

(21)申請案號：100120444

(22)申請日：中華民國 100 (2011) 年 06 月 10 日

(51)Int. Cl. : G06F21/24 (2006.01)

H04L9/28 (2006.01)

(30)優先權：2010/10/14 日本

2010-231745

(71)申請人：東芝股份有限公司 (日本) KABUSHIKI KAISHA TOSHIBA (JP)

日本

(72)發明人：長井裕士 NAGAI, YUJI (JP)；坂本廣幸 SAKAMOTO, HIROYUKI (JP)；中井弘人 NAKAI, HIROTO (JP)；宮田誠二 MIYATA, SEIJI (JP)；三村英紀 MIMURA, HIDEKI (JP)

(74)代理人：陳長文

申請實體審查：有 申請專利範圍項數：25 項 圖式數：18 共 64 頁

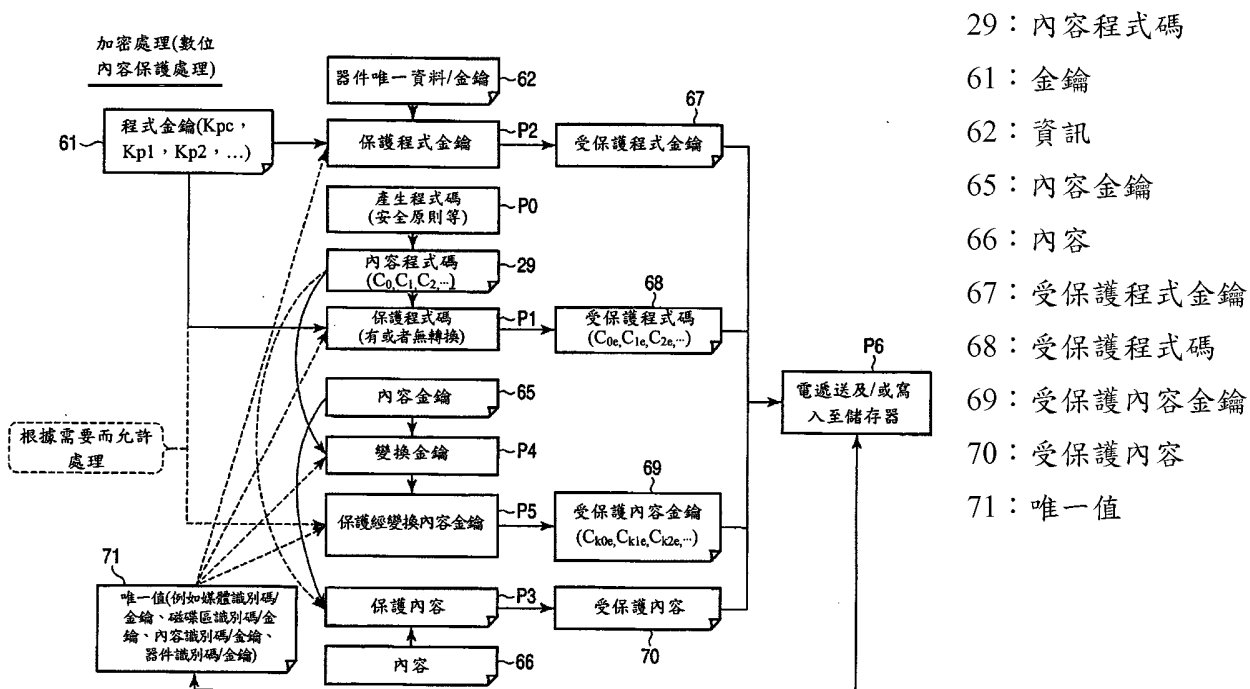
(54)名稱

數位內容之保護方法、解密方法、播放器、儲存媒體及加密裝置

PROTECTION METHOD, DECRYPTION METHOD, PLAYER, STORAGE MEDIUM, AND ENCRYPTION APPARATUS OF DIGITAL CONTENT

(57)摘要

一種數位內容保護方法包括連同一經加密內容散佈一經加密受保護程式金鑰、一受保護內容金鑰及包括一個別指令碼之一受保護程式碼，其中至少某些元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。



(21)申請案號：100120444

(22)申請日：中華民國 100 (2011) 年 06 月 10 日

(51)Int. Cl. : **G06F21/24 (2006.01)**

H04L9/28 (2006.01)

(30)優先權：2010/10/14 日本

2010-231745

(71)申請人：東芝股份有限公司(日本) KABUSHIKI KAISHA TOSHIBA (JP)

日本

(72)發明人：長井裕士 NAGAI, YUJI (JP)；坂本廣幸 SAKAMOTO, HIROYUKI (JP)；中井弘人 NAKAI, HIROTO (JP)；宮田誠二 MIYATA, SEIJI (JP)；三村英紀 MIMURA, HIDEKI (JP)

(74)代理人：陳長文

申請實體審查：有 申請專利範圍項數：25 項 圖式數：18 共 64 頁

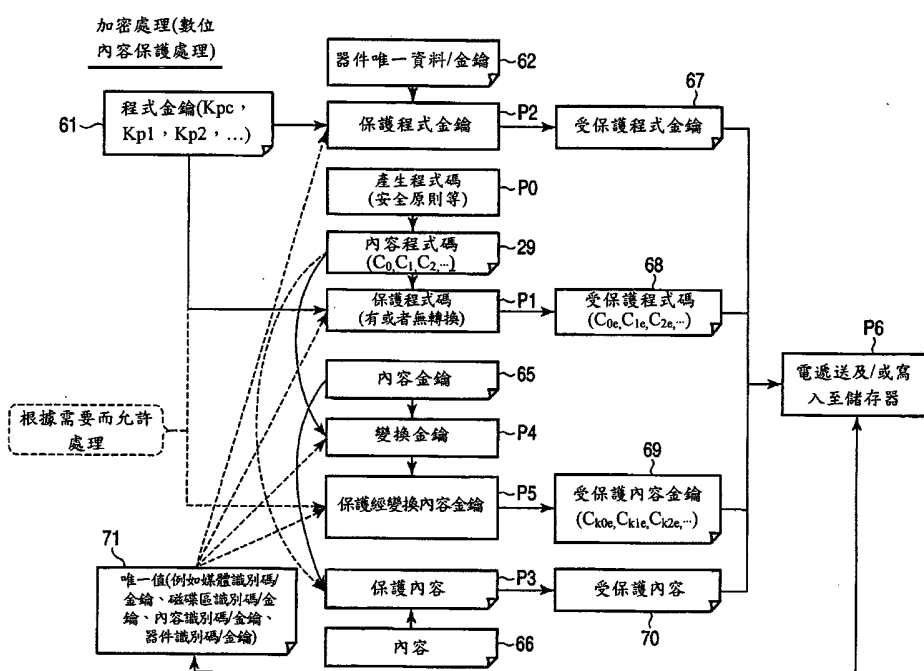
(54)名稱

數位內容之保護方法、解密方法、播放器、儲存媒體及加密裝置

PROTECTION METHOD, DECRYPTION METHOD, PLAYER, STORAGE MEDIUM, AND
ENCRYPTION APPARATUS OF DIGITAL CONTENT

(57)摘要

一種數位內容保護方法包括連同一經加密內容散佈一經加密受保護程式金鑰、一受保護內容金鑰及包括一個別指令碼之一受保護程式碼，其中至少某些元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。



29：內容程式碼

61：金鑰

62：資訊

65：內容金鑰

66：內容

67：受保護程式金鑰

68：受保護程式碼

69：受保護內容金鑰

70：受保護内容

71: 唯一值

六、發明說明：

【發明所屬之技術領域】

本發明係關於數位內容之保護方法、解密方法、播放器、儲存媒體及加密裝置。

【先前技術】

一著作權保護系統指定一種散佈通常作為呈一經加密格式之一受著作權保護作品之一內容之方法。因用於加密一內容之一加密金鑰係秘密資訊，故藉由(例如)使用另一加密金鑰加密該加密金鑰本身來進行非法複製保護。

【發明內容】

根據一實施例，一種數位內容保護方法包含：藉由加密包括一個別指令碼之一內容程式碼來產生一受保護程式碼；藉由加密一程式金鑰來產生一受保護程式金鑰；藉由用一內容金鑰加密一內容來產生一受保護內容；藉由加密該內容金鑰來產生一受保護內容金鑰；及連同該受保護內容散佈該受保護程式金鑰、該受保護內容金鑰及該受保護程式碼，其中該個別指令碼之至少一個元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而指定。

【實施方式】

作為著作權保護系統，已知由具體公司指定之專有規格及由包括複數個公司之一協會指定之實際標準規格。至於著作權保護系統之管理，已知其中(例如)一加密金鑰設定為秘密資訊但一系統向公眾開放之一情況及其中著作權保

護系統本身亦設定為秘密資訊之一情況。不論是哪樣情況，為了製造與任意著作權保護系統相容之播放器，必須自著作權保護系統管理組織獲得例如加密金鑰之秘密資訊及內容解密規格。播放器係根據內容解密規格而設計及製造，且在併入呈不容易被曝露之形式之加密金鑰時銷售。

然而，近年來，加密金鑰係自播放器之內部或經由其他途徑獲取，且用於對內容之非法複製。舉例而言，作為DVD(位數多功能光碟)中之著作權保護系統之CSS(內容置亂系統)之移除軟體及作為藍光光碟中之著作權保護系統之AACs(進階存取內容系統)之移除軟體用於使用非法獲取之加密金鑰來非法獲取並散佈內容。

出於這個理由，作為著作權保護系統中之額外內容非法使用措施，使用以下技術。亦即，連同內容提供執行內容安全原則及解密處理所需之資料處理/計算程式(下文中稱作內容程式碼)。作為播放器規格，指定處理內容程式碼之一虛擬機器，以便指定通常一致指定於著作權保護系統中之播放器相依安全處理之至少一些處理程序作為不可更新系統。

然而，甚至當應用額外內容保護時，一旦一程式碼執行環境以及一內容程式碼及虛擬機器之結構自一易受攻擊的器件曝露，則藉由更新內容保護處理獲得之安全效果在所有環境下消失。另一方面，當在不指定任何虛擬機器結構的情況下採用所有唯一個別規格時，必須在完全辨別該裝置之處理環境之後創建一內容程式碼，從而導致不佳產能

及相容性。

下文將參照圖式來闡述一實施例。應注意，在此說明中貫穿各圖式，共同元件符號表示共同部分。

[比較實例]

為了與稍後將闡述之一實施例比較，下文將使用圖1、圖2及圖3來闡述一比較實例。

<AACCS系統之內容保護>

圖1展示用於(例如)唯讀藍光光碟之一AACCS內容保護序列。

如圖1中所示，自一著作權保護管理組織給一光碟製造商100提供(例如)使用基於用於內容加密之媒體金鑰、媒體金鑰(Km)及KCD(金鑰轉換資料)之一器件金鑰群組產生之一MKB(媒體金鑰區塊)。光碟製造商100自一內容著作權所有人接收(例如)一內容與標題金鑰(Kt)，並使用Kt作為一加密金鑰來加密該內容。而且，藉由自該等媒體金鑰及一磁碟區識別碼藉由AES-G處理產生之一磁碟區唯一金鑰來加密Kt，從而產生包括經加密Kt之一標題金鑰檔案。應注意，AES-G處理係基於AES加密之單向函式處理。磁碟區識別碼係由光碟製造商100或內容著作權所有人產生之一標題磁碟區唯一值。

在一媒體200之指定位置處，記錄由光碟製造商100獲取或處理/產生之「MKB」、「KCD」、「磁碟區識別碼」、「標題金鑰」及「經加密內容」。之後，媒體200連同所儲存資料供應給市場。應注意，媒體200不僅限於碟形光碟，而

是可係一任意實體儲存媒體，例如SD(安全數位)卡。

一播放器300執行基於自媒體200讀出之所記錄資料之解密處理，並播放該內容。在播放器300中，自著作權保護管理組織提供之器件金鑰係以難以被曝露及偽造之形式保存。播放器300自媒體200讀出MKB，並使用器件金鑰來執行MKB處理(處理MKB)，藉此導出媒體金鑰。在這種情況下，根據由播放器300保存之器件金鑰之類型，作為MKB處理之結果導出不同值。在AACs中，播放器分為兩種類別：一種類別稱作「增強穩健性器件」，且另一種類別稱作「預動再生器件(Proactive Renewal Device)」。增強穩健性器件指示其中例如器件金鑰之秘密資料受(例如)硬體安全保護之一播放器。預動再生器件指示由在例如PC之開放平台上運行之軟體表示，且具有定期更新器件金鑰之要求而不是對器件金鑰之基於硬體之保護之一播放器。在增強穩健性器件之情況下，藉由對由MKB處理導出之值應用KCD及AES-G處理來導出媒體金鑰。在預動再生器件之情況下，使用由MKB處理導出之值本身作為媒體金鑰。藉由對使用磁碟區識別碼以此方式導出之媒體金鑰應用AES-G處理，導出一磁碟區唯一金鑰。藉由該磁碟區唯一金鑰解密來解密該標題金鑰檔案中之一標題金鑰，且隨後藉由該標題金鑰來解密該內容。

如由上述說明可見，作為加密及解密之一基礎之器件金鑰係非常重要的秘密資訊。因此，在一器件金鑰洩漏之情況下，對MKB應用允許使器件金鑰失效之一結構。MKB

係由經加密媒體金鑰組態而成，該等經加密金鑰係藉由分別藉由複數個器件金鑰來加密複數個媒體金鑰複製資料而獲得。若某一器件金鑰洩漏，且用於非法複製一內容，則可藉由自MKB移除由所洩漏器件金鑰加密之一媒體金鑰來防止使用所洩漏器件金鑰來解密該內容。此稱作一器件金鑰之失效或撤銷。然而，此失效資訊可應用至僅新近製造之媒體，但其無法應用至先前製造及出售之媒體。

<藉由MKB結構之金鑰失效>

下文將使用圖2來闡述使用MKB之金鑰失效。用於AACs之MKB具有稱作「NNL樹」之樹結構，且器件金鑰(Kd1、Kd2、Kd3...)存在於各別分葉上。媒體金鑰(Km)分別藉由對應於該等分葉之器件金鑰加密，且指派給MKB之對應分葉。基於此結構，諸如對應於該等分葉之經加密器件金鑰及分葉器件金鑰之節點編號之若干則資訊儲存於一MKB檔案中。若欲使對應於分葉2之一器件金鑰失效，則可把對應於彼分葉之經加密媒體金鑰排除在MKB之外。

<藉由SKB結構之金鑰失效>

圖3展示另一MKB結構(SKB(序列金鑰區塊)結構)。在上面的圖2中，基於一相同媒體金鑰之資料指派給所有分葉。然而，在圖3中所示之SKB結構中，稱作媒體金鑰變體(Kmv)之不同媒體金鑰指派給各別分葉。此結構用於一使用目的，例如針對相異後續加密處理所需之各別器件所獲取之媒體金鑰之個別化。在AACs系統中，複製一內容之一部分，且各別複製內容使用基於不同媒體金鑰變體之

