公告本

302455

申請日期	85 年 4 月 8 日
案號	35104074
類別	G06F 9/06, 9/14

Int.·Cl[6]

A4
C4

302455

（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	防拷保護執行程式的方法及裝置
	英文	Method and apparatus for securing executable programs against copying
二、發明 創作 人	姓名	(1) 愛德華・休瓦茲 Shwartz, Edward L. (2) 麥可・高米希 Gormish, Michael J.
	國籍	(1) 美國　(2) 美國
	住、居所	(1) 美國加州門羅公園沙丘路二八八二號一一五室 加州研究中心理光股份有限公司 c/o Ricoh Corporation, California Research Center, 2882 Sand Hill Road, Suite 115, Menlo Park, CA 94025 U.S.A. (2) 美國加州門羅公園沙丘路二八八二號一一五室 加州研究中心理光股份有限公司 c/o Richo Corporation, California Research Center, 2882 Sand Hill Road, Suite 115, Menlo Park, CA94025 U.S.A.
三、申請人	姓名（名稱）	(1) 理光股份有限公司 Ricoh Company, Ltd.
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都大田區中馬込１丁目３－６ No.3-6, 1-Chome, Nakamagome, Ota-Ku, Tokyo 143 Japan
	代表人姓名	(1) 屋間健治 Hiruma, Kenji

裝 訂 線

302455

（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	1995 年 4 月 18 日	08/423,402	☑無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

五、發明說明（ 1 ）

發明背景

本案關於可執行防拷程式之保全設施之領域。特別是，在一實施例中，本發明提供一在一可接通執行程式及儲存該程式的記憶體的處理器的一開放硬體系統中之防拷保護。

由於軟體係以一獨立產品銷售，軟體發展人員已對防拷保護之保全電腦程式（軟體）有相當之研究。其困難點在於軟體易於拷貝且任何防拷保護或防護設計在其被執行時終究必需容許其軟體的部份拷貝。除非軟體被保護於一同時包含可執行軟體的微處理器之晶片（積體電路）中，軟體之被執行部份必需自分佈媒體沿可監視之電路被傳至處理器。如此，爲使程式即安全又可被合法使用者使用，程式不同能在其一般存在之形式中或在其被合法使用者所執行的形式中爲可軟體的。

近來，由於程式研究人員之技術支援的需求增加，對完整文件之需求，及對病毒，某此軟體的非法軟體，特別是重要的商業軟體，已然消失。但是，在不需支援或文件處理，且被用於諸如使用其中遊戲軟體被儲存於惟讀記憶體（ＲＯＭ）中的電動玩具卡匣的電視遊戲系統的無病毒之系統所使用的軟體仍受防拷保護。其所需要的既是對用於遊戲卡匣的了解及一份遊戲程式。

此外電視遊樂器的製造者，由於其一般製造電視遊樂器之控制板並希望限制其遊戲者使用由經授權的生產者所生產的遊戲，不關心軟體拷貝，而是在於用以製造可執行

五、發明說明（ 2 ）

經授權或非授權的遊戲卡匣控制板，以及相容性之遊戲卡匣。

在一未經保護的系統中，一拷貝者（亦即，一〝軟體海盜〞或其它未經授權的軟體的分析者或拷貝者）可輕易地拷貝可取得之程式。在此處所用的程式資料係指執行程式所需的資料，其包括指令（程式碼），變數及用以產生螢幕影像的影像資料表。即使若程式碼無法輕易地以其分佈形式被存取，一拷貝者可藉由在儲存程式資料的儲存媒體及處理器間設立一匯流排以決定程式碼而獲得。如此，由於其在被使用時終究要被解碼，程式資料的編密碼本身並不能提供實質的防拷保護。在程式資料被儲存於遊戲卡匣及處理器位在一電視遊樂控制板的情況下，分析程式資料被簡化，因爲其間無任何隱藏之通信使介於儲存媒體及處理器間的界面容易取得。在許多電視遊樂器控制板中，ＣＰＵ的整個匯流排可輕易加以分析。當然，此特殊問題發生於所有可折式之程式儲存媒體，而非僅限於電視遊樂器卡匣。

許多防拷保護系統可防止一般的拷貝者，但對特定拷貝者無效。其可能願意花費大量金錢及時間用以打開防拷保護系統以便大量製造份數的非法程式。對某些一般拷貝者而言，使用一單純軟體的防拷保護已足夠，例如使用一般拷貝者所無法進入或破解的祕密檔案或碼。許多一般拷貝者在遇到涉及卡匣結構之拷貝即放棄拷貝，因爲其需要製造塑膠盒及電路板的能力。但是，卡匣的最專門拷貝者

五、發明說明（ 3 ）

通常爲計劃製造大量卡匣以供販賣者，因此一旦程式被拷貝後其具有製造卡匣的能力。

單純軟體的防拷保護系統，其可使用程式資料媒體的非文件部份來儲存隱藏碼，一般依賴〝模糊保護〞以僅防止那些不曉得拷貝方法的人製出可用之拷貝。因此，當其目的爲抑制大量及技術性拷貝者時，僅有軟體保護是不可靠的，所幸，如在電視遊樂器卡匣中之程式資料被分佈於包含硬體元件的情況中，可將硬體防拷保護包括於卡匣中。

許多硬體保護系統係依靠若知以程式之合法拷貝的硬體電路或裝置。該程式被執行時跑一常式以檢查該合法裝置之存在。若授權裝置不存在，則程式拒絕繼續或執行其它非期望之動作。這些防拷保護系統皆會受到兩種方式之破壞，而會使防拷保護失效。

在第一類的攻擊中，拷貝者會分析硬體授權裝置的電路以決定其重要元件並藉以複製資訊，將授權裝置非法化。即使若授權裝置的細節被埋藏於訂製的積體電路中，積體電路可使用化學剝離程序逐層以顯微鏡被檢視而被解出其電路結構。授權裝置的作業亦可藉由將授權裝置電路及處理器減速或加速進行觀察以幫助其對於一動作的詳細分析或者許多程式上之流通之高速分析。

在第二類的攻擊中，拷貝者會變更檢驗授權裝置之存在的軟體常式以使無論如何該常式總是回報授權裝置存在。藉由一附在一執行一程式的微處理器上的隨時可用之邏

五、發明說明（ 4 ）

輯分析器，一拷貝者可以慢速操作該處理器而使邏輯分析器記錄所有由微處理器所執行的指令及來至／自該微處理器的資料交通，然後使用此資訊以決定程式流。若程式流於存在該授權裝置（模擬－合法使用）及於不存在有授權裝置（非法使用）之下被記錄，則拷貝者比對程式流並決定在程式中的何處判斷授權裝置的存在。一旦位置決定，在該位置的軟體將被修改使檢驗授權裝置之存在的常式的結果永遠爲肯定。其經常是將一條件跳躍指令替換以一非條件跳躍或一ＮＯＰ（無消動作）。

所以，需要一種裝置可容許處理器在一可能不安全的匯流排上執行程式，並使拷貝者在複製與裝置分別使用的程式或複製裝置時必需作出超乎其所能承受之複雜工作。

發明概要

本發明提供一種保全系統用以在一不安全環境中執行程式同時使難以拷貝程式碼或相關資料。在依照本發明的一實例中，一程式記憶體包含密碼化程式資料（程式指令，資料表，數位化影像等）且包含於一積體電路中的保全電路被提供以將所需的資料藉由一處理器將之取出。在不同的實施例中，處理器爲一中央處理單元（ＣＰＵ），一影像像素處理器或其它需要程式資料的低階ＣＰＵ。將在一不安全系統中被處理器執行的部份處理步驟被利用不提供給處理器的部份密碼化程式資料執行於保全電路中的保全系統。保全晶片追踪程式記憶體中之那一段適合根據所

五、發明說明（ 5 ）

執行的程式碼被處理器所請求。保全電路包括一其中將程式碼解碼所需的解答值儲存於其中的解答記錄器。爲求保全，不同程式可使用不同的解答值。

由於存在有晶片剝層之可能，該解答可藉由一電池儲存於一揮發性記憶體中或以充電方式儲存於電容上，或放置及／或分佈於保全晶片表面上以使在取得揮發記憶體之前晶片剝層會將揮發記憶體井的電源切斷。

在一特定實施例中，保全晶片自程式指令抽取出分支陳述在密碼化之後及提供指令至處理器之前並將之儲存於內部分支表中。在一較佳實施例中，分支陳述在被密碼化之前被取出並儲存於程式記憶體中。因爲由分支表中可得知程式的可能流向，分支表僅需包含緊迫的分支表列，因而可節省記憶體。

在不同的實施例中，密碼爲複雜的傳統密碼而在其它情況中，爲節省硬體，其爲諸如ＸＯＲ´ｉｎｇ之較簡單密碼，而具備一假性亂數產生器（ＰＲＮＧ）之輸出。多數種類的其它的保全方式可因需要而提供。例如，若保全晶片被設置以讀取處理器匯流排，可設置一匯流排栓使保全晶片可監視所有的指令捉取以及自記憶體的資料捉取。例如，由於保全晶片提供所有分支資訊；分支間的程式流爲直線且已決定的。如此，保全模組可對所有分支間的匯流排動作上執行一核對和，將之與一編輯前之核對和作比較，且若核對和不符合時則拒絕提供更多的分支資訊，比如在若被提供至處理器的指令已被某方面的修改之情況下

五、發明說明（ 6 ）

。

保全晶片亦可包括一即時時鐘，ＲＣ（電阻－電容）時間常數電路，或其它動態邏輯電路以確認處理器以一預定速率執行處理器。如此避免處理器被加速而使之快速執行程式而跳過所有建立一非授權分支表所需之可能性或者免於被減速而進行硬體分析。

再者，由於保全晶片維持分支表，其可計算下個分支，因此處理器僅需提供估計是否採取一條件分支所需之值。爲處理送回指令，保全晶片亦維持處理器之程式堆疊。此保全功能避免處理器請求非預期之資訊。

爲使在密碼化程式資料選擇文件攻擊更爲困難，程式資料可先被壓縮而將資料中之圖案移去。

密碼化及解密碼化可如傳統的密碼／解密碼之方式執行。但是，若在降低硬體成本爲前提下，密碼器可僅爲一將程式資料的位元或位元組之順序依照ＰＲＮＧ的輸出作重組的一資料拌碼器。資料解密碼器則僅爲一序列之緩衝器，多工器及一解多工器。在保全晶片包括解壓縮的情況中，緩衝器可能已存在於解壓縮器中。若拌碼器被連同其它密碼化作業一起使用，選擇文件攻擊將更爲困難，因爲在資料中的任一字元或位元的位置將不法被推測。

ＰＲＮＧ中解答值所支持或根據該解答而得到一同意值。因爲檔案被壓縮，可使用較弱之密碼。爲進一步避免被分析，該分析中密碼程式資料的許多不同段被與封應的解密碼資料作比較以決定該解答值，因段而不同的次要解答值

五、發明說明（ 7 ）

被使用。另外，次要解答之一表可連同程式資料被儲存或被儲存在保全晶片中，而主要解答值被用以自該表選擇解答。

在某些應用中，希望阻止在一非授權遊戲控制板上的一授權遊戲卡匣之作業。對這些應用而言，遊戲控制板被設置以一難以拷貝的元件且在遊戲卡匣上的保全晶片在作業開始前即需設置這些元件。

