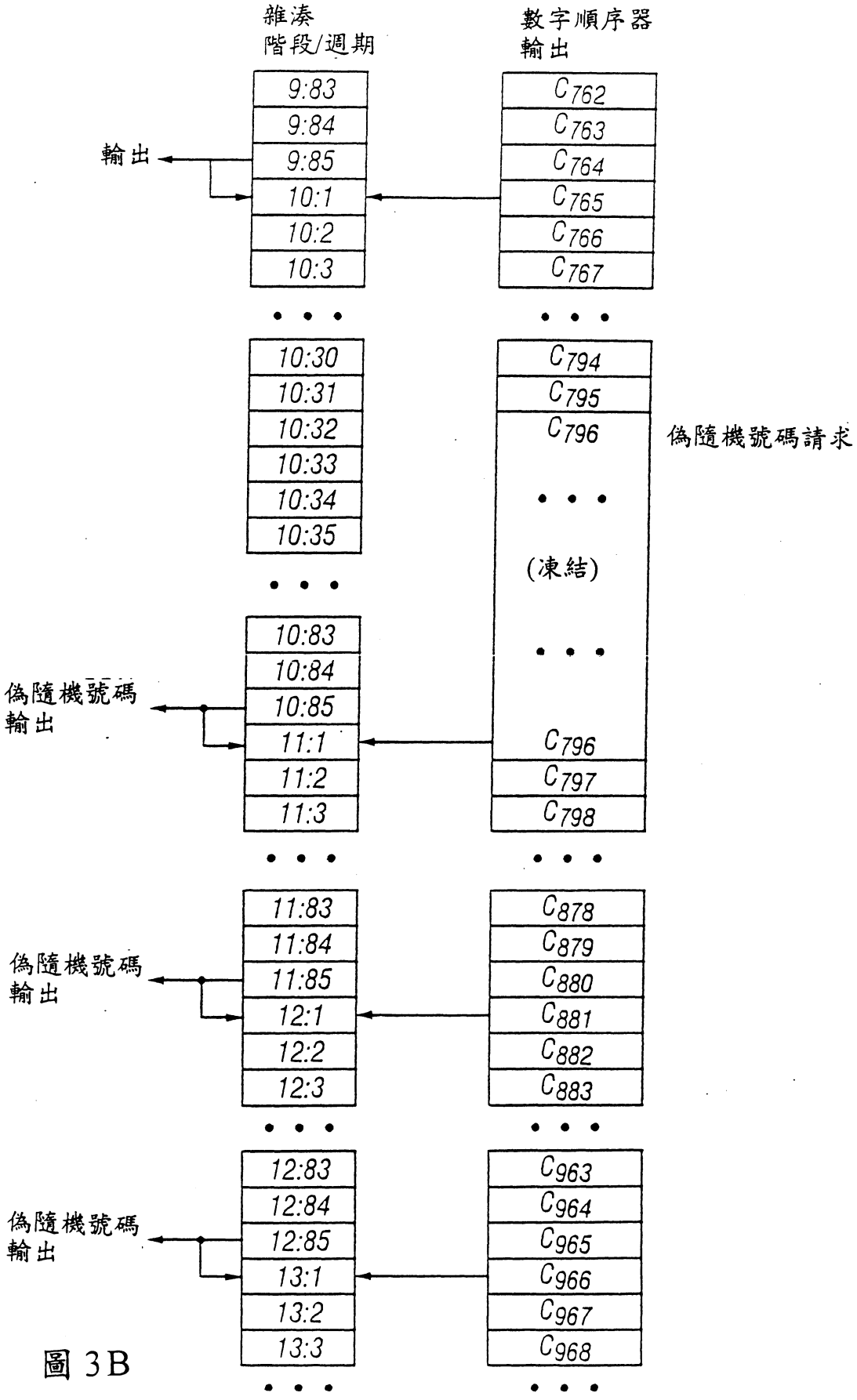

圖 3B