金鑰加密以相異各別器件之可播放內容。因此，此結構用於在一器件金鑰洩漏之後指定一器件。

以此方式，在AACCS系統中，當一器件金鑰洩漏時，採取用於指定器件金鑰之一手段及用於使器件金鑰失效之一手段。然而，當出現一易受攻擊的播放器或途徑時，複數個器件金鑰可經由複數個播放器及其他途徑洩漏，且對內容之非法複製可在彼器件失效的情況下使用其他器件繼續。

[第一實施例]

下文將使用圖4、5、6、7、8、9、10、11、12、13、14、15、16、17A、17B及18來闡述根據第一實施例之數位內容之保護方法、解密方法、播放器、儲存媒體及加密裝置。在下文說明中，將不給出與該比較實例中之部分重複之部分之詳細說明。

<0.前置條件(SPDC系統)>

作為前置條件，將首先闡述一種基於SPDC(自保護數位內容)系統之內容保護技術。SPDC系統係一種改變並更新該內容保護系統本身作為一內容非法使用措施以補充上述金鑰失效之技術。舉例而言，根據SPDC技術，作為一儲存媒體，藉由連同經加密內容提供執行內容安全原則及解密處理所需之資料處理及計算程式(下文中稱作內容程式碼)，可提供可更新播放器相依安全處理之系統。在SPDC中，內容保護處理之一部分由在一播放器中之一虛擬機器上執行之內容程式碼實施。在這種情況下，虛擬機器通常

係指界定將諸如電腦之CPU及儲存器件之資源虛擬化之電腦，且必須執行虛擬電腦之架構。

虛擬機器接收介於硬體相依機器語言與進階程式設計語言(例如C)之間的中間語言，並藉由虛擬機器中之解譯器將中間語言解譯成機器語言，從而允許具有不同機器語言格式之CPU及儲存器件執行同一程式。虛擬機器包括虛擬處理器及虛擬記憶體，且提供(例如)對播放器中之資源及光碟中之資源之存取功能以及對算術計算及加密計算之執行。

<1.配置實例>

1-1.播放器

下文將使用圖4來闡述一根據此實施例採用使用虛擬機器之SPDC技術之播放器。

如圖4中所示，根據此實施例之播放器包括由一由圖4中之一虛線指示之播放器邊界10分割，且由處理器12、解譯器17及執行與資料RAM 18組態而成之一虛擬機器30。稍後將闡述虛擬機器30之細節。

處理器12讀出(例如)由為播放器所獨有之環境/設定資訊組態而成之播放環境組態資料(Playback Environ. Config.) 11，並控制整體播放器之操作。

舉例而言，播放處理程序由可經由一媒體介面15存取一儲存媒體25之處理器12控制。當安裝儲存媒體25時，處理器12開始初始化處理程序並讀出儲存媒體之內容表。

解譯器17係基於自一中間語言至一機器語言之一解譯方

法安裝。解譯器17包括指令表19，該等指令表包括共同指令表及個別指令表。稍後將闡述指令表19之細節。

執行與資料RAM 18能夠儲存一內容程式碼29及經由媒體介面15自儲存媒體25讀出之經加密內容。解譯器17使用在安裝儲存媒體25時載入RAM 18及指令表19之內容程式碼29來執行預定處理。

一批量(BULK)解密模組13自處理器12接收(例如)對自儲存媒體25讀出之經加密內容及加密金鑰資訊之一真實解密金鑰及參數之指定。批量解密模組13自RAM 18或作為選擇直接自媒體介面15擷取經加密內容並解密經加密內容。

密碼編譯oracle 14賦予處理器12由密碼編譯oracle本身保存或允許印在一可拆卸式外部安全卡24中之一內容鑑別此播放器係一真實器件之一憑證之一辨識項、自媒體25讀出之例如加密金鑰之資訊或密碼編譯oracle 14對例如加密金鑰之資訊之處理結果。安全卡(SIM)24係(例如)一智慧卡。

媒體介面15自儲存媒體25讀出一內容程式碼29及經加密內容，並將其載入虛擬機器30中之RAM 18。以此方式，儲存媒體(媒體)25記錄根據每一內容之一安全原則描述之內容程式碼29。

一輸出介面16將由處理器12或批量解密模組13處理之一內容供應至意欲演現、記錄或播放該內容之一目的地程式/器件26。

虛擬機器30依序讀出內容程式碼29中所述之指令，將其解譯成一機器語言之指令以執行此等指令。在這種情況

下，虛擬機器30具有(例如)一存取環境/設定為播放器所獨有之資訊之功能、一存取記錄於播放器中之RAM 18或外部媒體(例如SIM卡24)中之與加密處理相關聯之資訊及函式之功能、及一執行對一解密處理模組之控制及處理之功能。使用此等功能所需之指令說明規則係預先定義的，且對虛擬機器30之實施及對內容程式碼29之說明係根據定義進行。

對於上述配置，到現在為止係一致之內容保護處理可擴展為內容程式碼29對各別內容之保護處理程序。舉例而言，不同於DVD之CSS，可藉由可擴展保護處理來避免其中一內容保護結構被完全曝露且所有對策皆無法採取之一情形。因此，除可改變內容保護處理本身之特徵以外，還可根據播放器之環境來執行處理程序。舉例而言，向自其洩漏一金鑰之一播放器提供額外處理。此外，可藉由將不同浮水印附加至各別播放器來個別化一內容。

然而，即使基於SPDC系統之內容保護技術亦往往在虛擬機器30之結構被曝露時無任何對策可採取。曝露虛擬機器30之結構意謂允許一非法使用者建立其中可執行描述內容保護處理之內容程式碼29之一環境，而且允許彼使用者解譯、掌握並執行內容程式碼29之處理內容。此外，至於根據一播放器之處理，可實施可避免此之一手段及一播放器環境之一假回應。亦即，在基於使用虛擬機器30之一程式之內容保護處理中，虛擬機器30之結構之保密非常重要。

如上文所述，就內容保護而言，在以與SPDC系統同樣的方式引入可更新內容保護處理之後，虛擬機器30之結構之保密很重要。另一方面，就產能及相容性而言，內容與播放器之間的相容性必須得到保證，內容本身之格式、內容保護格式、內容程式碼格式、器件規格等係標準化的，且內容製作者及器件製造商必須共用該等規格。通常，此等標準化及標準規格係由一標準規格制定組織制定，且標準規格制定組織向內容製作者及器件製造商提供所需則資訊，包括規格及資料。此等則資訊(例如規格及資料)包括(例如)要求保密且作為一全秘密處置之資訊，例如上述金鑰資訊及虛擬機器結構。因此，在披露虛擬機器之技術規格之後，必須在作為披露源之標準規格制定組織與一披露目的地之間達成等於或超過金鑰資訊之此等則資訊之機密性。作為在非法使用者解譯虛擬機器結構時之線索之元素包括內容程式碼本身及安裝虛擬機器之一器件，且必須採取防止其內容被輕易曝露之一措施。

然而，甚至當採取上述措施時，亦無法否認曝露虛擬機器之結構及內容程式碼之可能性。至於需要同樣具有保密之金鑰資訊，採取洩漏時之失效手段，如上文所述。另一方面，至於虛擬機器30，往往不採取任何有效的失效手段。此乃因使用相同之虛擬機器規格來達成內容程式碼之相容性。當該等規格失效時，基於該等規格製造之所有播放器皆失效。

出於這個理由，當不必要地自某一易受攻擊的器件掌握

虛擬機器結構時，影響蔓延至採用同一虛擬機器結構之所有其他器件。不存在針對此的對策，且使用虛擬機器之內容保護系統本身失效。

因此，下文將更詳細地闡述一種有利於藉由針對各別器件或器件群組個別化模擬機之至少一些處理程序來增強內容保護並提高產能及相容性，從而防止來自一易受攻擊的器件之經解譯內容應用至其他器件之方法及配置。

1-2. 虛擬機器之配置實例

下文將使用圖5來闡述根據此實施例之虛擬機器30之內部結構之一實例。

如圖5中所示，虛擬機器30由一播放器10內部之硬體、軟體或其組合實施。

內容程式碼29經由(例如)該器件內部或外部之一儲存器或一通信器件供應至播放器10。內容程式碼29包括(例如)可由播放器10(虛擬機器30)解譯之一指令集(稍後將闡述)及由該指令集處理之資料。

一記憶體31保存內容程式碼29。在這種情況下，記憶體31可係揮發性記憶體或非揮發性記憶體。

一指令載入器32呼叫保存於記憶體31中之內容程式碼29之指令及資料。由指令載入器32呼叫之各別指令可具有可由一指令處理器完整解譯之格式或可在其由圖5中所示之一指令轉換器34轉換之後由一指令處理器35解譯之格式。

一暫存器33保存(例如)用於計算之值、作為計算結果之

值及欲在保存於記憶體31中之內容程式碼29中執行之接下來的指令之位址值(程式計數器)。暫存器33係自指令載入器32及一系統呼叫操作36(稍後將闡述)以及指令處理器35存取。應注意，此實施例將暫存器33描述為一獨立於記憶體31之模組。然而，實務中，記憶體31之一部分可用作一暫存器。

指令轉換器34用於混淆內容程式碼29及其執行環境，且具有一旦在載入指令之後隨即計算保存於暫存器33或記憶體31中之值及所載入指令之值以將該等指令轉換成可由指令處理器34解譯之一格式之功能。在這種情況下，其中保存用於該等計算之值之暫存器33或記憶體31之位址可係可預先設定或者可由包括於所載入指令中之值或保存於暫存器33或記憶體31之一預定區中之值指示之固定位址。一計算方法可係位元計算、算術計算及密碼編譯計算中之任一者。一或複數個值可用於該等計算。

指令處理器35接收由指令載入器32呼叫之指令或由指令轉換器34轉換之指令。指令處理器35使用指令表(運算碼函式)19將各別指令之運算碼解譯成執行函式。指令表19可係硬接線的，可記錄於一EEPROM(電可抹除可程式化唯讀記憶體)中，或者可作為資料記錄於虛擬機器30外部之一儲存區中。指令處理器35在執行基於運算碼之處理程序之後使用暫存器33作為一儲存區。

由密碼編譯功能、使用控制功能、媒體存取功能及包括於虛擬機器30中之其他模組存取功能或由圖4中所示之播

播放器邊界指示之播放器10基於各別指令使用系統呼叫操作36。此等功能係在指令處理器35發出呼叫包括於虛擬機器30中之各別功能所需之系統呼叫時使用。與執行系統呼叫操作36相關聯之輸入/輸出交換處理程序使用上述暫存器33及記憶體31。

一密碼編譯模組41可包括(例如)用於由播放器單獨保存之密碼編譯計算以及基於一加密機之計算(例如加密、解密、隨機數產生、單向函式及簽章處理)之唯一資訊、加密金鑰、解密金鑰、簽章金鑰及證書。密碼編譯模組41可係不包括上述計算或唯一資訊中之任一者，而使用虛擬機器30之外部功能(例如圖4中之批量解碼模組13或密碼編譯oracle 14)之一介面。

一使用控制件42可包括與內容使用相關聯之控制程式，例如按播放開始時序、停止時序或信號輸出時序給一顯示器或其他外部器件指派複製控制資訊、由Macrovision代表之類比複製保護資訊及由HDCP(高頻寬數位內容保護系統)或DTCP(數位傳輸內容保護)代表之數位複製保護資訊。使用控制件42可係自身不包括上述控制資訊或控制功能，而使用虛擬機器30之外部功能(例如圖4中之目的地程式/器件26)之一介面。

一媒體介面43係記錄一內容及與該內容相關聯之資訊之一媒體之一存取介面。該媒體可係可抽換式媒體、播放器之內部媒體或外部器件上之媒體。媒體介面43可係自身不包括上述存取功能，而使用虛擬機器30之外部功能(例如

圖4中之媒體介面15及儲存媒體25)之一介面。

一模組介面44包括不同於上文所述之功能模組，例如，內容解碼器、器件內部時鐘、網路介面、USB介面、行動電話之SIM卡及信用卡。模組介面44指示播放器之內部功能模組或可經由播放器之介面使用之外部器件之功能模組。

1-3.指令集

下文將使用圖6來闡述根據圖5中所示之此實施例之一指令集39。

圖6展示根據此實施例之指令集39之一實例。指令集39包括指示對應於系統呼叫操作36之指令字以及記憶體31及暫存器33之資料載入指令、算術操作指令(例如加法、減法、乘法及除法)、位元計算指令(例如「與」/「或」/「互斥或」/移位)之運算碼(0x01、0x02、0x03等)。指示系統呼叫操作36之一運算碼與儲存於暫存器33或記憶體31上之一具體區中或包括於一指令中之一自變數或針對每一系統呼叫操作指定，且儲存於由該自變數指示之暫存器33或記憶體中之一位址處之一程式碼集一起使用。

1-4.指令格式

下文將使用圖7來闡述根據此實施例之一指令格式之一實例。

如圖7中所示，在該指令格式中，各別指令包括指示(例如)「RS1」、「RS2」、「SA」、「即時運算」、「函式」及「PC位移」之資料連同上述運算碼。

(a)展示32位元I型。(a)中之「RS1」係指儲存用於一運算中之一變數之暫存器33或記憶體33之一位址。「RD」係指儲存一運算結果之一值之暫存器33或記憶體31之一位址。此係使用用於(例如)一DLX處理器之一格式之一實例。「即時運算」係不儲存一儲存於暫存器33中之值但儲存一用於一運算中之即時運算值(直接指定變數)之一區。

(b)展示32位元R型。(b)中之「RS2」同樣係指儲存用於一運算中之一變數之暫存器33或記憶體31之一位址。「RD」係儲存一運算結果之一值之暫存器33或記憶體31之一位址。「SA」係用於一任意目的之一備用區。「函式」係根據需要針對一額外輸入/輸出之一指定或使用為每一運算碼指定之一經擴展函式區或另一經擴展函式。

(c)展示32位元J型。「PC位移」係用於保存與一指令序列之正常順序執行相反在跳至一具體指令之後使用之一程式計數器之一位址之一區。該程式計數器之該位址可係絕對位址或相對位址。

內容程式碼29係由(例如)包括上述系統呼叫操作36之指令集39及供該指令集處理並使用之資料組態而成。以此方式，藉由經由系統呼叫操作36實施基於各別播放器功能及其返回值之使用之進一步計算處理程序及條件分支處理程序以及使用內容程式碼29之資料計算，可實施進階及混淆安全處理。

如上文所述，當所有器件皆採用一相同虛擬機器結構時，若自某一易受攻擊的播放器掌握該虛擬機器結構，則

影響往往蔓延至採用該類似虛擬機器結構之所有其他播放器。另一方面，當不指定一虛擬機器，且所有播放器皆具有唯一規格時，內容程式碼必須在完全掌握播放器處理環境之後產生，且產能及相容性往往劣化。

因此，下文將更詳細地闡述可防止產能及相容性劣化同時藉由個別化虛擬機器30之結構來增強內容保護之方法及配置。

1-5.指令表

下文將使用圖8來闡述應用至該方法及配置之根據此實施例之指令表之實例。

圖8展示具有不同於指令集中之運算碼之函式指派之函式指派之(a)一共同指令表19-0及(b)個別指令表(指令表#1至#3)19-1至19-3之實例。

(a)中之共同指令表19-0係一為各別播放器所共有之指令表。以此方式，當各別播放器使用共同指令表19-0作為一共同內容程式碼時，有利於減小資訊磁碟區並提高產能及相容性。

(b)中之個別指令表(指令表#1至#3)19-1至19-3係其中針對各別播放器或播放器群組個別化指示運算碼與指令集之函式之間的指派關係之一指令表之至少一些元素之指令表。播放器群組係指(例如)屬於某一模型名稱之一播放器群組或屬於某一製造商名稱之一播放器群組。

舉例而言，表#1使用由 $X(i)$ 、 $X(i+1)$ 、 $X(i+2)$ 、...指示之一序列作為運算碼。表#2使用由 $Y(i)$ 、 $Y(i+1)$ 、 $Y(i+2)$ 、...