本發明的特性及優點可參照以下之說明及所附之圖式而被進一步了解。

較佳實施例之詳細敘述

圖１顯示本發明的一一般應用，亦即一電視遊樂器。在閱讀以下說明後應可清楚了解本發明並不限於電視遊樂器或儲存於卡匣中之程式。在圖１中，一遊戲控制板１０具有一將經由一匯流排１４被搭配至遊戲控制板１０的一遊戲卡匣。在此假設一拷貝者可讀取被儲存在遊戲卡匣１２中的遊戲程式及遊戲資料且知道在遊戲控制板１０中的所有情況。依照保全裝置的設計中之較佳操作，亦可假設拷貝者知道任何保全電路及運算之所有細節，除了任何解答或密碼之外。因爲該系統的主要目的爲容許一合法使用者去執行該程式，因此不可能避免拷貝者藉由以一組特定輸入資料來決定程式的結果及流動情形。如此，本系統的電路之目的在於要求程式被實際地以一般速度執行，並限制可以一組輸入資料推測自程式之一次執行的有關程式

五、發明說明（ 8 ）

的有限量之資訊。決定實際程式碼及資料的不可行性係根據是否用以破解系統的輸入資料組數過高而使執行如此之分析所花費的時間大於，或相當於此程式之合法銷售之數量所需之時間而定。

遊戲控制板１０具有一處理器２０，局部記憶體２２，一至影像顯示器１６之輸出界面，一來自輸入裝置的輸入界面１８，及一電路時鐘２４。遊戲控制板可包括其它未顯示的元件。輸入裝置１８被概略顯示，因爲其非本發明之重點，其可包括鍵盤，搖桿，軌跡墊或感應陣列。影像顯示器１６一般爲一像素顯示器（例如一保全監視器），其可顯示一由處理器２０或中間影像記憶體（未顯示）所指示的彩色像素二次元陣列。局部記憶體２２儲存用以執行程式以及程式之指令的目前頁數的變數。局部記憶體２２不需一次儲存整個程式，因爲程式可被翻頁至所需的局部記憶體２２。由以上之敘述中可清楚看出，保全系統參照遊戲系統之ＣＰＵ的處理器２０而被敘述，但是本發明亦可搭配影像處理器，畫像處理器或其它存在於該系統中的處理器而運作。

遊戲卡匣１２具有一保全晶片３０及一ＲＯＭ３２。其它形式之儲存器可代替ＲＯＭ３２，例如ＣＤ－ＲＯＭ（光碟ＲＯＭ），碟片，快閃記憶體或甚至經由一網路存取之遠方程式。ＲＯＭ３２包含一密碼化之遊戲程式。如此儲存的遊戲程式包含程式可執行碼，資料表，圖形畫像及其它相關的以卡匣實施之遊戲的作業所需或相關的物件

五、發明說明（ 9 ）

。在一較佳實施例中，保全晶片３０爲一不具保全資料流流於可外部接通之接腳上的單一積體電路。

本發明無法保護所有的攻擊。例如，若拷貝者自一遊戲製造者的不肖員工取得其未經密碼化之遊戲程式，則本發明無法防止拷貝者以該形式發行該遊戲。此處假設非授權拷貝者僅可取得一遊戲控制板及數個遊戲卡匣。在此限制取得之下，拷貝者將試圖使用如圖１所示的不同的分析及控制工具４０對控制板及卡匣的作業加以分析。一分析工具記錄信號，而控制工具改變信號，而同時分析工具正在記錄信號。此種工具包括微處理器追踪分析器，波形產生器，示波器等。圖１顯示在遊戲控制板１０及遊戲卡匣１２中拷貝者可下手分析及控制信號的幾個位置。特別是，拷貝者在沒有對保全晶片作化學剝層及進行顯微處理之下無法監控保全晶片３０的內部線路。

對於時鐘電路２４的一栓４１可被用以將遊戲控制板１０的處理速度減緩以更容易地分析其作業，或用以將電路時鐘加快以快速執行許多指令以測試不同的程式。爲使此栓失效，保全晶片３０亦可維持一若電路時鐘２４不以正確速度執行時則在保全晶片３０的內部決定拒絕將程式資料解密碼化的時鐘。

對ＲＯＭ３２之一栓４２提供拷貝者ＲＯＭ３２之內容，但在沒有由保全晶片３０所提供的解密碼下這些內容是無用的。對在匯流排１４上的資料交通上的一栓４４或在處理器２０及局部記憶體２２間的資料交通上的一栓

五、發明說明（ 10）

43可提供經解密碼的程式資訊，但僅提供用於對於遊戲之一執行的程式序列之情況而非可供不同組輸入使用的一序列。再者，該資訊不包括分支指令，其不被送至處理器，而被執行於保全晶片30中。

對於影像顯示上的栓45亦然。雖然栓45可記錄所有影像信號，其將僅對應至遊戲的一特殊戲局。例如，若一遊戲等級包括一從未被達到之圖面時，在該遊戲等級的圖面永不送至影像顯示器16因此無法被栓45獲得。

專業拷貝者可能在輸入裝置18及處理器20之間的信號上作一栓46以插入在遊戲中摸擬不同結果及事件的信號。在足夠的不同路徑之下，一拷貝者可能可決定所有的可能性以及反向工作以重建該遊戲程式，但因爲處理器的速度不能被增加以及由於機率極低，拷貝者不可能在遊戲公開於大眾及該遊戲售出足夠數量的時間內完成該工作，而影響到拷貝者的潛在市場。

如此，即使藉由所有的這些栓，僅進入遊戲控制板10的拷貝者無法達成一完整，可用之遊戲程式的拷貝。專業拷貝者可能將栓建立於保全晶片30本身的內部，其必需小心地將保全晶片的外殼移去並逐層分析保全晶片30。但是，即使知道保全晶片30的整體內部電路，拷貝者將無法取得用於將ROM32解密碼所需的解答之揮發性設定，因爲記錄這些解答的記憶體被設計爲當層被移去時將失去電力。若記憶體是在需要電力的層之下面數層，則記憶體在該層可被分析之前即已被抹除。爲破解保全

五、發明說明（ 11）

晶片３０，拷貝者必需分析ＲＯＭ３２的內容以及保全晶片的輸出以推出該解答。除了每一不同遊戲（不一定指包含該遊戲的每一遊戲卡匣）有不同的解答之外，保全晶片３０包含其它的功能，例如使拷貝者在未進入保全晶片３０的內部之下破解該密碼的工作更爲困難。

圖２更詳細地顯示保全晶片３０，其包括一將保全晶片３０耦接至匯流排１４並將程式資料之請求傳至一電晶體５２的一匯流排單元５０。電晶體５２將存取請求的地址轉換爲一地址位置，或在ＲＯＭ３２中之位置範圍。此地址由一地址匯流排５４被送至ＲＯＭ３２，其將該資料由資料匯流排５６送回。另外，ＲＯＭ３２的一些位置可在快取記憶體６０中被快取，其中若電晶體５２將地址資訊送至快取記憶體６０，則其供應快取之資料。

所有資料之來源皆被耦接至一解密碼器６２的一輸入，其將來自ＲＯＭ３２的資料利用一供自解答暫存器６４的解答值予以解密碼。如以下所解釋，不同解密碼器６２的構造視所需之保全程度而存在。由於解密碼器６２多少被限定於一用於將程式資料密碼化的一密碼器之一反向結構，以下討論有關密碼器之不同結構。

解密碼器６２的輸出被供飼至一選擇性之解壓縮的輸入。解壓縮器６８於是將該資料傳至路徑７０。路徑７０包括一清除ＲＯＭ資料的輸出以及用以隱藏資料的一栓。清除ＲＯＭ資料爲非密碼化程式碼及資料物件，但無分支資訊。隱藏資料包含分支資訊以及其它變數，諸如核對和

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 12）

以及預期之執行次數等。

隱藏資料輸出被耦接至一計算單元７２的一輸入，其處理保全晶片３０的所有控制。計算單元７２亦包括一用以讀取自及寫入至私用表７４的一埠，一用以讀取自一即時時鐘７６的一輸入，一用以自匯流排單元５０接收分支請求的輸入；一用於耦接至匯流排單元５０的分支回應之輸出，一來自提供有關發生於一處理器匯流排或匯流排１４上的動作之資訊的匯流排栓之匯流排單元的一輸入；以及用以接收及回應來自匯流排單元５０有關程式資料之請求的優先順序之疑問的埠。此保全晶片３０的詳細作業將參照圖４敘述如下。

圖３爲用於將一遊戲程式１１２密碼化爲一將被用於遊戲卡匣１２中的一經密碼化之ＲＯＭ３２的一系統１００之一方塊圖。系統１００包括用於耦接至輸出一保全程式114的一分支分離器１０２的遊戲程式１１２之儲存元，一核對和資料１１８的檔案及時序資料１２０的一檔案。儲存元被用於這些輸出資料組且該儲存元被耦接至壓縮器１０４，其爲選用但爲最好採用。壓縮器１０４的輸出被耦接至一密碼器１０８的一輸入，其亦具有一用以自一解答暫存器１１０接收一解答值的一輸入。密碼器１０８的輸出形成ＲＯＭ３２的內容。

如以上所解釋，遊戲程式１１２包含程式可執行碼，資料表，圖形畫像及其它相關物件。如表１所示者爲僅用於解釋用之程式可執行碼的一短例。表１所代表的程式爲

五、發明說明（ 13）

一〝清除〞程式，其中所有以任何可能的輸入執行該程式所需的資訊可由該程式本身清楚看出。事實上，自表1應可清楚看出，程式僅將陣列a口的前十個輸出移入任何可能輸入值的對應位置於b口中（例如，在a口中之值）。

表1.

線數	指令
0	i=0
1	if(i>=10)then goto 7
2	call 5
3	i=i+1
4	goto 1
5	mov a[i],b[i]
6	return
7	return

五、發明說明（ 14）

對應於表1的程式的C程式爲：

若表1的程式被供應至分支分離器102，將得到表2中所示的保全程式以及表3中所示的分支表。

五、發明說明（ 15）

表 2

表 2.