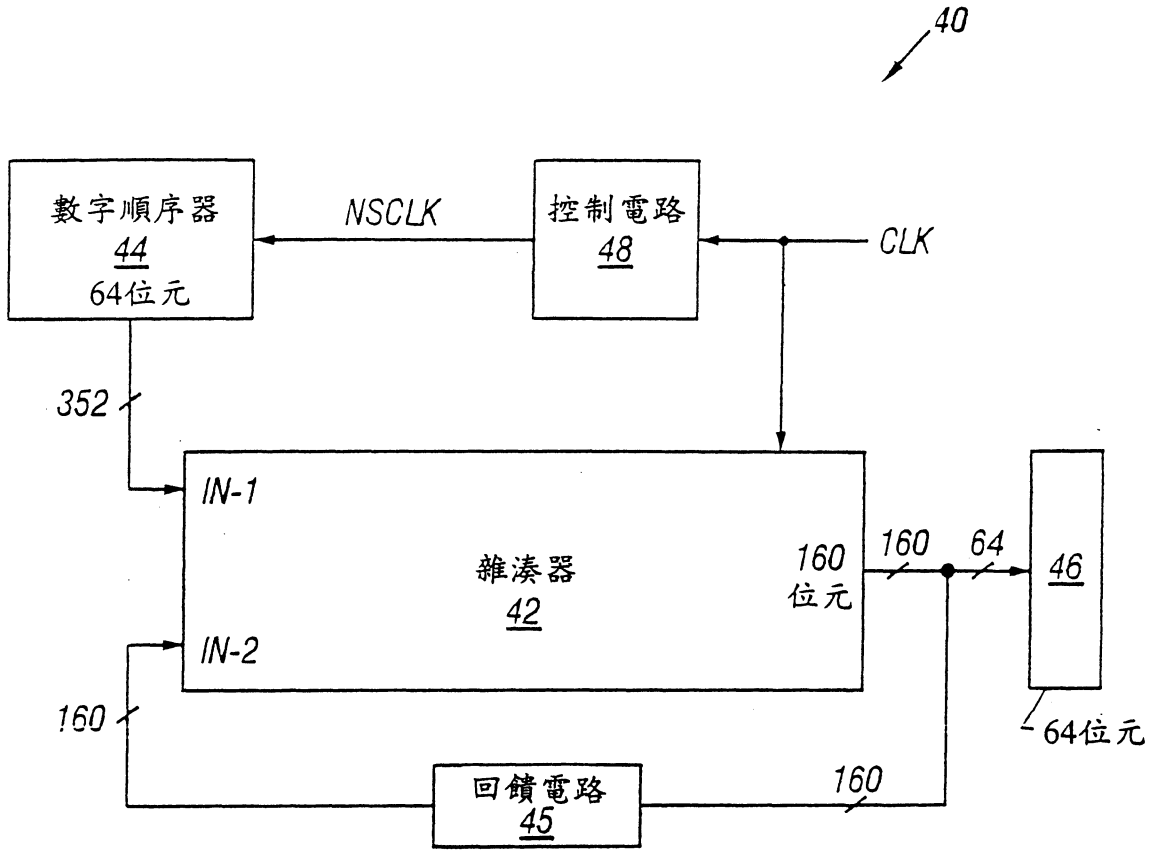

圖 4

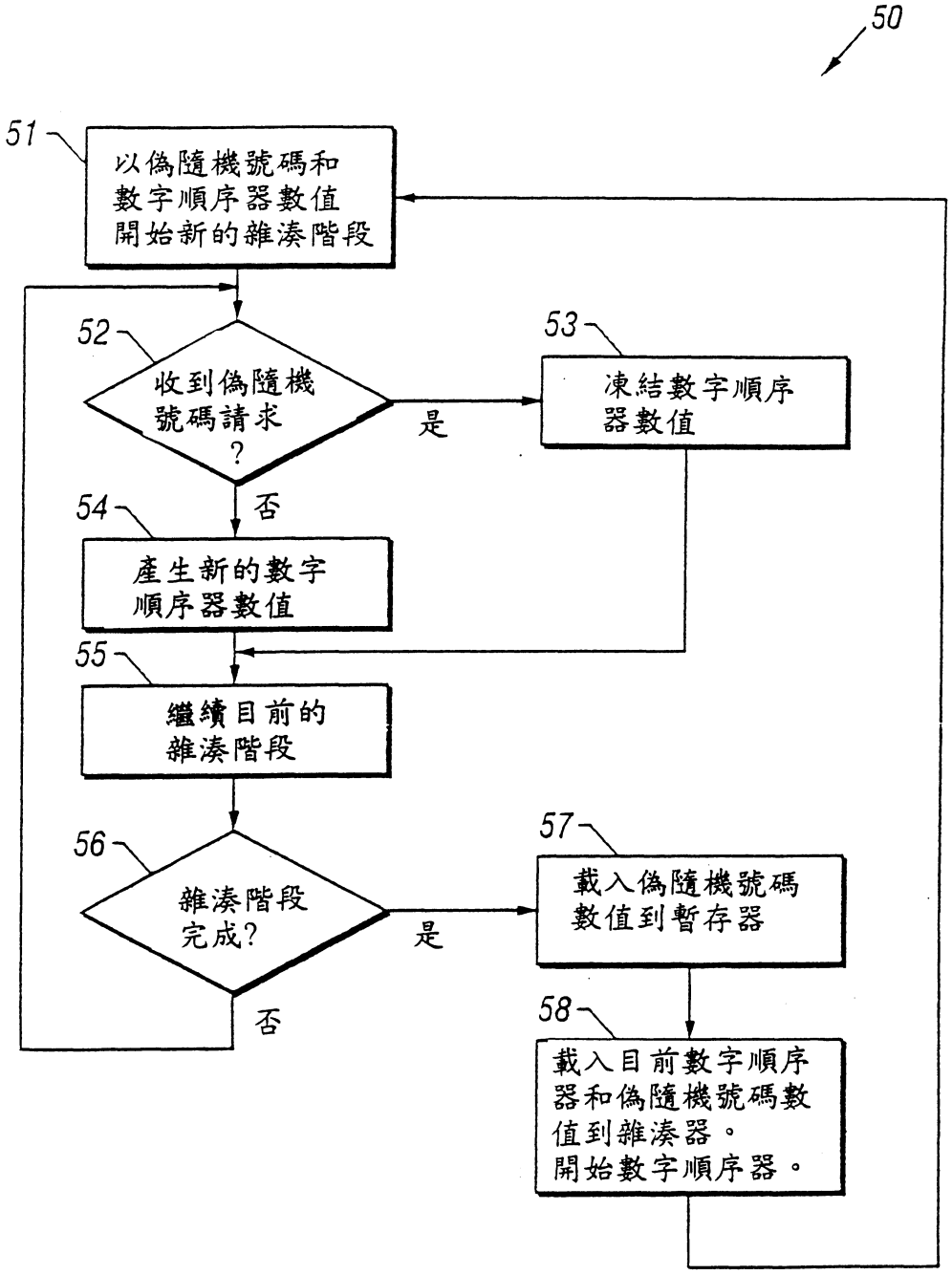