指示之一序列作為運算碼。表#3使用由 $Z(i)$ 、 $Z(i+1)$ 、 $Z(i+2)$ 、...指示之一序列作為運算碼。在這種情況下， X 、 Y 及 Z 序列係不同的資料指示符序列。以此方式，藉由針對各別播放器或各別播放器群組應用不同個別化指令表19-1至19-3，甚至當安裝(例如)表#1之一播放器遭受攻擊，且表#1之內容被曝露時，影響不蔓延至使用其他表#2及#3之播放器群組，從而提供增強內容保護之一優點。

如上文所述，在根據此實施例之指令表19中，為了藉由個別指令表(指令表#1至#3)19-1至19-3來個別化虛擬機器30，內容程式碼必須針對各別虛擬機器30製備且必須與一內容一起散佈及記錄。然而，因共同指令表19-0提供一共同內容程式碼，故減小資訊磁碟區。

因此，各自具有虛擬機器30之各別播放器儲存表，如圖9中所示。該等表儲存於(例如)每一播放器中之一ROM(唯讀記憶體)中。

(a)中所示之播放器A將共同指令表19-0及個別指令表(指令表#1)19-1儲存於其ROM中。

(b)中所示之播放器B將共同指令表19-0及個別指令表(指令表#2)19-2儲存於其ROM中。

(c)中所示之播放器C將共同指令表19-0及個別指令表(指令表#3)19-3儲存於其ROM中。

應注意本發明不僅限於此具體實例，且可根據需要進一步儲存個別指令表(指令表#4、#5、...)。舉例而言，可根

據需要針對各別內容播放器群組儲存不同個別指令表(例如，一第一群組{播放器A、播放器B}：個別指令表19-1；一第二群組{播放器C}：個別指令表19-2)。

<2.內容程式碼產生方法>

下文將使用圖10、11、12、13、14及15來闡述根據此實施例之內容程式碼29之一產生方法。該內容程式碼產生方法由光碟製造商100則上之一專用寫入裝置(加密裝置)執行。

編譯器基於指派給每一播放器或播放器群組之共同指令表19-0及個別指令表(指令表#n)19-n將每一原始程式碼轉換成內容程式碼(C0至C#n)。基於共同指令表19-0編譯之一內容程式碼(共同程式碼：C0)將在下文中稱作一共同內容程式碼，基於個別指令表(指令表#n)19-n編譯之一內容程式碼將在下文中稱作一個別內容程式碼(程式碼#n)。

該原始程式碼描述根據一內容之一安全原則由一播放器執行之一處理序列。每一編譯器亦在將一原始程式碼轉換成一內容程式碼之後針對上述指令轉換器34中之處理執行轉換處理。經產生內容程式碼29經歷根據需要補充簽章處理之處理，例如為散佈及記錄所需之加密及封裝。在這種情況下，需要簽章處理來防止由一非法使用者創建之內容程式碼29被執行，且播放器在執行內容程式碼29之前驗證一簽章，從而確定內容程式碼29是否係一非法內容程式碼或該內容程式碼是否係偽造的。因此，播放器可防止一內容程式碼而不是一真實內容程式碼被執行。在這種情況

下，簽章處理可藉由下述方法來實施：使用一私密金鑰來產生一簽章並基於一公開金鑰密碼系統（例如 RSA 及 ECDSA）來驗證其使用一公開金鑰之方法以及使用一私密金鑰來產生一訊息鑑別程式碼（MAC）並基於一對稱金鑰密碼系統（例如 AES（進階加密標準）來驗證該 MAC 使用同一私密金鑰之一方法。後一種私密金鑰可使用針對每一內容程式碼 29 製備之程式金鑰（稍後將闡述）。

2-1. 共同程式碼產生之實例（在不發生駭客攻擊時）

圖 10 展示當控制所有播放器以執行共同處理，且使用共同指令表 19-0 來編譯一原始程式碼時之一實例。此情況對應於（例如）其中所有播放器中皆不發生駭客攻擊，且因此，控制所有播放器以使用僅共同指令表 19-0 根據一共同安全原則來執行處理之一情況。

如圖 10 中所示，一對應編譯器（有指令轉換）134-0 基於共同指令表 19-0 將一原始程式碼（原始程式碼 0）轉換成一共同內容程式碼（共同程式碼（C0））64-0。

隨後，一後處理單元 135 將共同內容程式碼（共同程式碼（C0））64-0 處理成一受保護程式碼 68 以將用於程式碼保護之金鑰 61 作為私密金鑰。應注意，用於程式碼保護之金鑰 61 係包括程式金鑰（稍後將闡述）或根據需要一簽章金鑰之程式金鑰之金鑰。

2-2. 個別程式碼產生之實例（在共同指令表已被駭客攻擊時）

圖 11 展示其中控制所有播放器以執行共同處理但針對各

別播放器使用不同的個別指令表(指令表#n)來編譯一原始程式碼之一實例。舉例而言，此情況對應於其中共同指令表19-0已被駭客攻擊，且控制所有播放器以根據一共同安全原則來執行處理之一情況。

如圖11中所示，例如，當共同指令表19-0已被駭客攻擊時，不產生上述情況2-1中之共同內容程式碼64-0，但開始使用個別指令表(指令表#n)來編譯一原始程式碼。

亦即，對應個別編譯器(有指令轉換)134-1至134-4基於個別指令表(指令表#1至#4)19-1至19-4將一共同原始程式碼轉換成個別內容程式碼(程式碼#1至#4)64-1至64-4。

隨後，後處理單元135同樣使用用於程式碼保護之金鑰61作為私密金鑰將個別內容程式碼(程式碼#1至#4)64-1至64-4處理成受保護程式碼68。

2-3.具體程式碼產生之實例

圖12展示其中控制一具體播放器(在這種情況下，對應於指令表#4之一播放器)以執行不同的處理，且針對各別播放器使用不同的指令表來編譯一原始程式碼之一實例。舉例而言，此處理係在懷疑執行基於指令表#4之處理之一播放器駭客攻擊，且可針對僅彼播放器執行經由系統呼叫操作36之駭客攻擊狀態檢查、基於檢查結果之金鑰導出處理之選擇/停止、內容播放控制等時使用。

亦即，一對應於個別編譯器(有指令轉換)134-4基於個別指令表(指令表#4)19-4將原始程式碼2轉換成一個別內容程式碼(程式碼#4)64-4。

隨後，後處理單元135同樣使用用於程式碼保護之金鑰61將個別內容程式碼(程式碼#4)64-4處理成一受保護程式碼68。

2-4.當在處理原始程式碼1之後處理原始程式碼2時

圖13展示其中控制所有播放器以執行共同處理從而使用共同指令表19-0來編譯原始程式碼1，並隨後針對各別播放器使用不同個別指令表(指令表#1至#4)來編譯原始程式碼2(亦即，組合兩個內容程式碼)之一實例。舉例而言，此情況對應於其中在程式碼產生時未駭客攻擊共同指令表19-0，但在將來會發生駭客攻擊之假定下針對各別播放器使用不同指令表19-1至19-4編譯之程式碼中包括至少一些處理程序之一情況。在這種情況下，僅由於駭客攻擊共同指令表19-0，辨別整體處理變得困難。舉例而言，此對應於其中包括在執行原始程式碼1之後執行原始程式碼2之一分支指令之一情況。

亦即，如在上述情況下，對應編譯器(有指令轉換)134-0基於共同指令表19-0將原始程式碼1轉換成共同內容程式碼(共同程式碼(C0))64-0。隨後，後處理單元135使用用於程式碼保護之金鑰作為私密金鑰將共同內容程式碼(共同程式碼(C0))64-0處理成一受保護程式碼68。

然後，個別編譯器(有指令轉換)134-1至134-4基於個別指令表(指令表#1至#4)19-1至19-4將原始程式碼2轉換成個別內容程式碼(程式碼#1至#4)64-1至64-4。隨後，後處理單元135同樣使用用於程式碼保護之金鑰作為私密金鑰將

個別內容程式碼(程式碼#1至#4)64-1至64-4轉換成受保護程式碼68。

2-5.當在共同處理之後針對每一播放器執行個別處理時

圖14不同於圖13中所示之情況2-4，因為各別播放器執行不同處理程序(原始程式碼1至4)。作為此執行之結果，因原始程式碼對於各別播放器不同，故將作為駭客攻擊一具體播放器之結果所曝露之處理內容應用至其他播放器變得困難。

亦即，如在上述情況下，對應編譯器(有指令轉換)134-0基於共同指令表19-0將原始程式碼1轉換成共同內容程式碼(共同程式碼(C0))64-0。隨後，後處理單元135使用用於程式碼保護之金鑰作為私密金鑰將共同內容程式碼(共同程式碼(C0))64-0處理成一受保護程式碼68。

然後，對應個別編譯器(有指令轉換)134-1至134-4基於個別指令表(指令表#1至#4)19-1至19-4將原始程式碼1至4(原始程式碼2至4)轉換成個別內容程式碼(程式碼#1至#4)64-1至64-4。隨後，後處理單元135同樣使用用於程式碼保護之金鑰作為私密金鑰將個別內容程式碼(程式碼#1至#4)64-1至64-4處理成受保護程式碼68。

2-6.關於程式金鑰

下文將使用圖15來闡述程式金鑰61。

如圖15中所示，程式金鑰 K_{p0} 、 K_{p1} 、 K_{p2} 、 K_{p3} 、 K_{p4} 、...(61-0至61-4)用作內容程式碼64-0至64-4之密碼。

在這種情況下，程式金鑰61-0至61-4可係用於產生上述

訊息鑑別程式碼之私密金鑰。此外，程式金鑰61-0至61-4可彼此不同，至少一個金鑰可相同，或所有金鑰可相同。當使用不同程式金鑰時，甚至當一程式金鑰自一易受攻擊的播放器曝露且彼播放器之一個別內容程式碼被解密時，因其他播放器之個別內容程式碼無法被解密，故內容程式碼及處理內容程式碼之虛擬機器之保密不受影響。在這種情況下，程式金鑰合意地基於為一器件所獨有之一金鑰或資料受到保護。稍後將闡述細節。

<3.加密處理(數位內容保護處理)>

3-1.

下文將使用圖16來闡述根據此實施例之加密處理(數位內容保護處理)。下文將闡述之加密處理係由在媒體上寫入一內容之提供者100則上之一專用寫入裝置(加密裝置)執行，且包括圖10、11、12、13及14中所示之處理程序中之任一者。

如圖16中所示，根據此實施例之加密處理使用為一器件所獨有之資訊之一金鑰來加密用於保護內容程式碼29之程式金鑰及一內容金鑰以及其他處理程序。最後，受保護金鑰67、受保護程式碼68、受保護內容金鑰69及受保護內容70以電遞送或記錄其之實體媒體之形式作為已經歷保護處理之一資料群組散佈至播放器。

(步驟P0(產生程式碼(安全原則等)))

基於一基於一案例原則及內容保護方法所述之原始程式碼，作為一內容程式碼產生器之編譯器134以與圖10、

11、12、13及14中所述之內容程式碼產生方法同樣的方式產生一內容程式碼(C0、C1、C2、...)29。如圖10、11、12、13及14之變化形式中所述，可使用一或複數個原始程式碼。此外，可針對每一原始程式碼產生一個內容程式碼或者可在使用不同指令表編譯的同時產生複數個內容程式碼。

(步驟P1(保護程式碼(有或無轉換)))

經產生內容程式碼29經歷由作為一內容程式碼保護器之後處理單元135提供之保護處理且處理為一受保護程式碼(C0e、C1e、C2e、...)68。在這種情況下，使用程式金鑰61，如上所述。應注意，程式金鑰61藉由該保護處理與基於器件唯一值之資訊62相關聯，且對應於該關聯播放器之一內容程式碼之一程式金鑰61用於保護每一個別內容程式碼。如由一虛線所指示，諸如媒體識別碼/金鑰、磁碟區識別碼/金鑰、內容識別碼/金鑰及器件識別碼/金鑰之唯一值71可用於該保護處理。而且，可執行對應於由上述指令轉換器34提供之處理之混淆。受保護內容程式碼68以電遞送或記錄該內容之實體媒體形式作為一經加密內容散佈至播放器，如步驟P6中所示。

(步驟P2(保護程式金鑰))

用於加密內容程式碼之程式金鑰(Kpc、Kp1、Kp2、...)經歷使用(例如)基於器件唯一值之資訊62之保護處理。在這種情況下，基於器件唯一值之資訊62可直接使用器件唯一值以及使用器件唯一值導出之間接資訊。作為相關資訊

之一實例，可使用對應於基於器件唯一值之每一資訊62之一媒體金鑰群組。

作為一可行實例，上述SKB中之媒體金鑰變體係間接資訊，且處理SKB及導出媒體金鑰變體所需之器件金鑰對應於(例如)器件唯一資訊。此外，間接資訊可使用諸如媒體識別碼/金鑰、磁碟區識別碼/金鑰、內容識別碼/金鑰及器件識別碼/金鑰之唯一值71來導出，如由圖16中之一虛線所指示。已經歷保護處理之受保護程式金鑰67以電遞送或記錄該內容之實體媒體之形式作為一經加密內容散佈至播放器，如步驟P6中所示。

(步驟P3(保護內容))