地 址	線 數	指 令
0	0	i=0
1	1	mov i,br_req-arg[1]
2		br_req 0
3	5	mov a[i], b[i]
4	6	br_reg 1
5	2	br_req 2
6	7	br_req 3
7	3	i=i+1
8	4	br-req 4

五、發明說明（ 16）

表 3

表3.分支表（隱藏資料）

BR # 分支	類形	爭議（s）	正確地址	錯誤地址
0	Cond'l	arg[1]>10	6	5
1	Return	-	-	-
2	Call	-	3	-
3	Return	-	-	-
4	Goto	-	1	-

在產生保全程式時，指令的順序可能被維持，以使線數依序排列。但是，若其依序排列，則被送至保全晶片30的地址之分析將指示是否作跳躍。例如，若線數如表2的保全程式的順序，一跳躍地址數的請求跟著跳躍地址n＋1的請求將指示有關地址n的跳躍將不作用（否則n＋1以外之一跳躍地址將爲下一個跳躍地址）。爲避免此

五、發明說明（ 17）

類的分析，在保全程式中的線順序的攪亂。由於每一條件跳躍的一正及誤地址被儲存，跟在不作用的跳躍之後的碼不需被序列地跟在跳躍之後。

附錄A，B及C分別爲一清除程式的較長範例的表列，其對應的保全程式及分支表。附錄D爲用於分支分離器102（圖3）的軟體實施之程式的一表列。該程式被以〝awk〞語言寫成，其一般可通用於執行Unix作業系統的電腦上。可清楚看到的，附錄B在無參照附件C的分支表下無法被執行。

在某些實施例中，分支分離器102亦計算數個執行放參考分支表間的指令的一核對和。由於這數個指令並不包含任何分支，其每次必需被執行於相同次序，所以其核對和容易計算。這些核對和被當作核對和資料118儲存。同樣地，在某些實施例中，這數個指令的執行時間可被計算且當成時序資料120儲存。

若需要更多的反分析保全，而非使保全晶片30實施分支，則保全晶片30可產生岔斷以設置該提取分支。如此，則拷貝者將不會偵測到分支未被提取。

在保全程式114，分支表116，核對和資料118及時序資料120被產生後，若被使用，則此資訊被壓縮器104所壓縮。在一實施例中，壓縮器104爲如美國專利第5，381，145號，由Allen, Boliek及Schwartz持有，案名爲〝資料之平行編碼及解碼之方法及裝置〞一案中所示的狀態碼。壓縮不僅被用以容許更多

五、發明說明（ 18）

的資料被儲存於固定大小的ＲＯＭ中，且被用以將可能存在於資料中的圖形移去，使無解答的解密碼化更爲困難。

密碼器１０８可具備數種形式。若保全較使硬體成本壓低更爲重要，則密碼器１０８可爲一資料密碼標準（ＤＥＳ）密碼器，三－ＤＥＳ，或在資料保全技術中所知的更多保全密碼系統。可採用不同的密碼器１０８的實施例，其視遊戲所販售之國家以及其所要使用的國家之法律而定，同時取決於保全需要以及計算限制間之平衡。若密碼化程序的保全較使硬體成本壓低爲次要，則可使用數種較簡單的密碼電路。在一實施例中，密碼化僅爲將清楚資料與來自一假亂數產生器（ＰＲＮＧ）的輸出位元流作共斥〝或〞（ＸＯＲ）動作。在另一實施例中，清楚資料之順序根據ＰＲＮＧ的輸出而被記錄。在硬體成本之增加之下，這些方法可一起被使用。

簡單的密碼化屬低成本，因爲一ＰＲＮＧ可以幾個閘輕易地組成。參見圖７之由一移位暫存器所構建的一ＰＲＮＧ。圖６顯示一資料拌碼器１０６的內部結構的一詳細圖。資料拌碼器１０６使用數個緩衝器，但由於緩衝器原已爲壓縮器１０４的一部份，因此這些緩衝器並不增加成本。

在另一低本變化中，密碼化系與壓縮作組合。在此變化中，壓縮動作爲一狀態壓縮，其使用或然率表來決定最佳碼之使用。由於無論如何壓縮時需要這些表之記憶體，將之用於密碼化將不會增加額外授權裝置。他們被藉由依

五、發明說明（ 19）

照解答值或根據解答值之數字而在切始時或在壓縮過程中被植入而用於密碼化作業。此密碼方式的外加益處爲其避免一已知一般文件對密碼程序的攻擊，因爲在機率表有可能被建立之前壓縮程序不一定將被壓縮之資料中的圖形移去。由於解答值提供機率表的啓始，壓縮程序無法輕易地被分析。

在被解密碼化及可能地壓縮後，密碼器１０８的輸出被儲存於經密碼化的ＲＯＭ３２中。以下將參照圖１至４敘述使用經密碼化之ＲＯＭ３２的遊戲控制板１０及遊戲卡匣１２的作業。圖４包含圖４Ａ及４Ｂ，一併顯示處理器２０及保全晶片３０自請求一頁指令及／或資料開始（步驟１）之以保全方式執行遊戲程式的一部份時所採取之步驟。

爲便於實施，程式資料可能被分別於壓縮資料組中處理，而處理器２０藉由指示一指標至一壓縮資料組而請求一頁，或僅根據前一解碼頁而自有限組之頁中選擇一頁。爲更求保全，每一資料組可由一與其相關的隨機ＩＤ在程式被密碼化時被辨識。

一頁之請求被經由匯流排１４送至匯流排單元５０，然後詢問計算單元７２是否請求爲適當（步驟Ｓ２）。由於計算單元７２維持該分支表，可輕易決定那指令應該及不應該被處理器２０所請求。此功能避免拷貝者控制處理器２０而使其以一已知順序請求在程式的每一區塊而進而使拷貝者可清楚地組合整個程式。若請求不適宜，則計算

五、發明說明（ 20）

單元７２終止處理器２０（跳躍Ｓ３）。另外，計算單元７２可達成其它效果，諸如抹除解答值，抹除ＲＯＭ３２，造成資料對時間之緩慢劣化，或其它用以阻止進一步分析的步驟。在某些實施例中，計算單元７２藉由變化遊戲的流程而回應一被偵測之攻擊，使得若拷貝者成功地引導遊戲程式的流程，則被引導之流程將被限制。例如，計算單元７２可將程式流程限定於僅遊戲的前幾個階層。

若請求爲適當的，該頁被自ＲＯＭ３２中取出（Ｓ４）。爲達成此動作，該請求被匯流排單元５０所處理並送至電晶體５２。電晶體５２在處理器所用的地址與用於存取ＲＯＭ３２的地址相同時並不需要。如表１－２所示，地址並不經常對應。若密碼動作改變資料之地址則地址亦將需要翻譯。一旦其中儲存有請求頁的ＲＯＭ３２的地址被決定，該地址經由匯流排５４輸出至ＲＯＭ３２或快取記憶體６０。在任一情況下，請求資料被輸入至解密碼器６２。被送回之資料可爲程式指令或資料物件。若該資料爲程式指令，則分支表的對應輸入則包括該資料，連同核對和以及時序資訊，假如用到的話。

解密碼器６２使用來自解答暫存器６４的解答值以將資料解密碼。解密碼器６２爲密碼器１０８的反相結構，且解答值等於或爲儲存於解答暫存器１１０中的解答值之相反，其取決於所用之密碼的類型。解密碼資料接著被解壓縮器６８所解壓縮。這些元件的效果爲將圖３中所示的資料區塊１１４，１１６，１１８及１２０中的資料段再

五、發明說明（ 21）

生。此資料接著被分爲被經由匯流排單元５０傳回至處理器２０的保全程式（清楚ＲＯＭ資料）以及被送至計算單元７２的隱藏資料（分支表，核對和，時序資料）。計算單元７２將此資料儲存於私用表７４中（Ｓ５）。匯流排單元５０將清除之保全程式頁傳至處理器２０（Ｓ６）。如以上所解釋，保全程式頁本身並不容許拷貝者複製遊戲程式的作業。

一旦處理器２０具有一頁的程式資料，其執行在該頁中的下一指令（Ｓ７）。在執行該指令之前，處理器２０檢驗指令以視其是否爲一分支指令（Ｓ８）。若其非一分支指令，則處理器２０執行指令（Ｓ９）並檢查在該頁中之進一步指令（Ｓ１０）。若存在更多的指令，則處理器２０取得下一指令（回到步驟Ｓ７），否則處理器２０自ＲＯＭ３２請求下一頁（回到步驟１）。

另一方面，若指令爲一處理器２０不處理的分支指令，一分支請求被送至保全晶片３０（Ｓ１１）。若分支請求不適當，如步驟Ｓ１２中所決定，則計算單元７２將處理器２０（終止（Ｓ１３）。爲使一請求爲適當，其必需被預期，必需發生在預期時間，且該匯流排核對和必需正確。來自保全晶片３０的對適當分支請求的回應爲處理器２０所應分支的地址。當然，對條件分支而言，處理器２０將必需傳送一個或多個爭議至保全防拷保護保全晶片３０，其將計算何者爲正確地址以及將錯誤地址退回（Ｓ１４）。保全晶片３０接著將地址傳回至處理器２０（

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 22）

Ｓ１５），處理器跳躍至該跳躍（Ｓ１６）且在該跳躍取得指令（回到跳躍Ｓ７）。藉此方式，在處理器２０不被告知其爲何種分支或所有可能分支地址爲何之下一地址被提供給一分支。

計算單元７２被用以處理分支請求以及估計一分支的請求是否適當。爲達成此目的，其仗用一私用分支表，其當作私用表７４的一部份被儲存。此分支表不需儲存所有分支，僅儲存那些將到達者。對分支表中的每一分支輸入而言，維持有以下之欄：

種類－分支的種類，選自：

１）非條件跳躍

２）條件跳躍

３）次常式呼叫

４）次常式送回

條件一僅用於條件跳躍；指示所測試之條件。

地址（ADDRESS）1一對非條件跳躍及具有一正確條件之條件跳躍，此地址爲將被跳躍至之地址；對呼叫而言，其爲受呼地址；而對送回而言，其不被使用。

地址（ADDRESS）２一不用於非條件跳躍。對一具有錯誤條件之條件跳躍而言，此爲一將被跳躍至之地址；對呼叫而言此爲該送回地址，其被儲存於一堆疊中。其不被用於送回。

在某些實施例中，處理器２０不被指明，且從未被告

五、發明說明（ 23）

知將到達之分支表中的索引。在這些實施例中，分支表追踪那一分支索引應跟隨目前的分支。當然，下一分支取決於那一分支被提取，因此在這些實施例中資訊被儲存於以下的兩欄中：

下一分支１－指示在程式碼中之分支的索引，其爲ADDRESS　１後的碼中之第一個分支。

下一分支２－指示在程式碼中之分支的索引，其爲ADDRESS　２後的碼中之第一個分支。

核對和－在分支之前的所有程式碼的預期核對和。

執行時間－自前一分支至下一分支的預期執行時間。

密碼－執行目前分支所需的密碼。

類型欄指示分支的類型，以及，那些其它欄被使用。例如一非條件分支的一輸入（例如〝ｇｏｔｏ５〞）不需要包括一條件或一錯誤條件地址。當然，在某些系統中可能爲其它分支，諸如條件呼叫及條件送回。在某些高度保全系統中，ＮＯＰ分支亦可被包括於保全程式之中。

條件欄可被表示爲一運算子或一常數，用以將一變數與常數比較（例如，〝branch if（i>=10）〞）或僅爲一用以作變數對變數之比較的運算子（例如，〝branch if（X<Y）〞）。若變數需要比較，則他們被當成分支請求的一部份被處理器２０送至保全晶片３０。處理器２０不需被告知那一條件亦被採用，而只要告知有多少以及那些變數應當成一爭議被傳送。在一實施例中，類型（ＴＹＰＥ

五、發明說明（ 24）

）欄指示那一種類的條件欄被使用而一數值（ VALUE）欄指示所採用的常數值。

地址１及地址２欄供應目前請求分支的下一地址。對條件分支而言，地址２不被使用。對呼叫而言，地址１爲受呼地址且被供至處理器２０，同時地址２爲跟隨呼叫之後的指令的地址（亦即送回地址）。該地址２之值被置於一堆疊中以供稍後的對應送回分支之用。對一送回而言，地址欄皆不被使用；送回地址來自堆疊中。

表２顯示意欲由一諸如處理器２０的處理器所執行的一保全程式。當處理器取得一分支請求（其替換在清除程式中之一分支），處理器作出一分支請求並連同估計一條件所需的爭議將分支請求的索引送至保全晶片。例如，在表２中之地址４，一分支請求被針對一特定分支索引而作出。指令〝ｂｒ＿ｒｅｑ　１〞顯示輸入１爲將被使用的分支表。但是，對某些專門拷貝者而言，分支請求的索引可被用以取出分支資訊。例如，藉由抽取出足夠〝ｂｒ＿ｒｅｑ　１〞指令，拷貝者可決定其等同於一送回指令。依照順序，被索引之每一分支請求可被分析以決定每一分支的類型及條件。