圖 5

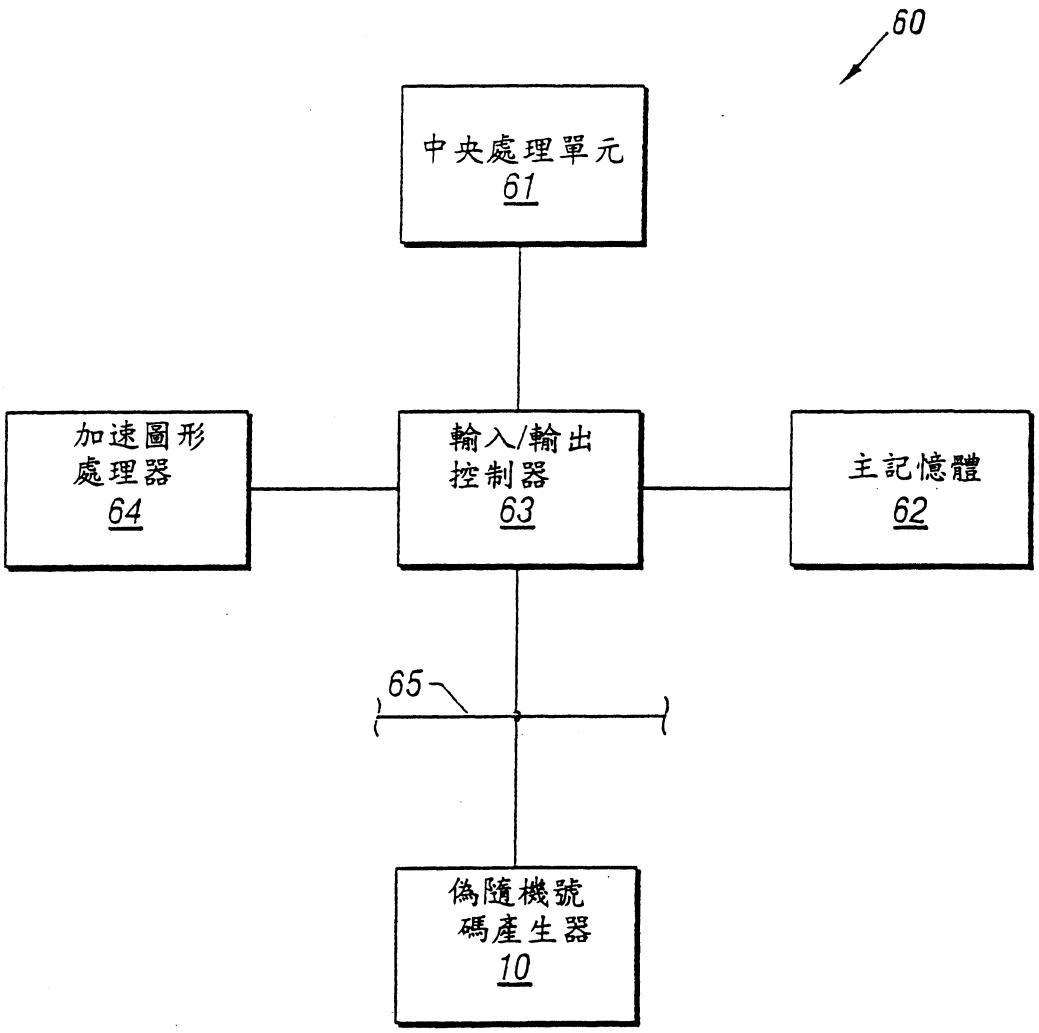

圖 6