一內容66經歷使用一內容金鑰65之保護處理，且處理為一受保護內容70。

在這種情況下，可對使用內容程式碼29之一內容之至少一部分應用額外處理。額外處理可包括(例如)資料轉換、加密及替換處理程序。受保護內容70以電遞送或記錄該內容之實體媒體之形式作為一經加密內容散佈至播放器，如步驟P6中所示。

(步驟P4(變換金鑰))

用於加密內容之內容金鑰65根據包括於內容程式碼29中之一金鑰變換方法變換，且變換為一經變換內容金鑰。在這種情況下，可同樣使用唯一值71來執行額外處理。

(步驟P5(保護經變換內容金鑰))

隨後，經變換內容金鑰經歷保護處理，且處理為受保護

內容金鑰(Ck0e、Ck1e、Ck2e、...)69。在這種情況下，諸如媒體識別碼/金鑰、磁碟區識別碼/金鑰、內容識別碼/金鑰及器件識別碼/金鑰之唯一值71可用於金鑰變換處理及保護處理。在這種情況下，步驟P4中之金鑰變換處理與步驟P5中之保護處理之次序可顛倒，且金鑰變換處理可在保護處理之後執行。此外，可採用不同於一系列處理連接(亦即，一個處理包括另一個處理)之一結構。受保護內容金鑰69以電遞送或記錄其之實體媒體之形式散佈至播放器，如步驟P6中所示。

3-2.儲存於實體儲存媒體中之格式

作為加密處理之步驟P6之結果，作為一經加密內容儲存於一實體儲存媒體中之受保護程式金鑰67等展示於(例如)圖17A及圖17B中。

在圖17A中所示之實例中，一儲存媒體儲存已經歷保護處理之受保護程式金鑰67、受保護程式碼(C0e、C1e、C2e、...)68、受保護內容金鑰(Ck0e、Ck1e、Ck2e、...)69及受保護內容70作為經加密內容。此儲存媒體散佈至播放器。

更特定而言，圖17B中所示之實例展示一SD卡®之一實例。該SD卡包括一記憶體控制器76及一非揮發性半導體記憶體之一NAND快閃記憶體77。記憶體控制器76控制NAND快閃記憶體77之整體操作。

NAND快閃記憶體77儲存已經歷保護處理之受保護程式金鑰67、受保護程式碼(C0e、C1e、C2e、...)68、受保護

內容金鑰(Ck0e、Ck1e、Ck2e、...)69及受保護內容70。此SD卡同樣散佈至播放器作為經加密內容。

應注意，經加密內容可藉助(例如)下載(如步驟P6中所示)而不是儲存媒體經由一電通信線路以電遞送之形式散佈至播放器。

<4.解密處理>

下文將使用圖18來闡述根據此實施例之解密處理。根據此實施例之解密處理執行與大體上使用圖16所述之加密處理相反之處理，且係由針對消費者銷售之一播放器(在播放器300側上)執行之處理。

(步驟UP0(電遞送/或自儲存器讀取))

以經加密內容之電遞送或儲存該內容之一實體媒體之形式，已經歷保護處理之程式金鑰67、受保護程式碼68、受保護內容金鑰69及受保護內容70以及唯一值71散佈至播放器。唯一值71包括(例如)媒體識別碼/金鑰、磁碟區識別碼/金鑰、內容識別碼/金鑰及器件識別碼/金鑰。唯一值71藉由相同或不同手段提供至播放器。

(步驟UP1(撤銷保護程式金鑰))

受保護程式金鑰67使用基於器件唯一值之資訊62解密為程式金鑰(Kp0、Kp#n)61。如上所述，在這種情況下，解密處理使用基於器件唯一值之資訊62。

在這種情況下，基於器件唯一值之資訊62可直接使用器件唯一值，或者可使用使用器件唯一值導出之間接資訊。作為相關資訊之一實例，可使用對應於基於器件唯一值之

每一資訊62之一媒體金鑰群組。作為一可行實例，上述SKB中之媒體金鑰變體係間接資訊，且處理SKB及導出媒體金鑰變體所需之器件金鑰對應於(例如)器件唯一資訊。此外，間接資訊可使用諸如媒體識別碼/金鑰、磁碟區識別碼/金鑰、內容識別碼/金鑰及器件識別碼/金鑰之唯一值71來導出。經解密程式金鑰(Kp0、Kp#n)61用於隨後的解密處理。

(步驟UP2(選擇並撤銷保護程式碼))

受保護內容程式碼(C0e、C1e、C2e、...)68由播放器之一內容程式碼選擇/解密單元解密為內容程式碼(C0、C#n)64。在這種情況下，選擇處理使用附加至程式金鑰61或器件唯一金鑰71及資料之內容程式碼選擇編號、預先確定之選擇編號或藉由另一手段提供之選擇編號。解密處理使用程式金鑰61。另一選擇係，選擇可解密處理可使用諸如媒體識別碼/金鑰、磁碟區識別碼/金鑰、內容識別碼/金鑰及器件識別碼/金鑰之唯一值71。

(步驟UP3(選擇並撤銷保護金鑰))

受保護內容金鑰(Ck0e、Ck1e、Ck2e、...)69由播放器之一內容金鑰選擇/解密單元解密，且傳遞至步驟UP4。

(步驟UP4(執行程式碼(變換金鑰等)))

隨後，內容程式碼(C0、C#n)64使用(例如)由播放器之虛擬機器30提供之程式金鑰61及經變換金鑰等來解密內容金鑰65。當受保護內容70之至少一些處理程序已經歷由內容程式碼29提供之額外處理時，亦在此步驟中執行此等處

理程序之解密處理。

(步驟UP5(撤銷保護內容))

受保護內容70使用內容金鑰65解密為內容66。

(步驟UP6(播放控制(演現等)))

經解密內容66經歷根據需要基於由播放器之虛擬機器30執行之一程式碼(執行程式碼)之播放控制。

<5.效果>

根據第一實施例之一位數內容之保護方法，解密方法、播放器儲存媒體及加密裝置，獲得至少下面的效果(1)及(2)。

(1)此實施例有利於增強保密。

如(例如)圖16中所示，根據第一實施例之一數位內容之保護處理(一位數內容之加密處理)連同受保護內容70散佈至少經加密受保護程式金鑰67、受保護內容金鑰(Ck0e、Ck1e、Ck2e、...)69及包括一個別指令碼(C1e、C2e、...)之受保護程式碼68，其中至少一些元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

以此方式，因包括個別指令碼(C1e、C2e、...)，其中至少一些元素係針對各別內容播放器或內容播放器群組個別化，例如，甚至當使用一個別指令碼(C1e)之一播放器遭受攻擊，且個別指令碼(C1e)之內容被曝露時，故使用另一個別指令碼(C2e)之一播放器群組不受影響，從而防止(例如)對一數位內容之非法複製。以此方式，數位內容保

護可得到增強，且此實施例有利於增強保密。

(2)此實施例可減小一資訊磁碟區，且有助於防止產能及相容性之劣化。

另外，受保護程式碼68進一步包括為各別內容播放器共有之一共同指令碼(C0e)。

因包括為各別內容播放器所共有之共同指令碼(C0e)，故可減小一共同部分之資訊磁碟區，且此實施例有利於提高產能及相容性。

(3)關於數位內容之解密方法、播放器、儲存媒體及加密裝置

一數位內容之上述解密方法(例如，圖18等)、播放器(例如，圖4及圖5等)、儲存媒體(例如，圖17等)及加密裝置(例如，圖1及圖10等)同樣具有效果(1)及(2)。

舉例而言，播放受根據第一實施例之數位內容保護方法保護之一內容之一播放器由虛擬機器30之處理器(指令處理器)35使用圖8中所示之指令表19執行。

圖8之(a)中所示之共同指令表19-0係為各別播放器所共有之一指令表。

圖8之(b)中所示之個別指令表(指令表#1至#3)19-1至19-3係藉由針對各別播放器或播放器群組個別化指示運算碼與指令集之函式之間的指派關係之一指令表獲得之指令表。

舉例而言，表#1使用由 $X(i)$ 、 $X(i+1)$ 、 $X(i+2)$ 、...指示之一序列作為運算碼。表#2使用由 $Y(i)$ 、 $Y(i+1)$ 、 $Y(i+2)$ 、...指示之一序列作為運算碼。表#3使用由 $Z(i)$ 、 $Z(i+1)$ 、

$Z(i+2)$ 、...指示之一序列作為運算碼。

因此，各自具有虛擬機器30之各別播放器儲存表，如圖9中所示。

(a)中所示之播放器A將共同指令表19-0及個別指令表(指令表#1)19-1儲存於其ROM中。

(b)中所示之播放器B將共同指令表19-0及個別指令表(指令表#2)19-2儲存於其ROM中。

(c)中所示之播放器C將共同指令表19-0及個別指令表(指令表#3)19-3儲存於其ROM中。

另外，如圖10、11、12、13及14中所示，各種情況可有利地根據需要應用至一內容程式碼之產生。

[包括於此實施例中之態樣]

上述比較實例及實施例包括以下態樣。

(1)一數位內容保護方法包含連同經加密內容散佈經加密受保護程式金鑰、受保護內容金鑰及包括一個別指令碼之受保護程式碼，其中至少一些元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

(2)在(1)中所述之數位內容保護方法中，受保護程式碼進一步包括根據為各別內容播放器所共有之一共同運算碼規格設計之一共同指令碼。

(3)在(1)或(2)中所述之數位內容保護方法中，個別指令碼係由不可能由根據不同唯一運算碼規格設計之內容播放器或內容播放器群組導出之一程式金鑰予以加密。

(4)在(3)中所述之數位內容保護方法中，程式金鑰係由使用內容播放器之唯一資訊導出之一金鑰予以加密。

(5)在(2)至(4)中所述之數位內容保護方法中，共同指令碼係由允許由一任意內容播放器群組導出之一程式金鑰予以加密。

(6)在(1)或(2)中所述之數位內容保護方法中，個別指令碼及共同指令碼係基於包括至少助憶程式碼及運算碼之個別指令表及一共同指令表而編譯。

(7)在(1)或(2)中所述之數位內容保護方法中，允許共同指令碼由任意內容處理裝置執行，但不允許個別指令碼由根據不同唯一運算碼規格指定之內容處理裝置或內容處理裝置群組執行。

熟習此項技術者易於想出本發明之額外優點及修改。因此，本發明之寬廣態樣並非侷限於本文所示及所述之具有細節及典型實施例。因此，在不脫離隨附申請專利範圍及其等效內容所定義的一般發明概念之精神與範疇之前提下，可對本發明做各種修改。

【圖式簡單說明】

圖1係展示根據一比較實例之一AACCS內容保護序列之一圖表；

圖2係用於解釋基於根據該比較實例之一MKB之金鑰失效之一視圖；

圖3係用於解釋基於根據該比較實例之一SKB之金鑰失效之一視圖；

圖4係展示基於使用根據第一實施例之一虛擬機器之一SPDC技術之一播放器之一方塊圖；

圖5係展示根據第一實施例之虛擬機器之結構之一實例之一方塊圖；

圖6展示根據第一實施例之一指令集；

圖7展示根據第一實施例之一指令格式；

圖8展示根據第一實施例之指令表；

圖9展示儲存根據第一實施例之指令表之播放器之實例；

圖10係展示根據第一實施例之一內容程式碼之一產生方法之一圖表；

圖11係展示根據第一實施例之一內容程式碼之一產生方法之一圖表；

圖12係展示根據第一實施例之一半導體儲存器件之一2行模式(2)之控制序列之一圖表；

圖13係展示根據第一實施例之一內容程式碼之一產生方法之一圖表；

圖14係展示根據第一實施例之一內容程式碼之一產生方法之一圖表；

圖15係用於解釋根據第一實施例之程式金鑰之一圖表；

圖16係用於解釋根據第一實施例之加密處理(數位內容保護處理)之一流程圖；

圖17A係展示在根據第一實施例之加密處理之後一儲存媒體之一實例之一視圖；

圖 17B 係展示在根據第一實施例之加密處理之後一儲存媒體之一實例之一視圖；及

圖 18 係用於解釋根據第一實施例之解密處理之一流程圖。

【主要元件符號說明】

10	播放器邊界
11	播放環境組態資料
12	處理器
13	批量解密模組
14	密碼編譯 oracle
15	媒體介面
16	輸出介面
17	解譯器
18	執行與資料隨機存取記憶體
19	指令表
19-0	指令表
19-1	指令表
19-2	指令表
19-3	指令表
19-4	指令表
24	安全卡
25	裝儲存媒體
26	目的地程式/器件
29	內容程式碼

30	虛 擬 機 器
31	記 憶 體
32	指 令 載 入 器
33	暫 存 器
34	指 令 處 理 器
35	指 令 處 理 器
36	系 統 呼 叫 操 作
39	指 令 集
41	密 碼 編 譯 模 組
42	使 用 控 制 件
43	媒 體 介 面
44	模 組 介 面
61	程 式 金 鑰
61-0	程 式 金 鑰
61-1	程 式 金 鑰
61-2	程 式 金 鑰
61-3	程 式 金 鑰
61-4	程 式 金 鑰
62	資 訊
64	內 容 程 式 碼
64-0	內 容 程 式 碼
64-1	內 容 程 式 碼
64-2	內 容 程 式 碼
64-3	內 容 程 式 碼

64-4	內容程式碼
65	內容金鑰
66	內容
67	受保護程式金鑰
68	受保護程式碼
68	受保護程式碼
69	受保護內容金鑰
70	受保護內容
71	唯一值
76	記憶體控制器
77	NAND快閃記憶體
100	光碟製造商
134-0	編譯器(有指令轉換)
134-1	編譯器(有指令轉換)
134-2	編譯器(有指令轉換)
134-3	編譯器(有指令轉換)
134-4	編譯器(有指令轉換)
135	後處理單元
200	媒體
300	播放器

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：100120444

※申請日：100.6.10

※IPC 分類：G01F 2/24 2006.01
H04L 9/58 2006.01

一、發明名稱：(中文/英文)

數位內容之保護方法、解密方法、播放器、儲存媒體及加密裝置

PROTECTION METHOD, DECRYPTION METHOD, PLAYER,
STORAGE MEDIUM, AND ENCRYPTION APPARATUS OF DIGITAL
CONTENT

二、中文發明摘要：

一種數位內容保護方法包括連同一經加密內容散佈一經加密受保護程式金鑰、一受保護內容金鑰及包括一個別指令碼之一受保護程式碼，其中至少某些元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

三、英文發明摘要：

A digital content protection method includes distributing, together with an encrypted content, an encrypted protected program key, a protected content key, and a protected code including an individual instruction code, at least some elements of which are designed according to a unique operation code specification for each content player or for each content player group.