爲使此類的分析更爲困難，指令之索引可被消除。如此，在指令〝ｂｒ＿ｒｅｑ　１〞及〝ｂｒ＿ｒｅｑ　２〞不可被處理器取得之下，其皆成爲僅有〝ｂｒ＿ｒｅｑ〞。索引資訊被儲存於欄下一分支１（ NEXT BRANCH　1）及下一分支２（ NEXT BRANCH　２）。由於所有分支皆

五、發明說明（ 25）

由計算單元７２所控制，在目前分支的地址之後的分支請求爲已知且因此可被容易地儲存。NEXT BRANCH 1欄包含當ADDRESS 1爲該分支被提取的分支之下一分支的地址而NEXT BRANCH 2欄包含當ADDRESS 2爲該被提取的分支的下一分支的索引。對一呼叫而言，ADDRESS 1爲受呼次常式的開始而ADDRESS 2爲在呼叫指令之後的指令的地址。如此，NEXT BRANCH 1爲在次常式中的第一分支的索引而NEXT BRANCH 2爲ADDRESS 地址之後的第一分支的索引。對呼叫而言，ADDRESS 2及NEXT ADDRESS 2被推入在計算單元７２中的一堆疊中。

在使用的情況中，核對和，執行時間以及密碼欄被用以決定分支請求是否爲經授權的。在一分支之後，來自匯流排栓的資訊被供飼至計算單元７２，其對匯流排資料作核對和直到找到一分支爲止。所得的核對和被與所儲存的核對和值相比較。若有不同，計算單元７２將採取行動以防止遊戲的進一步動作。核對和可被用於在處理器匯流排上的所有交通，當然除了變數資料以外。

同樣的，即時時鐘７６被用以記錄介於分支間的時間且該時間被與執行時間值相比較。若處理器時鐘速率已知則所預期的時間量可容易地被決定，因爲在分支之間無反向分支以及已知數量之指令。另外，不需一分離之即時時鐘。若一ＰＲＮＧ被用作解密碼程序的一部份，可將其設定爲每一指令週期計時，不無其是否被使用。如此，若額外指令被插入，該ＰＲＮＧ將使資料失去同步元並將之破

五、發明說明（ 26）

壞。

對特別靈敏的分支而言，一密碼（PASSWORD）值被分派，其中處理器必需供應將被提取之分支的密碼。密碼值可能由已知的處理器或局部記憶體的記憶體內容的組合計算而得。

將分支處理依賴於保全晶片可能較處理器執行一清除程式更爲耗時。若碼之執行具時效性，程式碼的所選段的保護將被除能以使處理器進行其本身的分支處理。另外，時效性程式碼所需的處理部份可由保全晶片執行以節省處理時間。

圖5顯示爲被用以實施以上規則的計算單元72的一部份之分支單元500。分支單元500接收來自分支表502的一輸入，來自一匯流排栓504的一資料，以及來自資料進入匯流排506的爭議，且根據這些輸入，其輸出一指示一不當分支被請求或一適當請求之分支地址的一信號。在某些實施例中，該分支地址被送至處理器20，而在其它實施例中分支地址被用以不告知處理器以這些指令的地址之下控制那些指令被提供給處理器20。

分支單元之作業如下。一旦在分支表502中的一輸入被選擇，值（VALUE），類型（TYPE），核對和（CHECKSUM），密碼（PASSWORD），時序（TIMING），地址1（ADDRESS 1），地址2（ADDRESS 2），使NEXT 1及NEXT 2等欄被輸出。VALUE欄爲相關於一條件跳躍且有關於與一常數之比較的一常數，

五、發明說明（ 27）

且形成一輸入至減法器５０８。其它往減法器５０８的輸入來自保留保全進入匯流排的最近內容的一暫存器５１０。減法器５０８提供用以將一變數爭議與一常數相比較之結果，且在某些情況中僅指示該一輸入是較其它輸入爲大，相等或較小。減法器５１２同樣地將暫存器５１４的輸出與耦接至暫存器５１０的第二暫存器５１４的輸出作比較。兩暫存器的輸出被提供至一控制段５１６。

控制段５１６決定錯誤信號是否被輸出以及控制兩多工器（ｍｕｘｅｓ）５１８，５２０。多工器５１８的輸出爲分支地址，其選自ADDRESS 1，ADDRESS 2及來自一堆疊５２２的一疊頂值中之一。多工器５２０的輸出爲ＮＥＸＴ 1，ＮＥＸＴ 2，初始值及疊頂值中之一。多工器５２０的輸出指示下一分支的索引且被供饲回分支表５０２之一索引輸入。初始值爲一指向地址鏈的第一分支之一指標，其使懸擺（PENDING）線被適當地啓始。

控制段５１６根據其輸入決定多工器５１８的那一輸出被致動，其如以上所示：當分支類型爲一非條件跳躍，一呼叫，一具有正確條件的一條件跳躍，地址１被選擇。地址２被一具有一錯誤條件的一條件跳躍所選擇且疊頂被一送回分支所選擇。在所有情況中，地址２被推入堆疊中，以用於下一送回中。

控制段５１６亦決定多工器５２０的那一輸出：當分支類型爲一非條件跳躍，一呼叫，或一具有一正確條件的條件跳躍，ＮＥＸＴ 1被選擇並供至PENDING線。

五、發明說明（ 28）

ＮＥＸＴ　２被具有一錯誤條件的條件跳躍所選擇且疊頂被一送回分支所選擇。

若來自分支表５０２的核對和值與核對和邏輯５２４所計算之當作來自匯流排栓５０４的核對和不吻合，若由監控即時時鐘７６而得的執行時間與由執行時間（時序）欄所指示的預期執行時間不吻合，或若由處理器２０所提供的處理器２０與密碼欄不吻合，則控制段５１６輸出一錯誤信號。

圖６進一步詳細顯示一拌碼器１０６。拌碼器１０６包含一解多工器（demux）６０２，一多工器，一假亂數產生器（ＰＲＮＧ）６０６及數個緩衝器６０８。有３個緩衝器６０８Ａ，６０８Ｂ及６０８Ｃ被顯示，但緩衝器之數目並不限於３個。在一輸入資料流上的拌碼器１０６的功效爲重排輸入資料流的位元，位元組，字元或區塊之順序爲一確定且可反相之方式。

爲達成此目的，解多工器６０２將在其輸入上的輸入資料元素（位元，位元組，字元或區塊）解析爲由其一最新假亂數所決定的輸出之一。當最新假亂數改變時，元素所指向的輸出改變。多工器６０４將被緩衝器所輸出的分離之元素流組合爲一流。由於緩衝器的設計，爲元素需要不等量之時間以在解多工器６０２及多工器６０４之間移動，元素被重排順序。每一緩衝器６０８或爲一先進先出（ＦＩＦＯ）模式，其改變其頭及尾，或爲一ＦＩＦＯ模式，其替換爲一後進先出（ＬＩＦＯ）緩衝器。在前者中

五、發明說明（ 29）

，每次元素被由左邊移入至一緩衝器６０８時，一元素被自右邊輸出至多工器６０４。且每次一元素被自右邊移入緩衝器時，一元素被自左邊輸出。在後者中，元素被自兩端推入緩衝器，但其被自右端輸出。元素自其被移入緩衝器６０８的該端由ＰＲＮＧ６０６所輸出的值所控制。

如此，在知道假亂數序列後，吾人可發現該記錄格式以並將之反相。爲發現假亂數序列，解答值必需要知道（其儲存於圖２的解答暫存器６４或圖３的解答暫存器），因爲解答值當成ＰＲＮＧ６０６之植入值。當然，若硬體爲最優先考慮時，拌碼器１０６可使用解壓縮器的部份，或解答值可被用以拌碼或修正內部解壓縮表，諸如機率估計或Ｒ－碼表。

若硬體邏輯爲特別重要時，可使用圖７所示的假亂數產生器（ＰＲＮＧ）。ＰＲＮＧ７００僅需要一解答移位暫存器７０２，一極大長度序列（ＭＬＳ）移位暫存器７０４，兩個多工器７０６，７０８，以及一ＸＯＲ閘７１０。送往ＰＲＮＧ７００的輸入由一解答時鐘７１２，一ＭＬＳ時鐘７１４，一解答進入序列輸入，一解答載入信號及一啓始／執行信號所提供。一旦載入，解答移位暫存器７０２可被用作解答暫存器６４或１１０，並利用一不斷電電源７１６。

圖７顯示爲多工器７０６的輸出的送往解答移位暫存器７０２的輸入，其根據在多工器７０６的選擇輸入上的解答載入信號是否被插入而決定爲解答移位暫存器７０２

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 30）

的送回輸出或解答進入輸入。圖７亦顯示爲多工器７０８的輸出的送往ＭＬＳ移位暫存器７０４的輸入，其根據在多工器７０８的選擇輸入上的ＩＮＩＴ／ＲＵＮ信號是爲ＩＮＩＴ或ＲＵＮ而決定或爲解答移位暫存器７０２的輸出或爲ＸＯＲ閘７１０的輸出。送往ＸＯＲ閘７１０的輸入爲ＭＬＳ移位暫存器７０４的輸出以及來自ＭＬＳ移位暫存器的一非最終級的一栓。所用的特定栓以及在ＭＬＳ移位暫存器中的級數決定所得之假亂數序列之長度。序列長度及栓點的範例可見於Knuth D.E.，電腦程式之方法，第二版，１９８１，第２７－２９頁，及表１。在一實施例中，ＭＬＳ移位暫存器７０４的級數（正反器）爲９８而在一解答值中之位元數爲９８，但其它長度及栓則有相同的工作效果。當然，在解答值中的位元數應足夠大以便拷貝者無法輕易地猜到其值。一９８級ＭＬＳ移位暫存器將產生一僅每$2^{98}-1$位元重複一次的位元序列。藉由如此多之級，移位暫存器不需極大長度。不使移位暫存器爲極大長度的一優點爲極大長度移位暫存器的栓組在業界爲人所熟知，因此非極大長度移位暫存器將更不容易進行逆向工程。

解答值藉由供以解答載入信號而被啓始載入，其中將解答供至解答進入輸入及計時解答時鐘７１２直到解答值被載入。一旦解答值被載入，解答載入信號則被掩蓋，因此解答時鐘７１２之計時僅在解答移位暫存器７０２中循環該解答值。解答載入信號應被永久掩蓋，其可藉由將解

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 31）

答加上一帶頭的〝１〞位元而達成。該位元接著被用以當其到達解答移位暫存器７０２的輸出時設定一正反器（未顯示）。該正反器時控制解答載入多工器是否可被提出以及由一不斷電電源所供電。

解答值被循環於解答移位暫存器７０２並將之讀出。當ＩＮＩＴ／ＲＵＮ信號被設爲ＩＮＩＴ時，解答值將藉由ＭＬＳ時鐘７１４被定爲ＭＬＳ移位暫存器７０４中，其連同解答時鐘７１２一起被計時。一旦被載入，ＭＬＳ移位暫存器７０４將執行並循環其變換之內容，當然其係藉由ＸＯＲ閘，以形成業界所熟知的極大長度序列之假亂數。該序列之假亂數可被自ＭＬＳ移位暫存器７０４平行讀出。藉由諸如剛才所敘述的低成本ＰＲＮＧ，多解答可變得更爲可行。

綜上所述，以上所述之敘述係藉描述一用以防止一僅可得到使用者之硬體部份及或執行程式所需的軟體的拷貝者拷貝程式資料的系統。雖然係有關提供於遊戲卡匣上及用於遊戲控制板上的遊戲程式之保護的特定用途之範例，然而亦提到其它的應用。再者，本發明即使在程式主要被用作軟體的亦有作用，只要設置有包含保全晶片的小型硬體成份即可。然而本發明在與習知技術相較之一改良爲程式資料被保持密碼化，直到其被一保全晶片解密碼化爲止，而即使如此亦非所有程式資料被提供給處理器一僅其流程由使用者所提供之特定組輸入所決定之程式的目前執行部份之程式碼爲可得的。不提供給處理器的資料亦僅在一

五、發明說明（ 32）

處理器所知道的請求程式資料的適當時間上可提供給處理器，否則永不提供給處理器。在後者中，保全晶片執行其當保全晶片提供所有程式資料則處理器可執行的作業。在一實施例中，由保全晶片所得到的資訊爲分支資訊。如此，每當一處理器遇到一分支資訊時，該指令僅可藉由保全晶片的協助而被完成。

以上之敘述亦述及保全晶片的內部結構及作業，一用以產生密碼化程式資料的系統，保全晶片及處理器在一般作業中以及在遇到一拷貝者之攻擊時之交互作用，以及根據一所儲存的解答值之低成本假亂數產生器。

以上之敘述爲說明用途而非限制用途。在透過本案之揭示熟習該項技藝者可明瞭本發明的許多變化處。僅藉由舉例，上述之敘述提及一本發明的一實施例，其保護遊戲程式使免於受非法拷貝及使用，然而本發明之揭示亦可用於非遊戲之用途。其它用途討論如下。

在依照本發明的一電視遊樂器之一特定實施例中，保全晶片追踪遊戲者所留下的〝生命〞數以及遊戲者必需進至下一級之所剩時間。保全晶片一次解碼一級之程式資料，如此開始時僅提供遊戲之第一級之程式資料。程式資料包含從未顯示於保全晶片之外的初始值且該值被用以設定該級之一計時器。若遊戲者玩該遊戲，當特定事件發生時程式告知該保全晶片。若來自處理器的資訊爲預期中，則遊戲被正常地使用。但是，若資訊爲非預期的，則時間可被加至計時器上或者〝生命〞可能被移除。若在計時器上

五、發明說明（ 33）

之時間被延展，則遊戲者必需等候更久以進入下一級。若由於程式被異於所希望之方式執行而造成時間頻繁地被延展，則計時器永不跳完而使遊戲者永遠維持在第一級。此方法較諸經將處理器關閉的保全晶片的優點爲如此當保全晶片在程式中首先偵測出問題時將較不明顯。

前一方法並非無優點。若處理器爲一容許錯誤之系統的一部份，其可能或不會受到拷貝者之攻擊，保全晶片可被用作一防止一錯誤處理器在其一旦錯誤後繼續運作的一裝置。相同的保全晶片可被用以當一不當執行被偵測時將處理器停止或發出一警訊，但此處假設非預期作業係由硬體或軟體錯誤所造成，而非拷貝者的一有心行爲。

其一非遊戲用途之範例爲處理器可執行影像處理。在影像處理中，可能需要一旋捲。一旋捲係由一系列之乘積及加成運算而得。由於保全晶片可監視處理器的資料匯流排，當乘積結果出現在匯流排時保全晶片可執行加法動作。當需要總合時，處理器自保全晶片請求之。若處理器在無保全晶片下執行時，則旋捲或是錯誤或是執行較慢，因爲其將必需自行累加之。

若程式資料被壓縮，解壓縮器的元件可被用於達成解密碼程序。例如，圖 6 顯示一資料拌碼器，其可由解壓縮器的緩衝器構成。同時，若解壓縮器爲一狀態編碼器，保全晶片可使用用以形成解壓縮程序的初始參數的解答值，其例如初始機率值。此具有防止位元之一對一映成之優點，此現象經常發生於在還未接收足夠的位元以自位元本身

五、發明說明（ 34）

推算機率之狀態編碼器之開始時。

當保全晶片偵測到保全侵害時，其不需將處理器停止。其它選擇爲在一隨機延遲後將處理器重新設定，輸出假亂數當成經解碼之資料或藉由互補致能而調整ＰＲＮＧ或其它方法以使ＰＲＮＧ緩慢地將輸出資料劣化。

因此本發明的範圍不應受以上之敘述之限制，需是參照所附之申請專利範圍連同其效之完整範圍而被決定。

圖式之概要敘述

圖１爲依照本發明的一電腦系統的一方塊圖，其中程式資料位在一經由一包括一在卡匣上的保全晶片的插入式匯流排被連接至一處理器的卡匣上；

圖２爲保全晶片的一更詳細之方塊圖；

圖３爲被用以將程式密碼化爲用於卡匣中之經密碼化記憶體的一系統之方塊圖；

圖４Ａ及４Ｂ一起顯示由一處理器執行一程式的一流程圖；

圖５爲一分支單元的一方塊圖；

圖６爲一資料流拌碼器的一方塊圖；

圖７爲一假亂數產生器的方塊圖。

A5
B5

四、中文發明摘要（發明之名稱：防拷保護執行程式的方法及裝置）

一種保全系統用以在一不安全環境中執行一程式碼，並使決定如何拷貝程式碼及相關資料成爲不可能，或至少不實用。一程式碼包含保護之程式碼且包含於一積體電路中的一防護電路被提供以將處理器所需之程式解碼。將在一不安全系統中被處理器執行的處理步驟的一部份利用未提供至處理器的解碼程式資料的部份在此安全系統的防護電路中被執行。程式資料根據自處理器至防護晶片的適當請求而被剖析。儲存於揮發記憶體內的解答值被用於解碼程序且揮發記憶體被置於該積體電路中使其內容在一晶片剝層分析到達揮發記憶之前被消滅。

英文發明摘要（發明之名稱：）

METHOD AND APPARATUS FOR SECURING EXECUTABLE PROGRAMS AGAINST COPYING

ABSTRACT OF THE DISCLOSURE

A secure system for executing program code in an insecure environment while making it impossible, or at least impractical, to determine how to copy the program code and associated data is provided. A program memory contains encrypted program data and security circuitry contained within an integrated circuit is provided for decrypting th. program data as it is needed by a processor. A portion of the processing steps which would be done by the processor in an insecure system is performed in this secure system within the secure circuitry using portions of the decrypted program data which are not provided to the processor. Program data is parsed it out based on a proper request to the security chip from the processor. A key value stored in volatile memory is used in the decrypting process and the volatile memory is positioned on the integrated circuit such that its contents are lost before a chip peel provides access to the volatile memory.

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

六、申請專利範圍

1．一種用以在一電腦系統中執行一保全程式的裝置，其中禁止自電腦系統拷貝保全程式之可使用之拷貝，該裝置包含：

一程式記憶體其中保全程式資料被以一密碼化形式儲存；

一耦接至程式記憶體的一保全晶片，該保全晶片包含：

用於將輸出程式之部份解密碼爲一清除部份及一剩餘部份之裝置；

用以提供該清除部份至可被一處理器存取的一記憶體位置之裝置；以及

用以儲存保全程式的剩餘部份的剩餘部份記憶體，該剩餘部份記憶體不可由處理器直接存取；

用以請求剩餘部份之次集合以供處理器使用的裝置；以及

在保全晶片中用以檢驗所請求之次集合爲在處理器之一特定之系統狀態下所預期應被請求之一次集合的裝置。

2．如申請專利範圍第1項所述之裝置，其中保全程式係在程式部份以及剩餘部份被分開儲存之下被儲存於程式記憶體中。

3．如申請專利範圍第1項所述之裝置，其中剩餘部份爲一組保全程式的分支指令。

4．如申請專利範圍第3項所述之裝置，其中保全晶片進一步包括用以根據最近執行的分支而快取分支陳述的

六、申請專利範圍

裝置。

5．如申請專利範圍第1項所述之裝置，其中用以將分支解密碼化的裝置被構建以一解密碼解答。

6．如申請專利範圍第5項所述之裝置，其中該解密碼解答被儲存於揮發性記憶體中。

7．如申請專利範圍第6項所述之裝置，其中該揮發性記憶體被分佈於保全晶片上，該保全晶片進一步包含覆蓋及模糊揮發性記憶體的至少一部份之覆蓋電路。

8．如申請專利範圍第7項所述之裝置，其中該覆蓋電路被耦接至揮發性記憶體的一電源以使覆蓋電路被移除將會連帶將覆蓋電路之電源移除。

9．如申請專利範圍第7項所述之裝置，進一步在保全晶片中包含一計時裝置，用以決定處理器的指令執行之速率，其中僅當計時裝置判斷速率處於預期範圍內保全晶片才會相應於處理器之請求。

10．如申請專利範圍第1項所述之裝置，進一步包含一用以在解密碼化後將保全程式解壓縮之一資料解壓縮器，其中該保全程式在被密碼化前被壓縮。

11．如申請專利範圍第10項所述之裝置，其中該解壓縮器爲一狀態解碼器。

12．如申請專利範圍第1項所述之裝置，進一步在保全晶片中包含一核對和裝置，用以判斷在處理器匯流排上的匯流排存取之一核對和，其中該保全晶片僅當判定核對和符合一預期核對和時才相應於處理器請求。

六、申請專利範圍

13. 如申請專利範圍第1項所述之裝置，進一步包含一用以依照一可逆向及一由一解答值所決定的確定形式記錄保全程式的資料元素之一資料拌碼器，其中該保全程式在被置於程式記憶體中之前藉由資料拌碼器之反向動作而被記錄。

14. 如申請專利範圍第13項所述之裝置，其中該資料拌碼器包含多數個先進先出緩衝器。

15. 如申請專利範圍第13項所述之裝置，其中該可反向及確定形式係參照一假亂數產生器的輸出而被產生。

16. 如申請專利範圍第1項所述之裝置，其中該解密碼裝置根據該解答值以永一假亂數產生器的輸出而運作。

17. 如申請專利範圍第1項所述之裝置，進一步包含用以當檢驗裝置偵測到一非預期次集合被請求時將保全晶片的作業以及程式流程改變，以使經改變之作業造成在程式流程以及作業上之負面效果的裝置。