七、申請專利範圍：

1. 一種數位內容保護方法，其包含：

藉由加密包括一個別指令碼之一內容程式碼來產生一受保護程式碼；

藉由加密一程式金鑰來產生一受保護程式金鑰；

藉由用一內容金鑰加密一內容來產生一受保護內容；

藉由加密該內容金鑰來產生一受保護內容金鑰；及

連同該受保護內容散佈該受保護程式金鑰、該受保護內容金鑰及該受保護程式碼，其中

該個別指令碼之至少一個元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

2. 如請求項1之方法，其中該內容程式碼進一步包括根據為各別內容播放器所共有之一共同運算碼規格設計之一共同指令碼。

3. 如請求項1之方法，其中藉由不可能由根據不同唯一運算碼規格設計之該內容播放器或該內容播放器群組導出之該程式金鑰加密該個別指令碼。

4. 如請求項3之方法，其中藉由使用該內容播放器之唯一資訊導出之一金鑰加密該程式金鑰。

5. 如請求項2之器件，其中藉由允許由一任意內容播放器群組導出之該程式金鑰加密該共同指令碼。

6. 一種數位內容解密方法，其包含：

連同受保護內容擷取一受保護程式金鑰、一受保護程

式碼及一受保護內容金鑰；

藉由解密該受保護程式金鑰來產生一程式金鑰；

藉由解密該受保護程式碼來產生包括一個別指令碼之一內容程式碼；

藉由解密該受保護內容金鑰來產生一內容金鑰；及

藉由用該內容金鑰解密該受保護內容來產生一內容，其中

該個別受保護程式碼之至少一個元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

7. 如請求項6之方法，其中該內容程式碼進一步包括根據為各別內容播放器所共有之一共同運算碼規格設計之一共同指令碼。

8. 如請求項6之方法，其中藉由允許由根據該唯一運算碼規格設計之該內容播放器或該內容播放器群組導出之該程式金鑰解密該個別指令碼。

9. 如請求項8之方法，其中藉由使用該內容播放器之唯一資訊導出之一金鑰解密該程式金鑰。

10. 如請求項7之方法，其中藉由允許由一任意內容播放器群組導出之該程式金鑰解密該共同指令碼。

11. 一種數位內容播放器，其包含：

一媒體介面，其經組態以連同一受保護內容擷取一受保護程式金鑰、一受保護內容金鑰及一受保護程式碼；

一解密模組，其經組態以

藉由解密該受保護程式金鑰來產生一程式金鑰，

藉由解密該受保護程式碼來產生包括一個別指令碼之一內容程式碼，

藉由解密該受保護內容金鑰來產生一內容金鑰，及

藉由用該內容金鑰解密該受保護內容來產生一內容；及

一處理器，其經組態以播放該內容，其中

該個別指令碼之至少一個元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

12. 如請求項11之播放器，其中該內容程式碼進一步包括根據為各別內容播放器所共有之一共同運算碼規格設計之一共同指令碼。

13. 如請求項11之播放器，其中該處理器藉由允許由根據該唯一運算碼規格設計之該內容播放器或該內容播放器群組導出之該程式金鑰來解密該個別指令碼。

14. 如請求項13之播放器，其中該處理器藉由使用該內容播放器之唯一資訊導出之一金鑰來解密該程式金鑰。

15. 如請求項12之播放器，其中該處理器藉由允許由一任意內容播放器群組導出之該程式金鑰來解密該共同指令碼。

16. 一種數位內容儲存媒體，其包含：

一受保護程式金鑰，其係藉由加密一程式金鑰而產生；

一受保護程式碼，其係藉由加密包括一個別指令碼之一內容程式碼而產生；

一受保護內容金鑰，其係藉由加密一內容金鑰而產生；及

一受保護內容，其係藉由用該內容金鑰加密一內容而產生，其中

該個別指令碼之至少一個元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

17. 如請求項16之媒體，其中該內容程式碼進一步包括根據為各別內容播放器所共有之一共同運算碼規格設計之一共同指令碼。

18. 如請求項16之媒體，其中該個別指令碼係藉由不可能由根據不同唯一運算碼規格設計之該內容播放器或該內容播放器群組導出之該程式金鑰予以加密。

19. 如請求項18之媒體，其中該程式金鑰係藉由使用該內容播放器之唯一資訊導出之一金鑰予以加密。

20. 如請求項17之媒體，其中該共同指令碼係藉由允許由一任意內容播放器群組導出之該程式金鑰予以加密。

21. 一種數位內容加密裝置，其包含：

一處理器，其經組態以

藉由加密包括一個別指令碼之一內容程式碼來產生一受保護程式碼，

藉由加密一程式金鑰來產生一受保護程式金鑰，

藉由用一內容金鑰加密一內容來產生一受保護內容，且

藉由加密該內容金鑰來產生一受保護內容金鑰；及
一寫入模組，其經組態以連同該受保護內容將該受保護程式金鑰、該受保護內容金鑰及該受保護程式碼寫入於一數位內容儲存媒體中，其中

該個別指令碼之至少一個元素係針對每一內容播放器或針對每一內容播放器群組根據一唯一運算碼規格而設計。

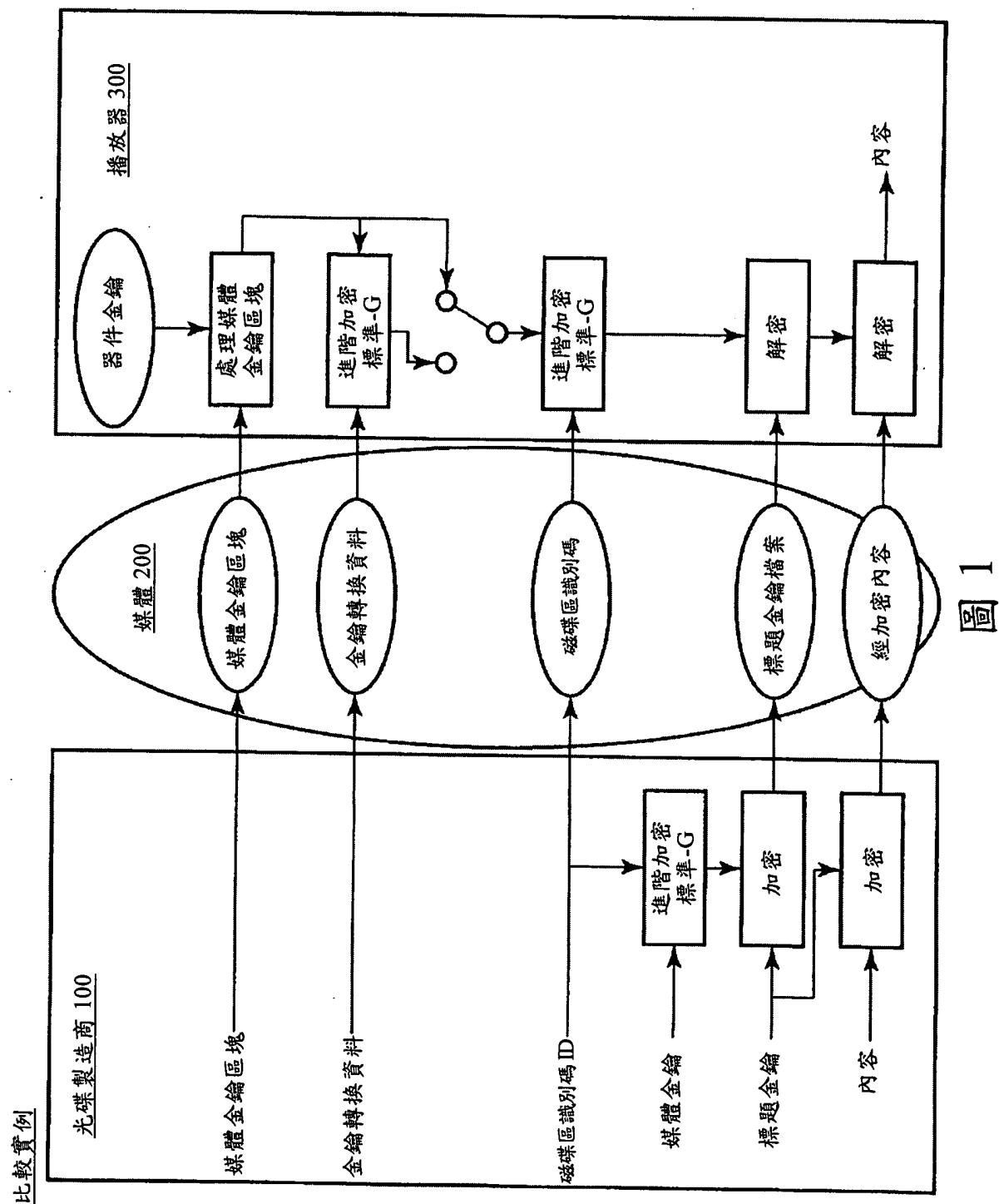
22. 如請求項21之裝置，其中該內容程式碼進一步包括根據為各別內容播放器所共有之一共同運算碼規格設計之一共同指令碼。