18. 如申請專利範圍第17項所述之裝置，其中該改變裝置爲一用以中斷處理器的一裝置。

19. 一種用以保護保全程式使免於非授權拷貝的裝置，包含：

一用以自程式資料取出分支陳述的分支分離器；

一用以壓縮所取出之分支陳述以及一程式資料的剩餘部份以形成壓縮資料的一壓縮器；以及

六、申請專利範圍

一用以將經壓縮之資料密碼化的密碼器。

２０．如申請專利範圍第１９項所述之裝置，其中該分支分離器包含：

用以自動地產生代表程式資料的核對和的核對和資料之裝置；以及

用以自動地產生用於程式資料處理的存取時序之時序資訊的裝置；

其中該核對和資料以及時序資訊被壓縮器壓縮且被密碼器密碼化。

２１．一種用以執行一保全程式以防止一可用形式下之保全程式經由一不安全之處理器匯流排取得資訊而被拷貝之方法，包含以下步驟：

自不安全處理器接受程式資料之一區塊的一請求，該程式資料的區塊包括至少一或多個程式指令或一或多個程式資料元素；

以一保全方式將該程式資料的區塊解密碼爲一清除部份以及一剩餘部份；

提供清除部份至不安全處理器；以及

自不安全處理器接受剩餘部份的元件之請求；

根據不安全處理器及先前之請求檢驗該請求爲適當的；

處理來自不安全處理器之剩餘部份的元件之請求；以及

對應該請求，其中覆蓋剩餘部份元件僅參照對一請求

六、申請專利範圍

之回應的資訊內容不足以達成決定。

22. 如申請專利範圍第21項所述的方法，進一步包含以下步驟：

將一程式分爲清除部份以及剩餘部份以形成一保全程式；以及

在將該保全程式置入一拷貝者在對保全程式作非法拷貝時可存取之一記憶體中之前將保全程式密碼化。

23. 如申請專利範圍第22項所述的方法，其中分離步驟爲將保全程式的分支指令自保全程式的其它指令分離的一步驟。

24. 如申請專利範圍第21項所述的方法，其中解密碼的步驟係配合一解密碼解答而被實施。

25. 如申請專利範圍第24項所述的方法，進一步包含將解密碼解答儲存於揮發性記憶體中之步驟。

26. 如申請專利範圍第25所述的方法，進一步包含以下步驟：

提供一電源至該揮發性記憶體；

將該揮發性記憶體覆蓋以一層電路以使當電路受到干擾時該電源被自該揮發性記憶體移去，且該揮發性記憶體之內容在不將該電路移去之下無法輕易地被測出。

27. 如申請專利範圍第21項所述的方法，進一步包含在提供一回應至一資訊請求之前檢驗處理器的指令執行速率的一步驟。

28. 如申請專利範圍第21項所述的方法，進一步

六、申請專利範圍

包含將該保全程式解壓縮之步驟，其中該保全程式在被解密碼前被壓縮。

29. 如申請專利範圍第21項所述的方法，進一步包含以下之步驟：

判斷在一處理器匯流排上的匯流排存取之一核對和；

將該核對和與一預期被執行的保全程式的指令所預期的預先計算之核對和作比較；以及

當該核對和與該預先計算之核對和不同時防止保全程式之受外力打通之作業。

30. 如申請專利範圍第21項所述的方法，進一步包含以下步驟：

在儲存於一可被拷貝者存取的一記憶體中之前依照一可反向以及由一解答值所決定的確定形式將保全程式的資料元素之順序作拌碼動作；以及

因應處理器的適當請求而對資料元素之順序入解拌碼動作。

31. 如申請專利範圍第30項所述的方法，其中該解拌碼之步驟進一步包含產生用以形成可反向及確定形式之假亂數的一步驟。

32. 一種用以保護一程式防止非法拷貝的一方法，包含以下步驟：

依照非分支指令以及分支指令將程式分離；

將非分支指令壓縮以形成一第一組壓縮資料；

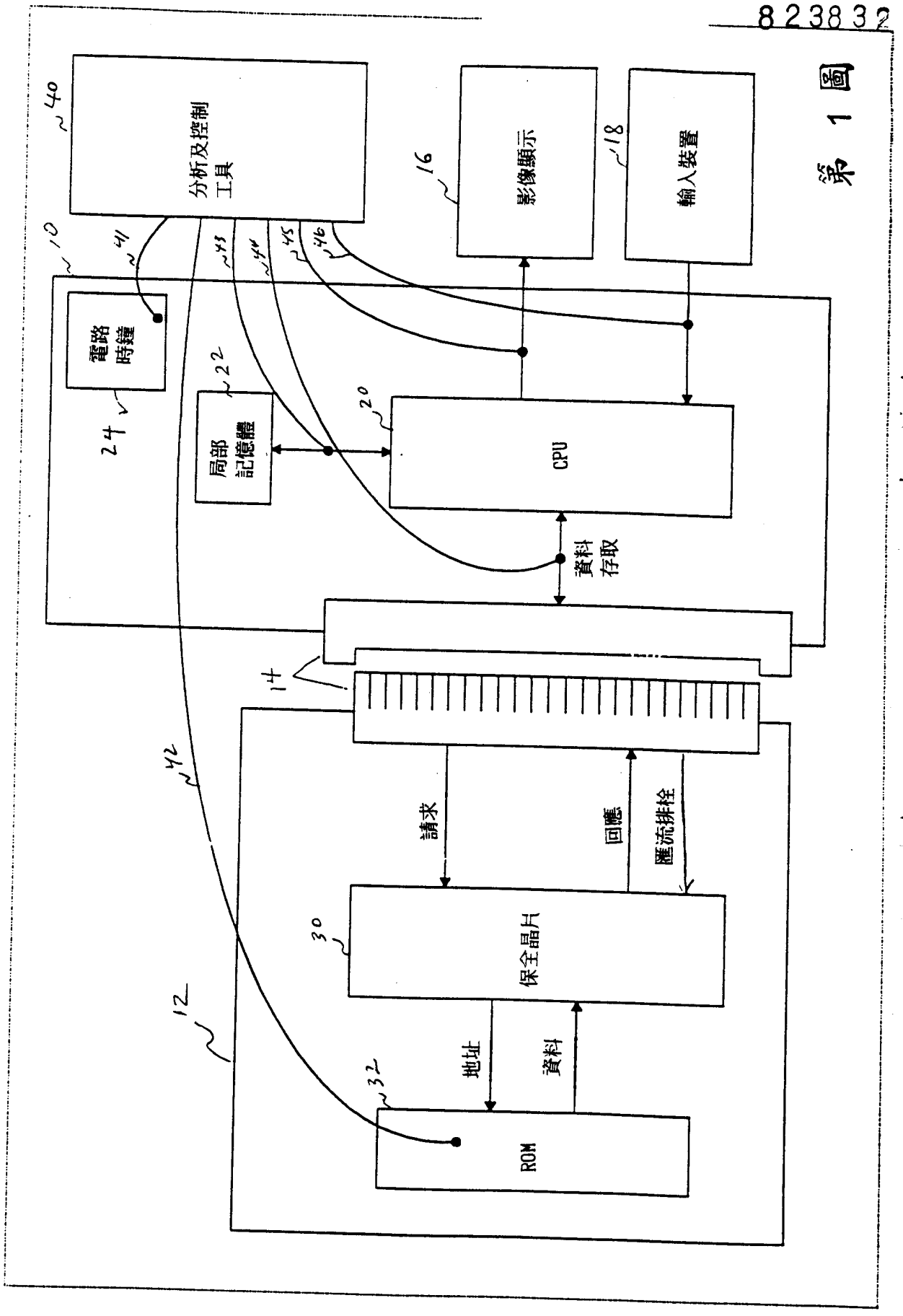
將分支指令壓縮以形成一第一組壓縮資料；以及

六、申請專利範圍

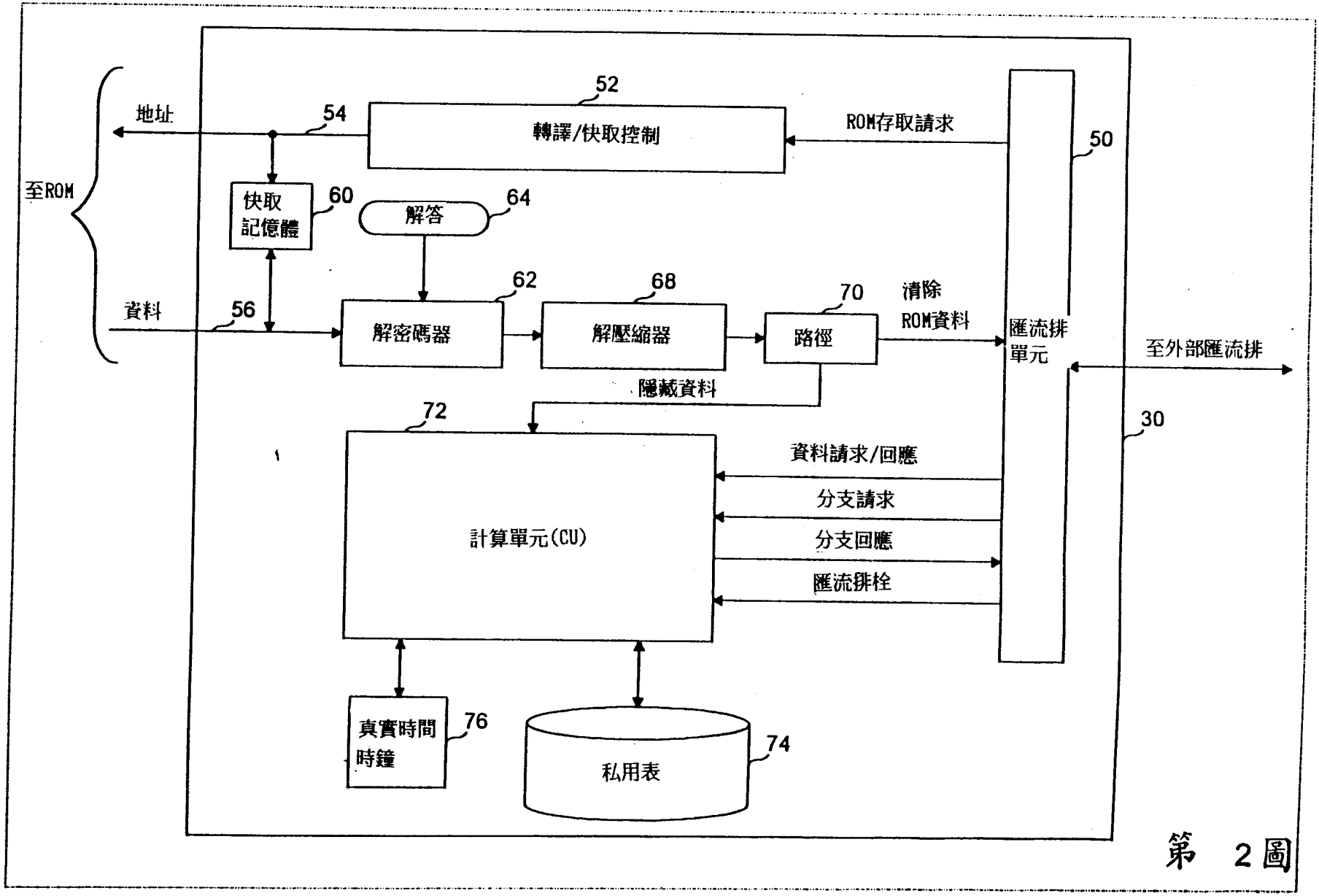
將該第一及第二組壓縮資料密碼化。

302455

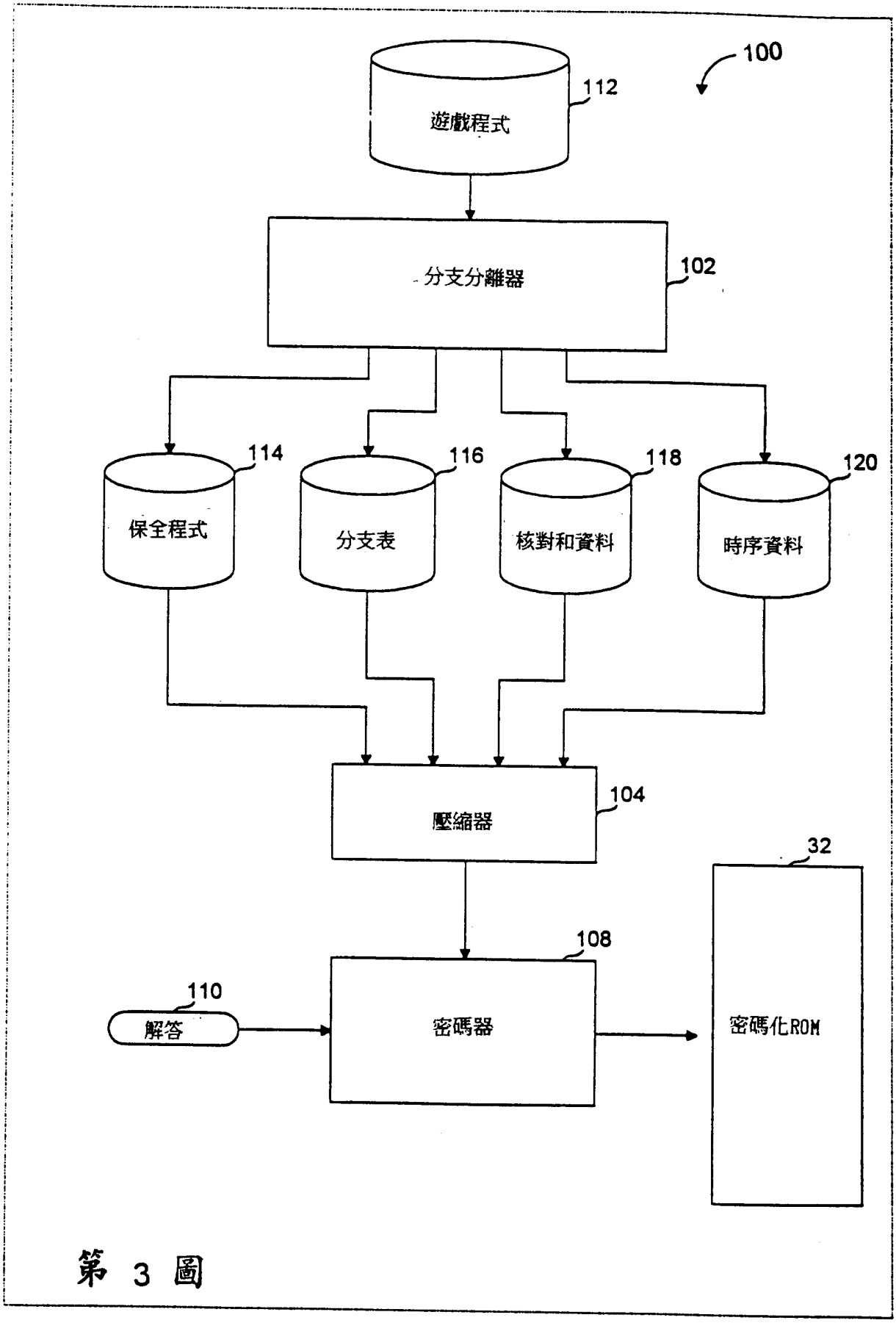
823832



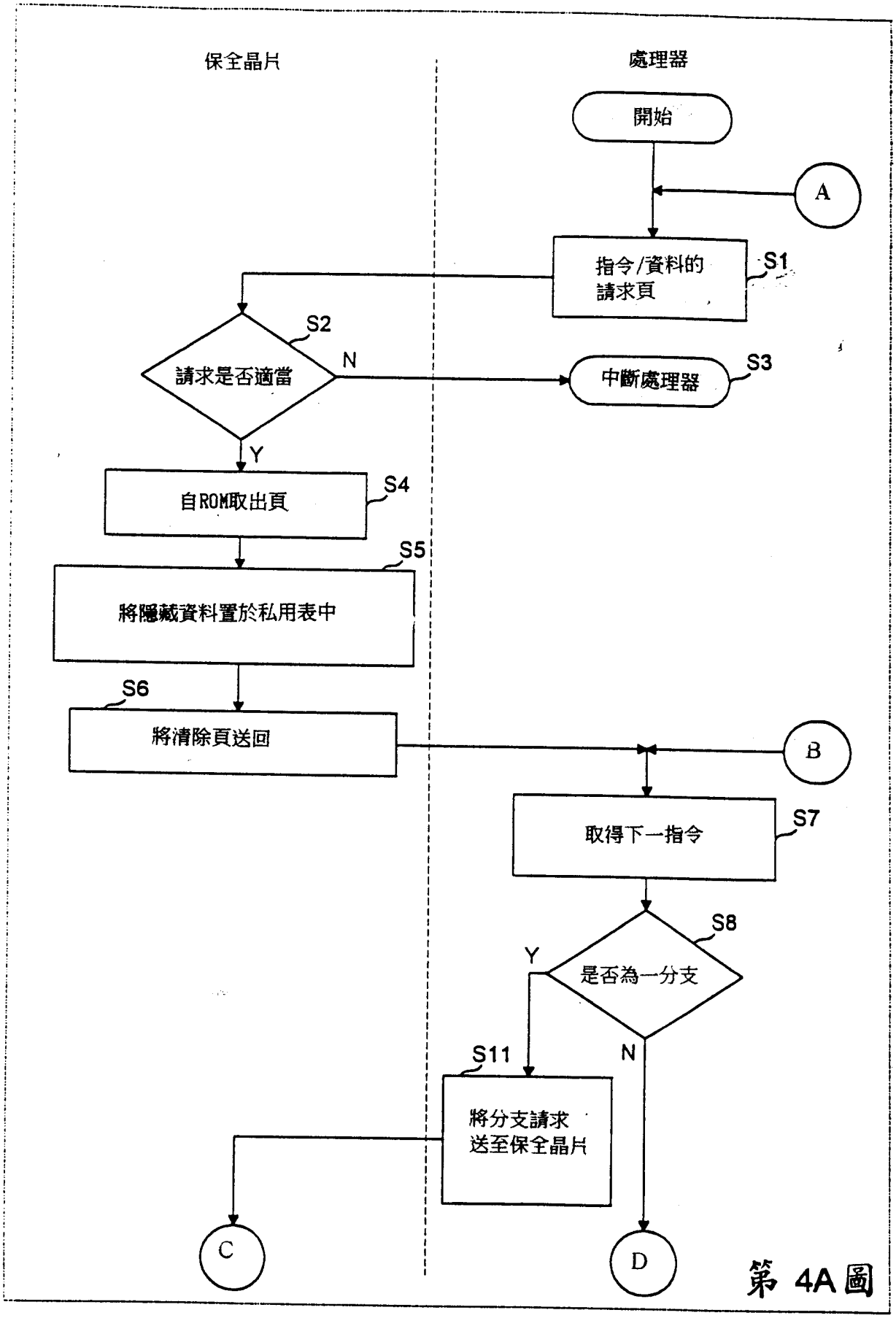
第 1 圖


52
地址
54
轉譯/快取控制
ROM存取請求
50
至ROM
快取
記憶體
60
解答
64
62
68
70
清除
ROM資料
資料
56
解密碼器
解壓縮器
路徑
匯流排
單元
至外部匯流排
隱藏資料
72
30
資料請求/回應
分支請求
計算單元(CU)
分支回應
匯流排栓
真實時間
時鐘
76
私用表
74

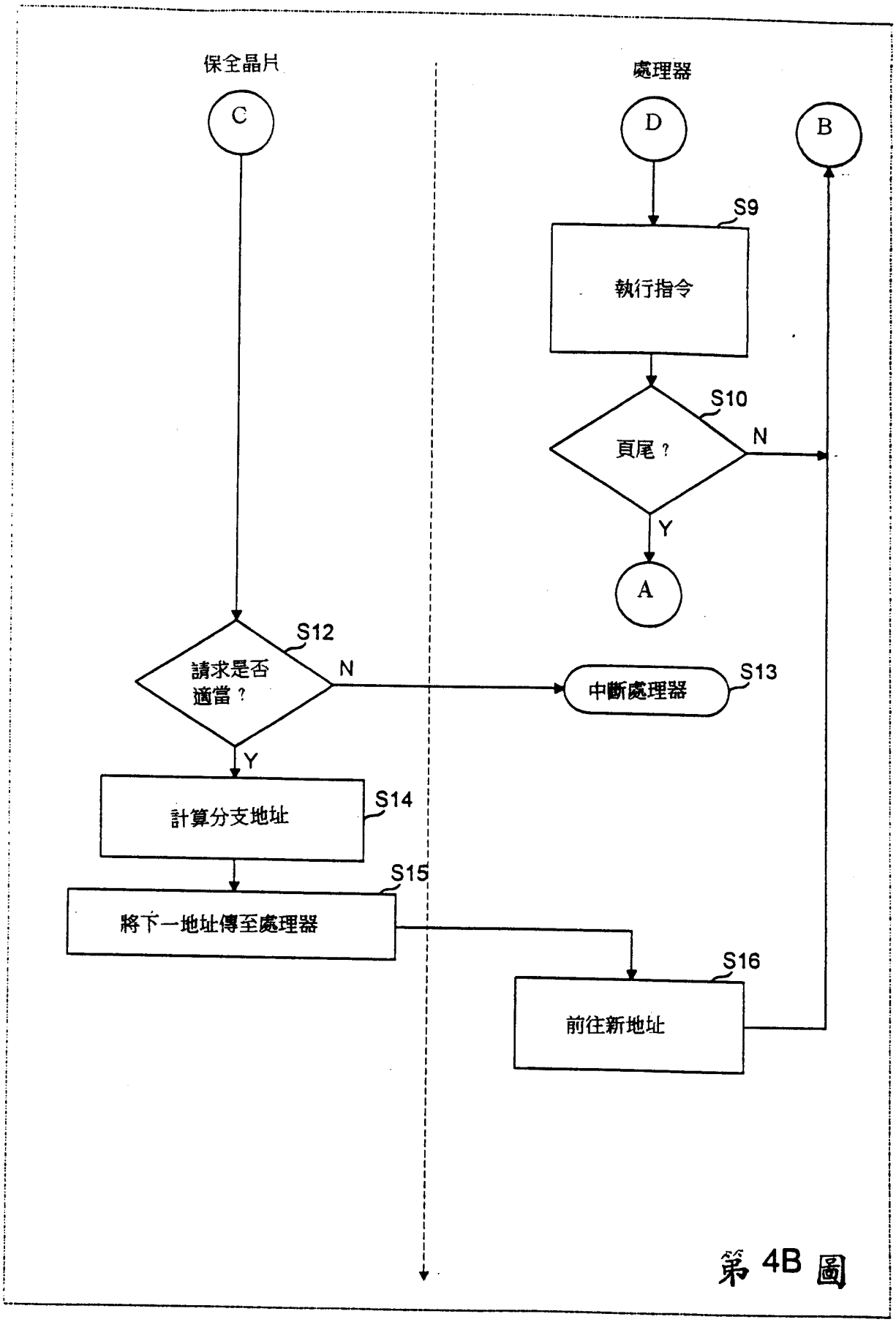
第 2 圖


100
遊戲程式
112
分支分離器
102
保全程式
114
分支表
116
核對和資料
118
時序資料
120
壓縮器
104
32
108
110
解答
密碼器
密碼化ROM