23. 如請求項21之裝置，其中該處理器藉由不可能由根據不同唯一運算碼規格設計之該內容播放器或該內容播放器群組導出之該程式金鑰來加密該個別指令碼。

24. 如請求項23之裝置，其中該處理器藉由使用該內容播放器之唯一資訊導出之一金鑰來加密該程式金鑰。

25. 如請求項22之裝置，其中該處理器藉由允許由一任意內容播放器群組導出之該程式金鑰來加密該共同指令碼。

八、圖式：



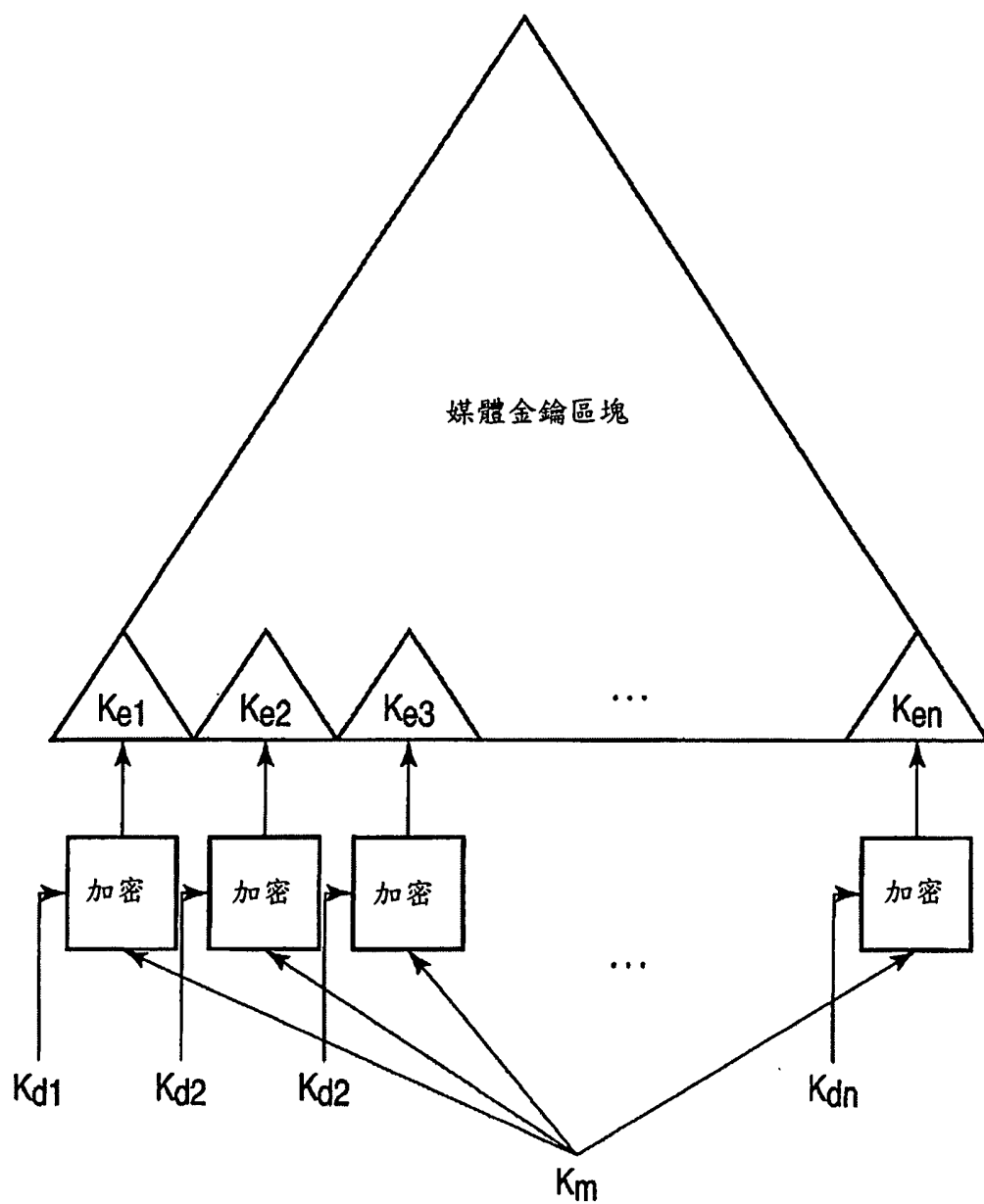


圖 2

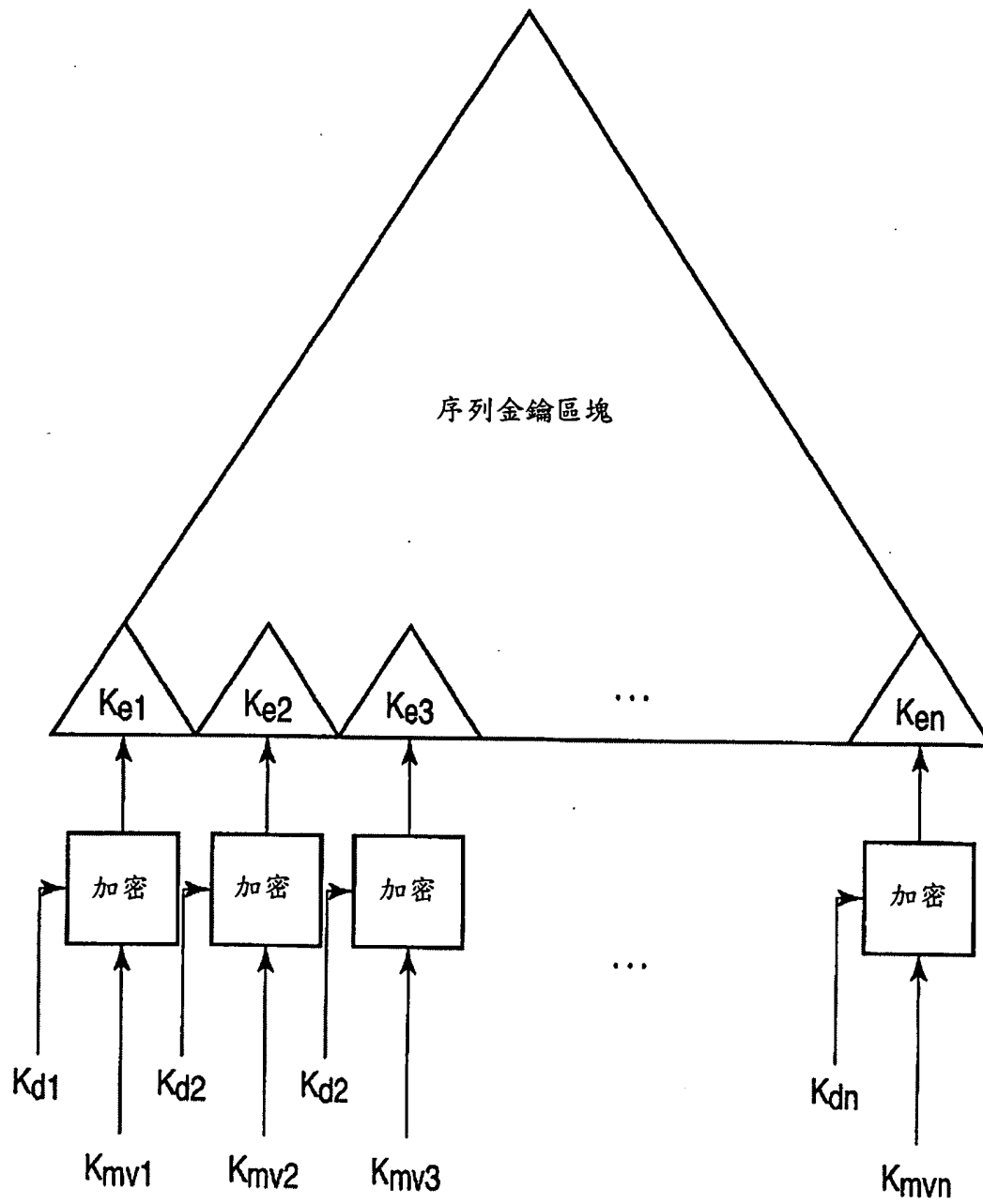


圖 3

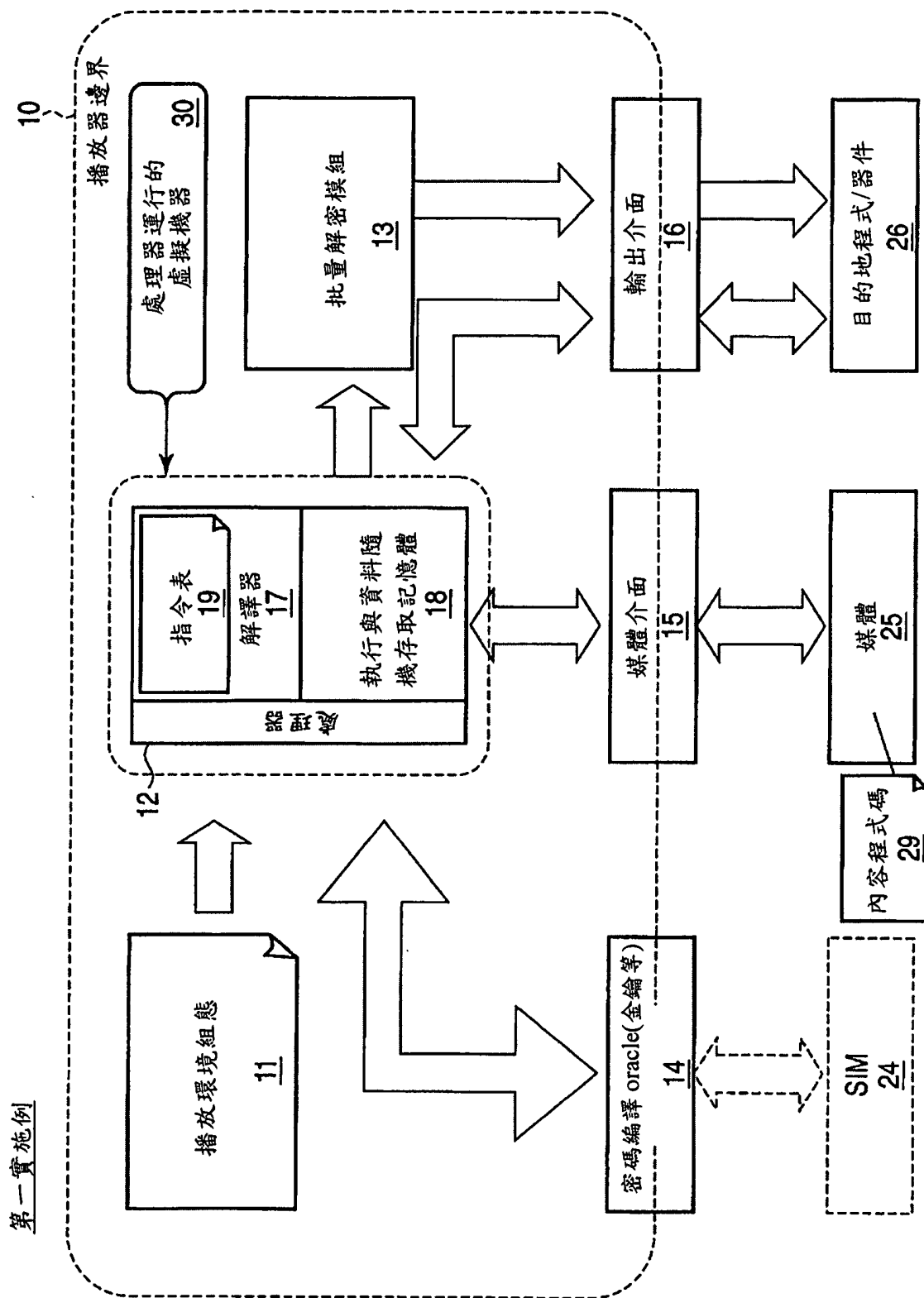


圖 4

虛擬機器 30

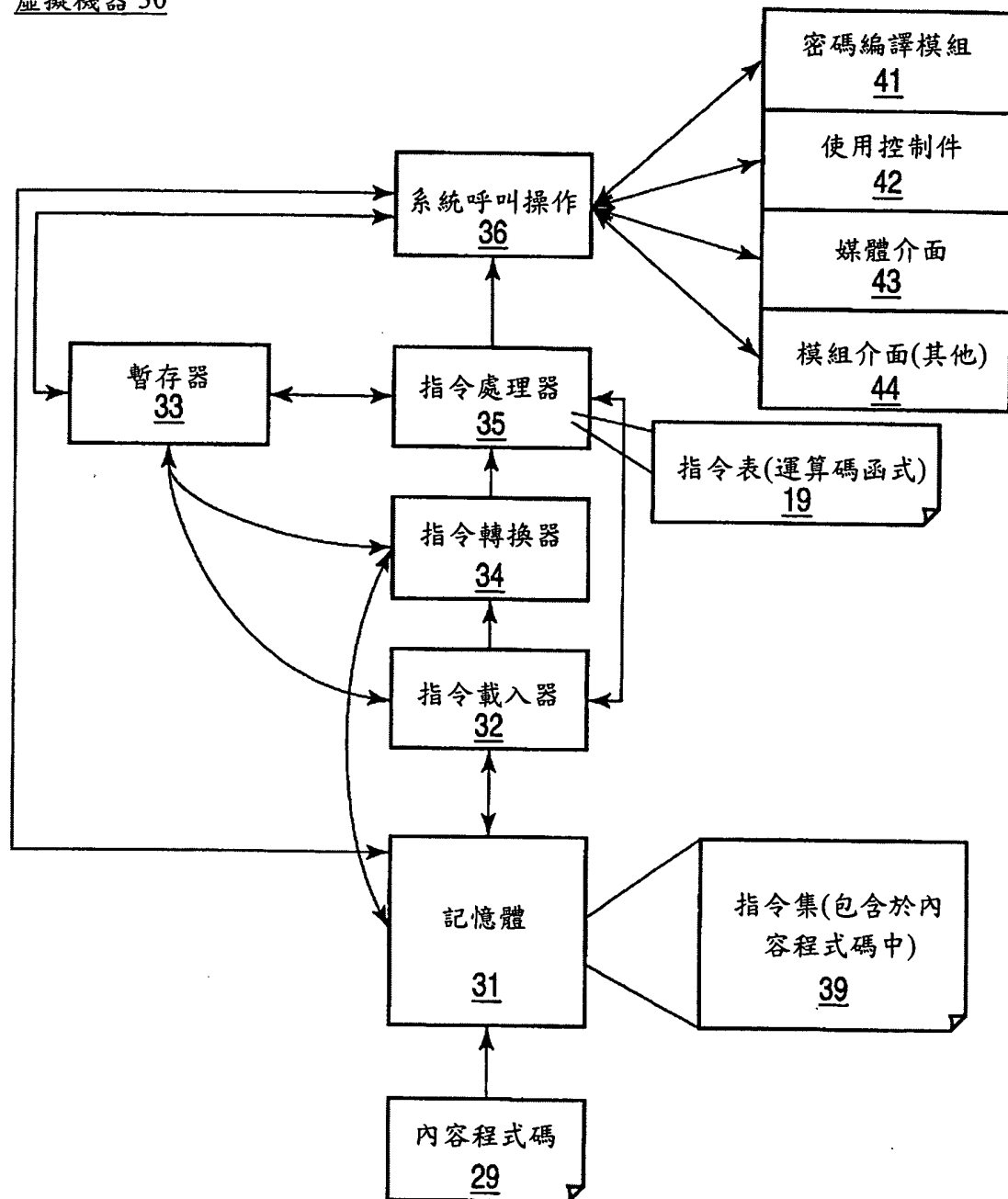
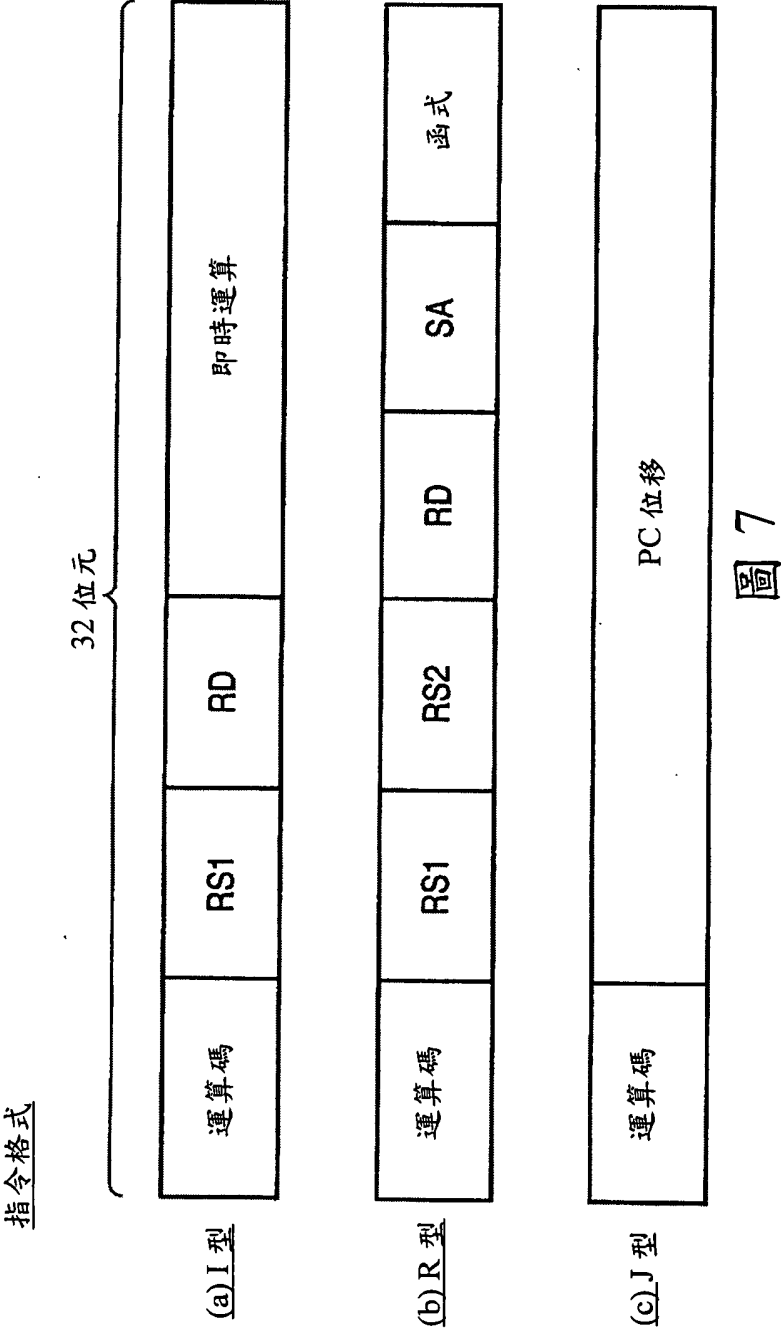