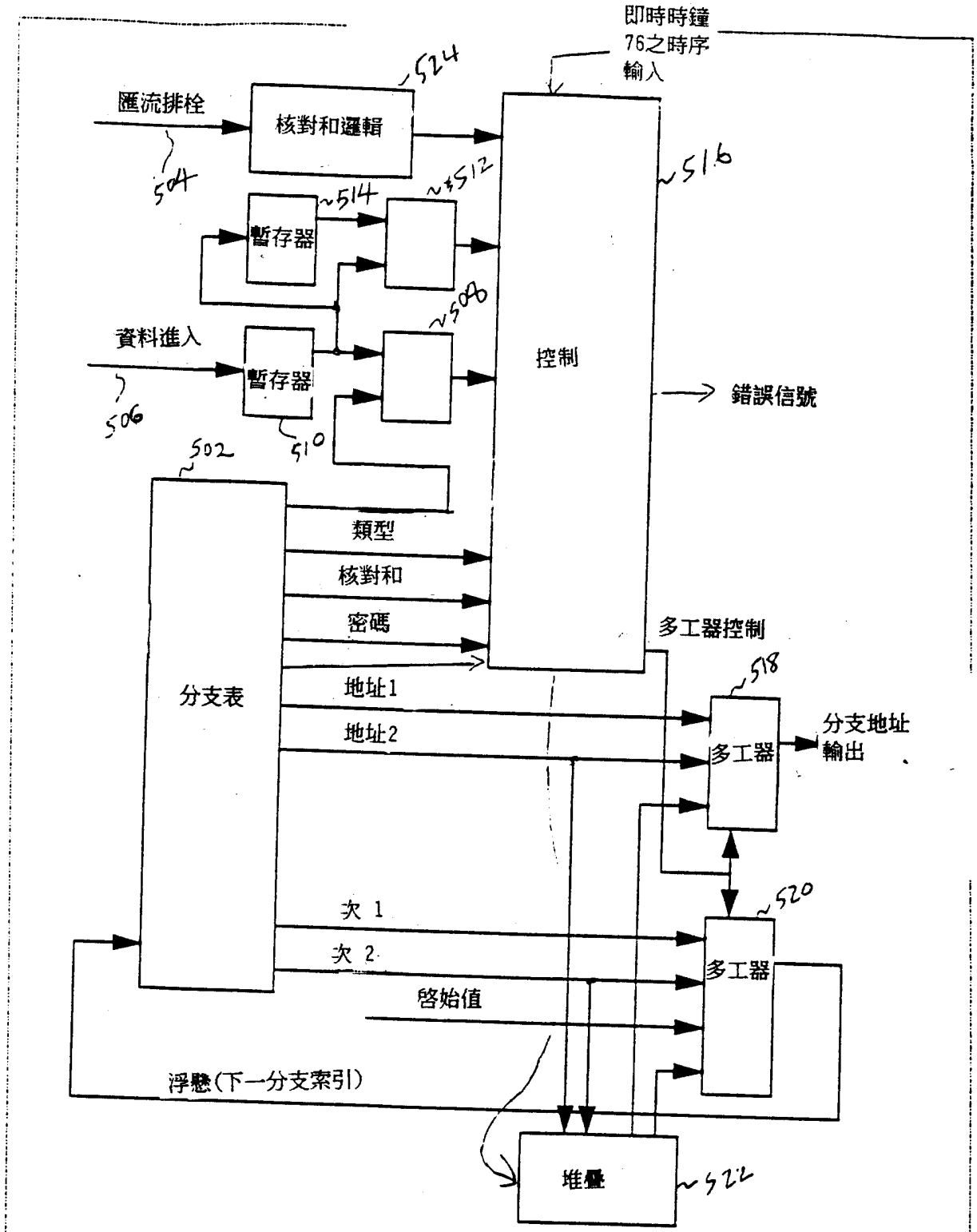
第 3 圖


保全晶片
處理器
開始
A
指令/資料的請求頁
S1
S2
請求是否適當
N
中斷處理器
S3
Y
自ROM取出頁
S4
S5
將隱藏資料置於私用表中
S6
將清除頁送回
B
取得下一指令
S7
S8
Y
是否為一分支
N
S11
將分支請求送至保全晶片
C
D

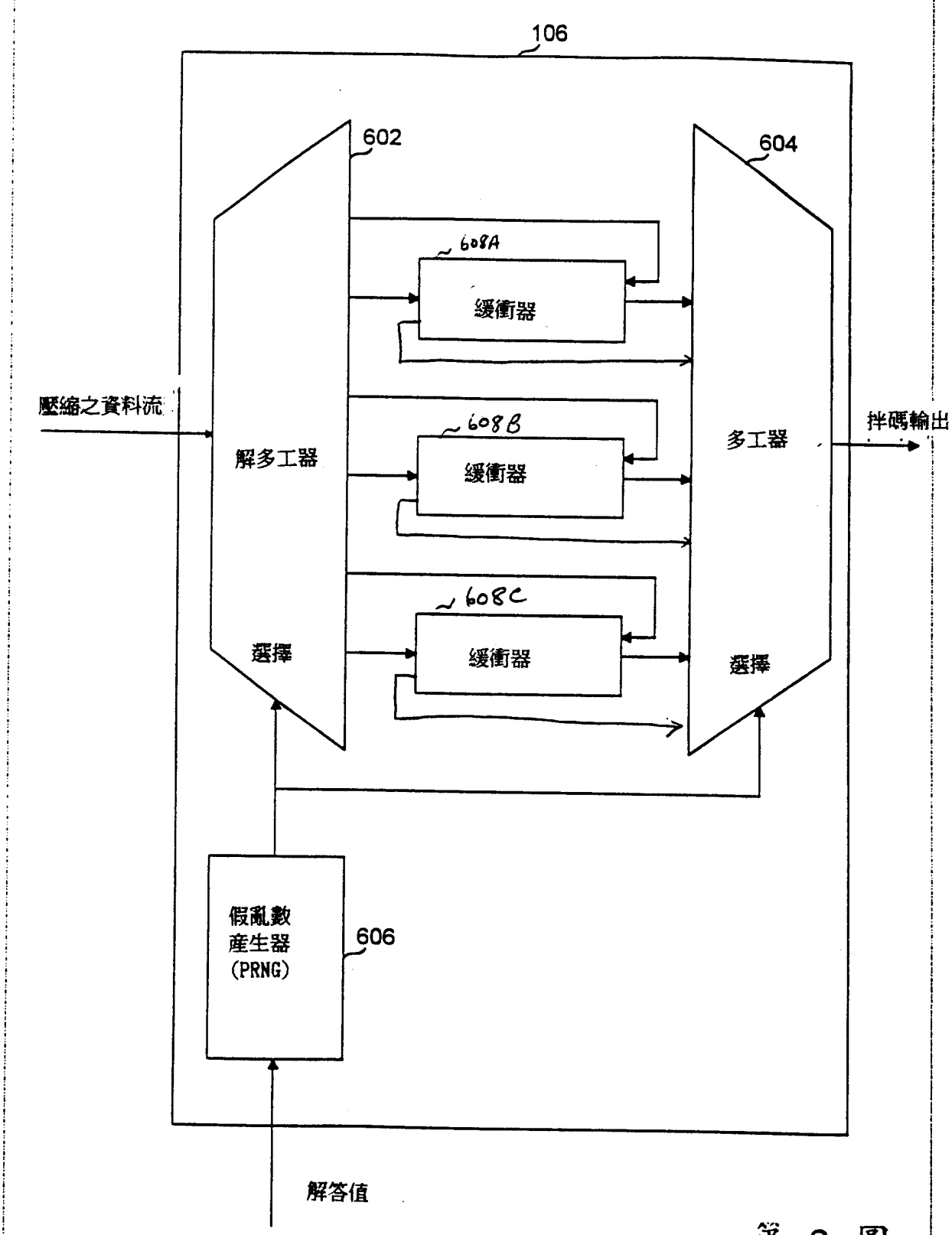
第 4A 圖


保全晶片
處理器
C
D
B
S9
執行指令
S10
頁尾？
N
Y
A
S12
請求是否
適當？
N
S13
中斷處理器
Y
S14
計算分支地址
S15
將下一地址傳至處理器
S16
前往新地址

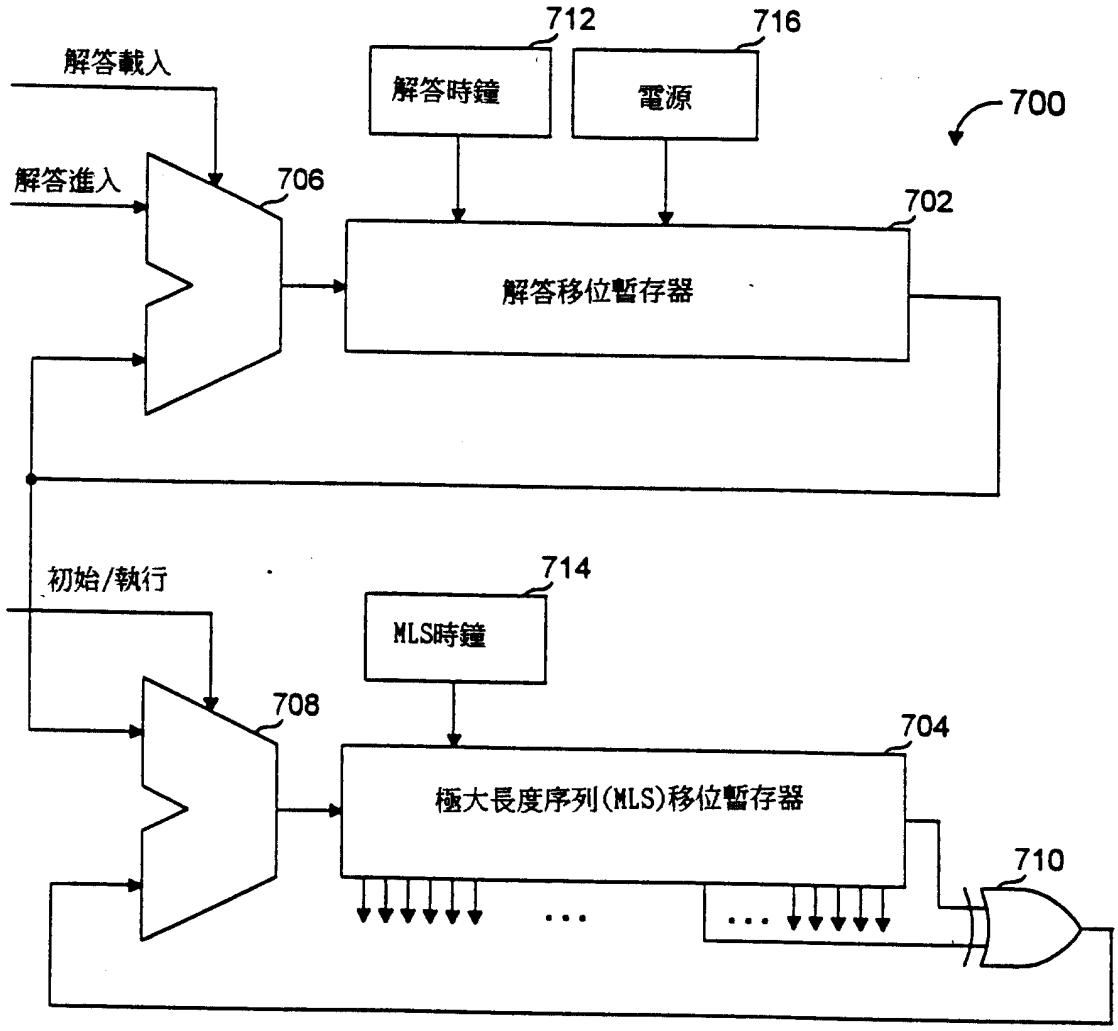
第 4B 圖


即時時鐘
76之時序
輸入
匯流排栓
504
核對和邏輯
524
暫存器
514
512
516
資料進入
506
暫存器
510
500
控制
錯誤信號
502
類型
核對和
密碼
多工器控制
分支表
地址1
地址2
518
多工器
分支地址
輸出
次 1
次 2
啓始值
520
多工器
浮懸(下一分支索引)
堆疊
522

第 5 圖


106
602
604
608A
緩衝器
608B
緩衝器
608C
緩衝器
壓縮之資料流
解多工器
多工器
拌碼輸出
選擇
選擇
假亂數
產生器
(PRNG)
606
解答值

第 6 圖


712
716
解答載入
解答時鐘
電源
700
解答進入
706
702
解答移位暫存器
初始/執行
714
MLS時鐘
708
704
極大長度序列(MLS)移位暫存器
710

第 7 圖