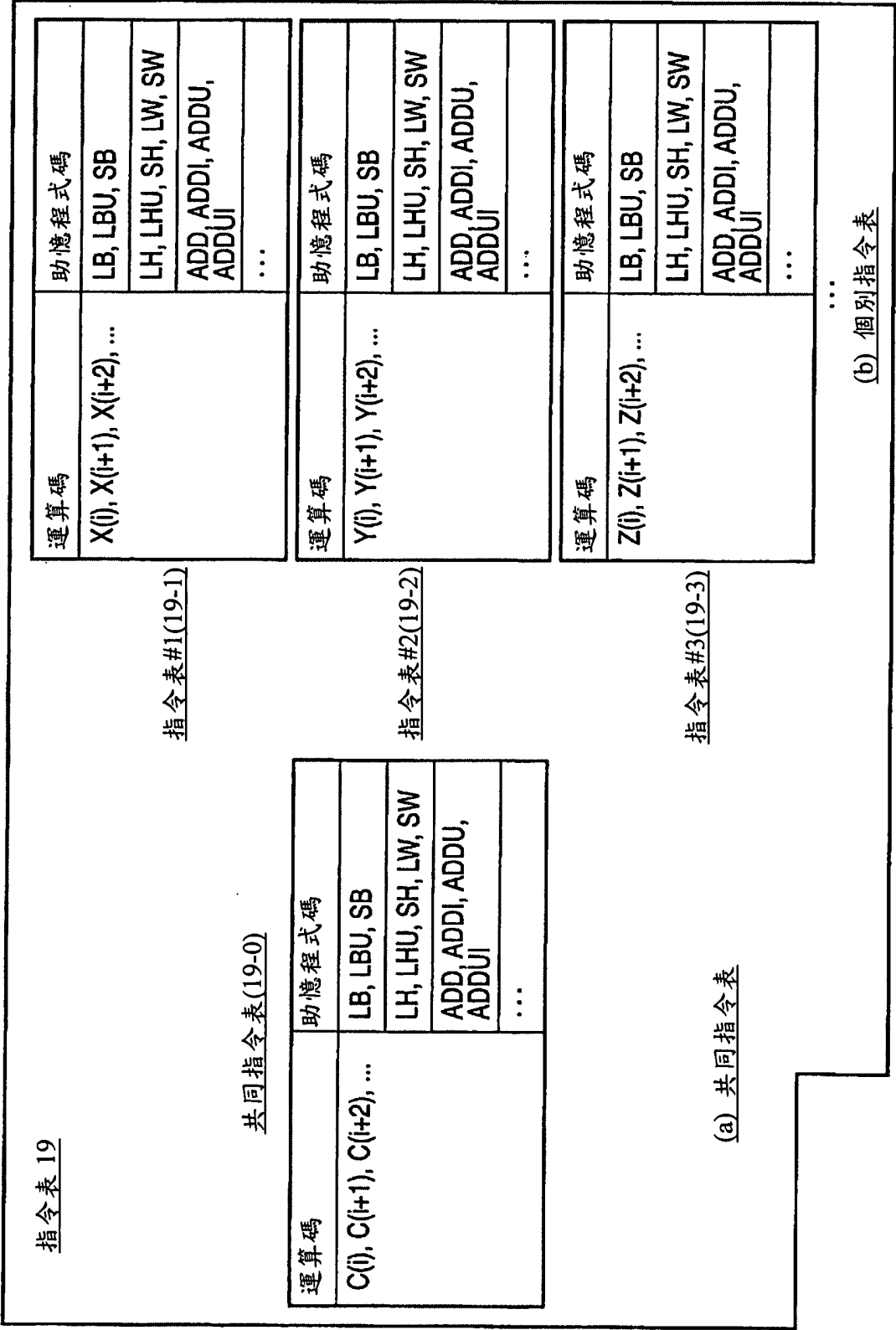
圖 5

指令集 39

運算碼	助憶程式碼	意義
0x01, 0x02, 0x03	LB, LBU, SB	載入位元組、載入不帶正負號位元組、儲存位元
0x04, 0x05, 0x06, 0x07, 0x08	LH, LHU, SH, LW, SW	載入半字組(帶正負號/不帶正負號)、儲存半字組、載入字組、儲存字組
0x09, 0x0A, 0x0B, 0x0C	ADD, ADDI, ADDU, ADDUI	加法、加法即時運算、加法(不帶正負號)、加法即時運算(不帶正負號)
0x0D, 0x0E, 0x0F, 0x10	SUB, SUBI, SUBU, SUBUI	減法、減法即時運算、減法(不帶正負號)、減法即時運算(不帶正負號)
0x11, 0x12, 0x13, 0x14	MULT, MULTU, MULTU, MULTUI	乘法、乘法即時運算、乘法(不帶正負號)、乘法即時運算(不帶正負號)
0x15, 0x16	AND, ANDI	「與」、「與」即時運算
0x17, 0x18	OR, ORI	「或」、「或」即時運算
0x19, 0x1A	XOR, XORI	「互斥或」、「互斥或」即時運算
0x1B, 0x1C	SLL, SLLI	逐位元左移位(變數/即時運算)
0x1D, 0x1E, 0x1F, 0x20	SRA, SRAI, SRL, SRLI	算術右移位(變數/即時運算) 逐位元右移位(變數/即時運算)
0x21, 0x22, 0x23, 0x24, 0x25, 0x26	SLT, SGT, SLE, SGE, SEQ, SNE	條件集
...	...	...
0x??	SYSCALL	系統呼叫
...	...	...

圖 6





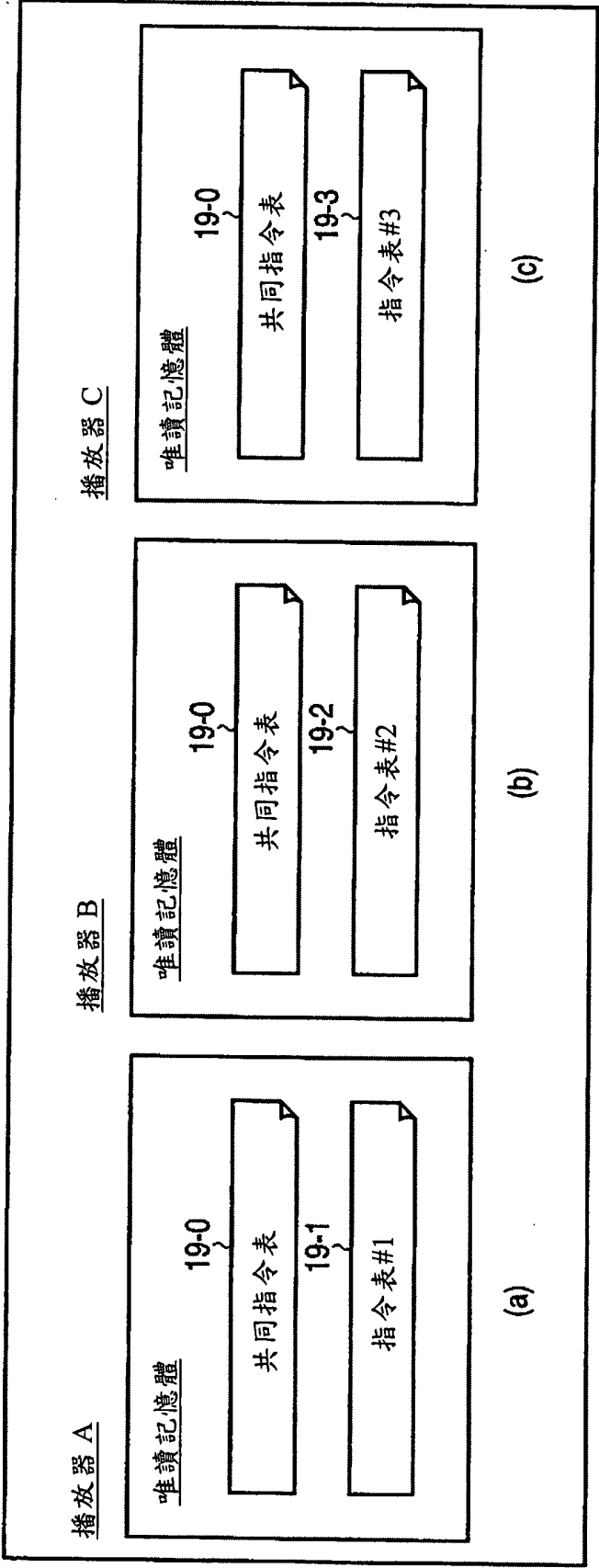
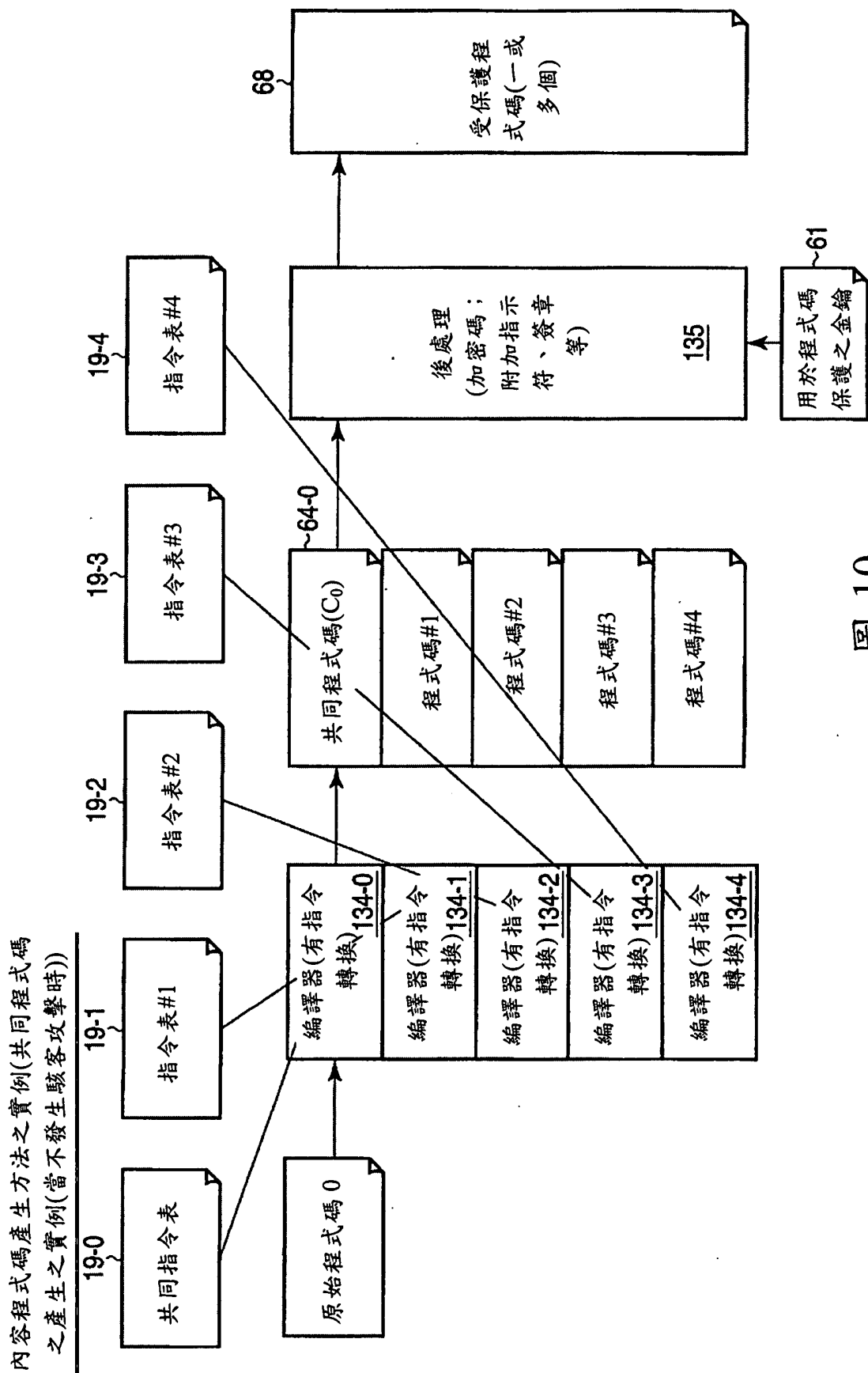


圖 9



內容程式碼#1 至#4 之產生方法之實例
(當共同指令表已被駭客攻擊時)

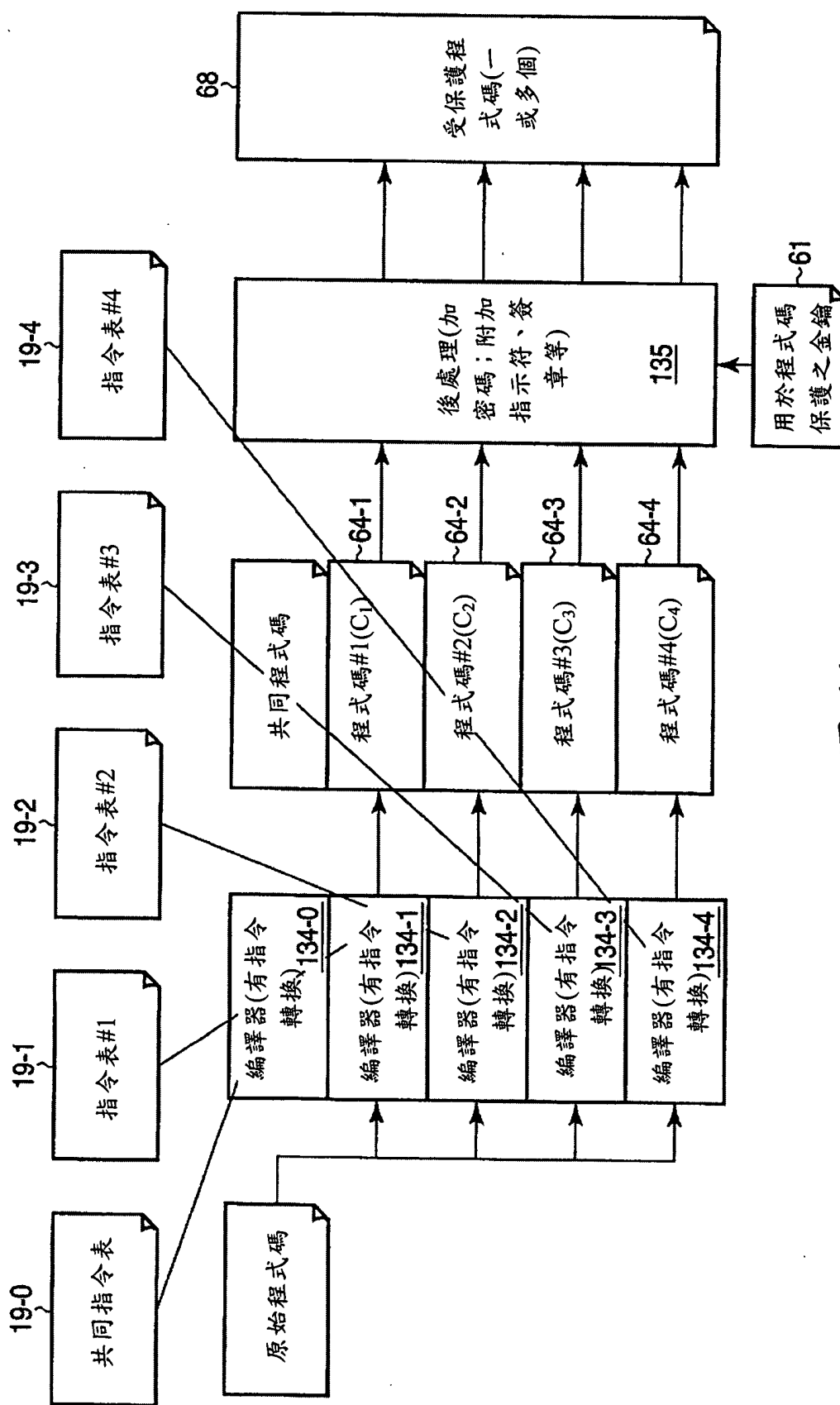


圖 11

當對應於指令表#4之播
放器已被駭客攻擊時

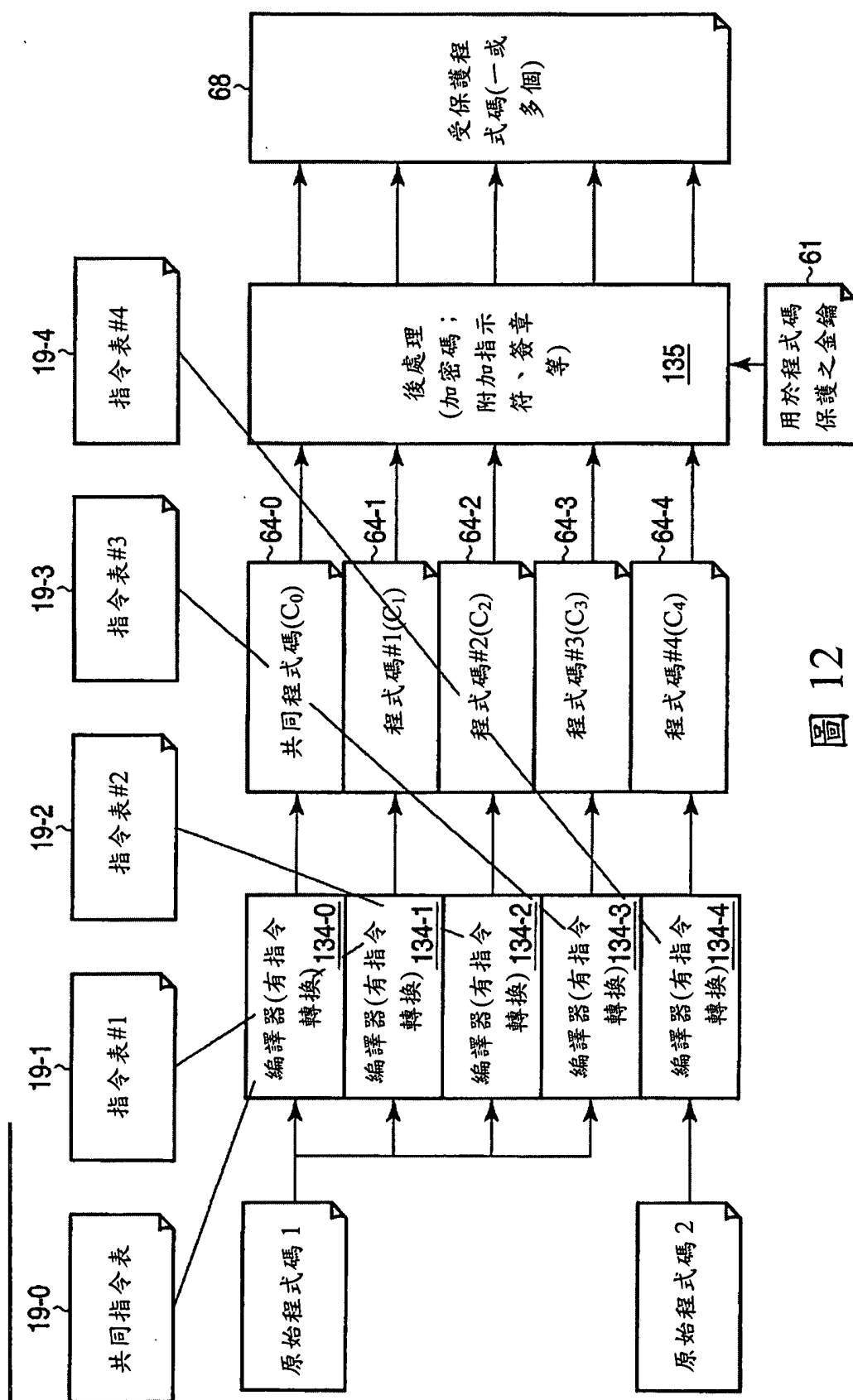


圖 12

當在處理原始程式碼 1 之後處理原始
程式碼 2 時

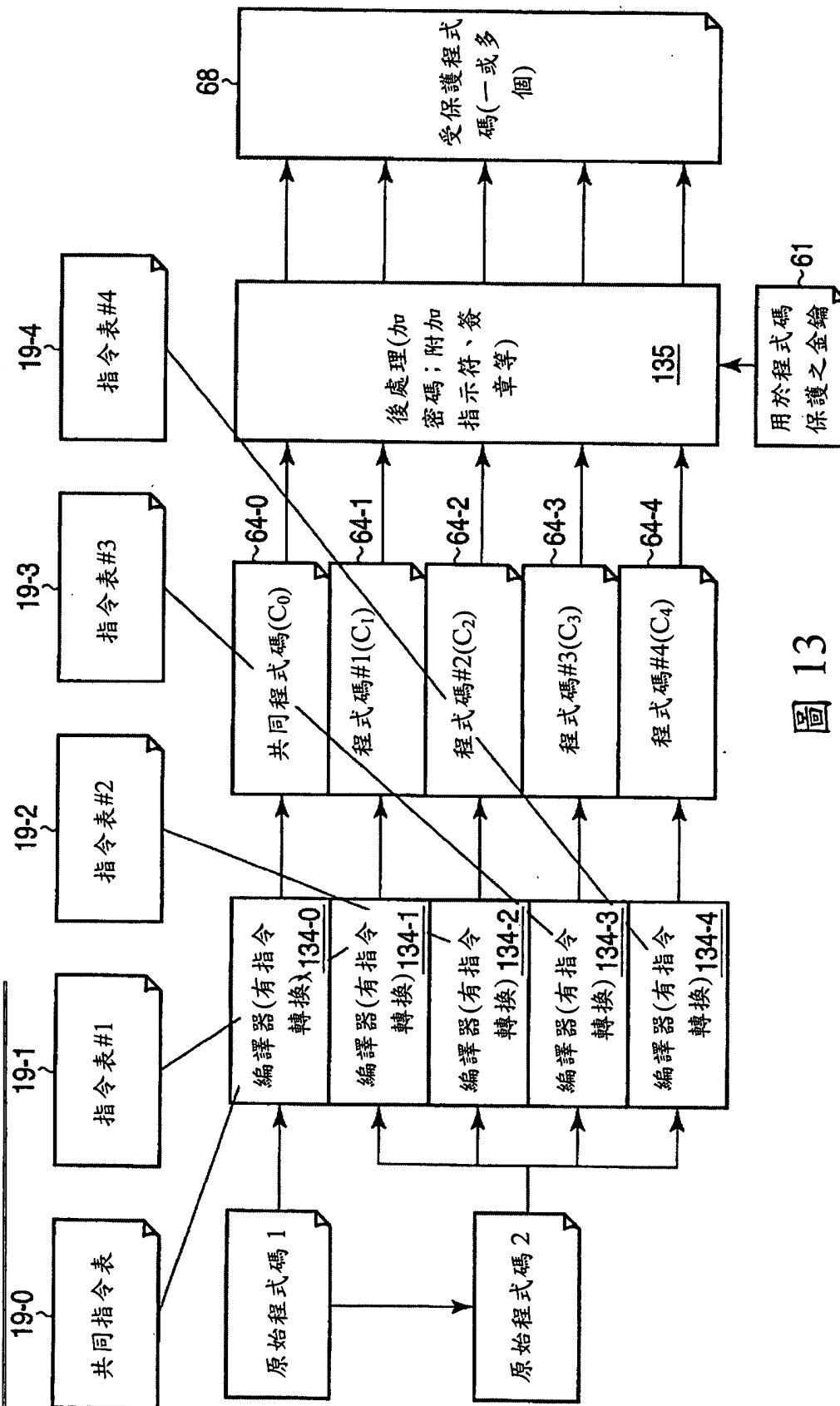


圖 13

當在共同處理之後執行個別處理時(當在處理原始程式碼 0 之後處理原始程式碼 1 至 4 時)

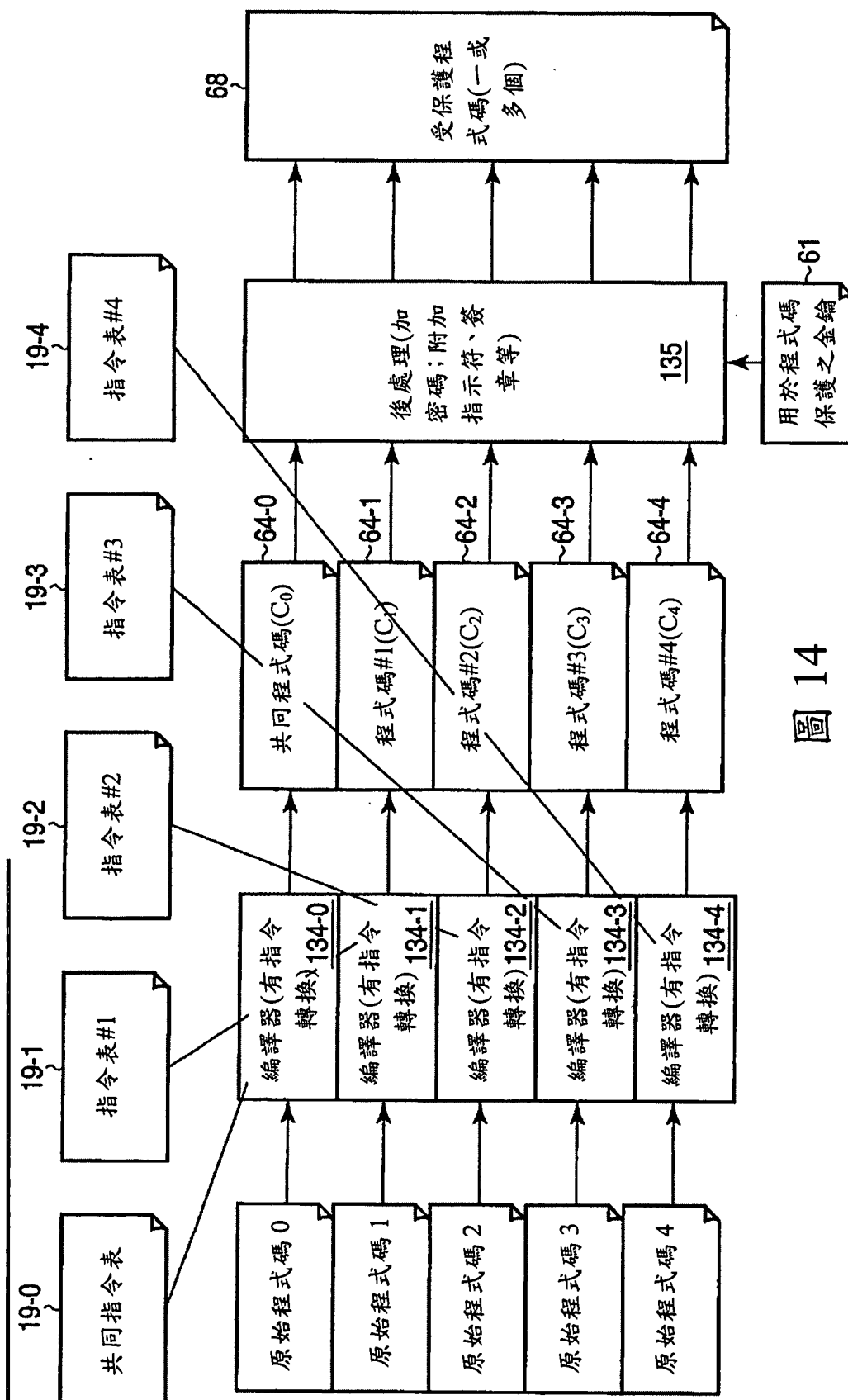


圖 14

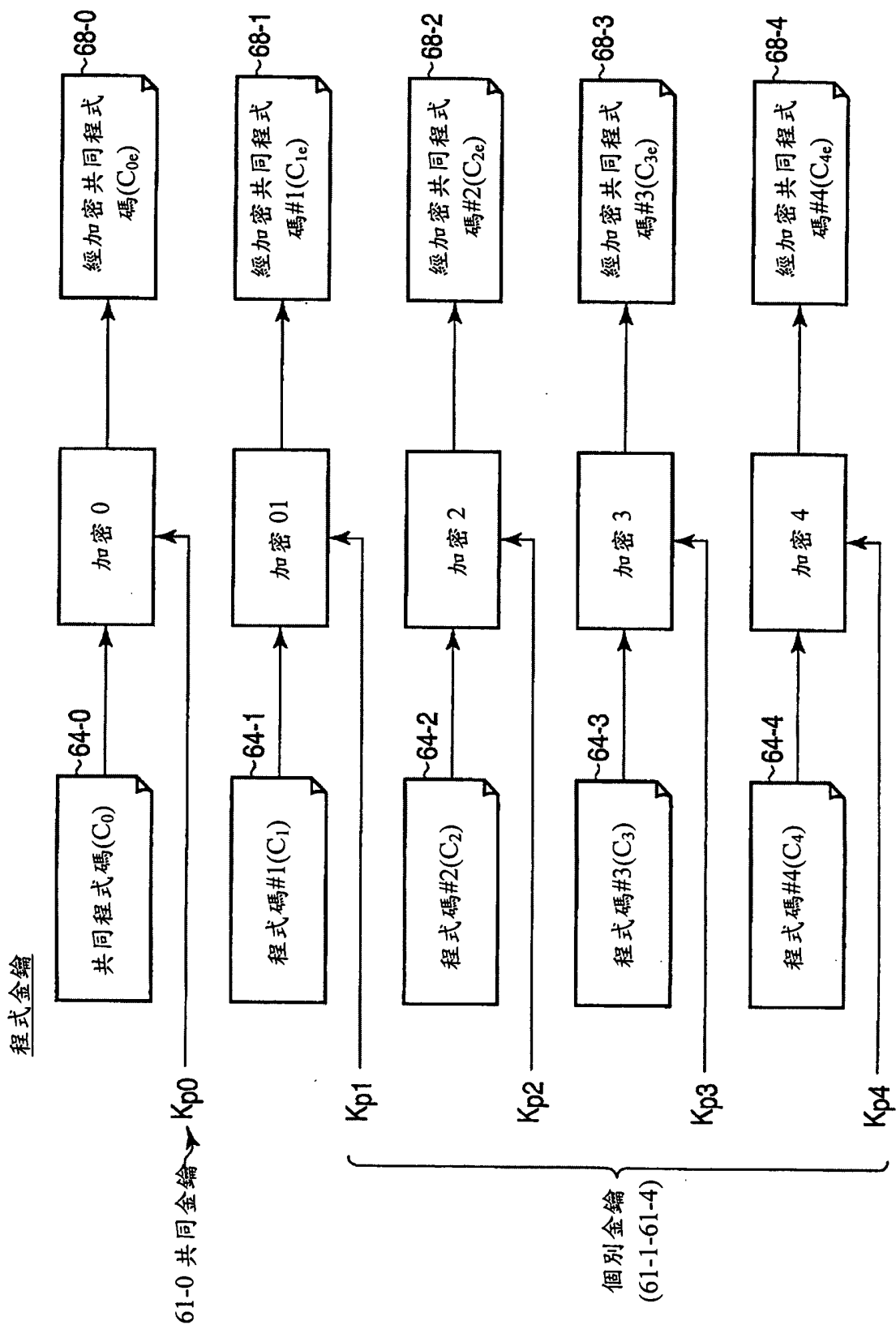


圖 15

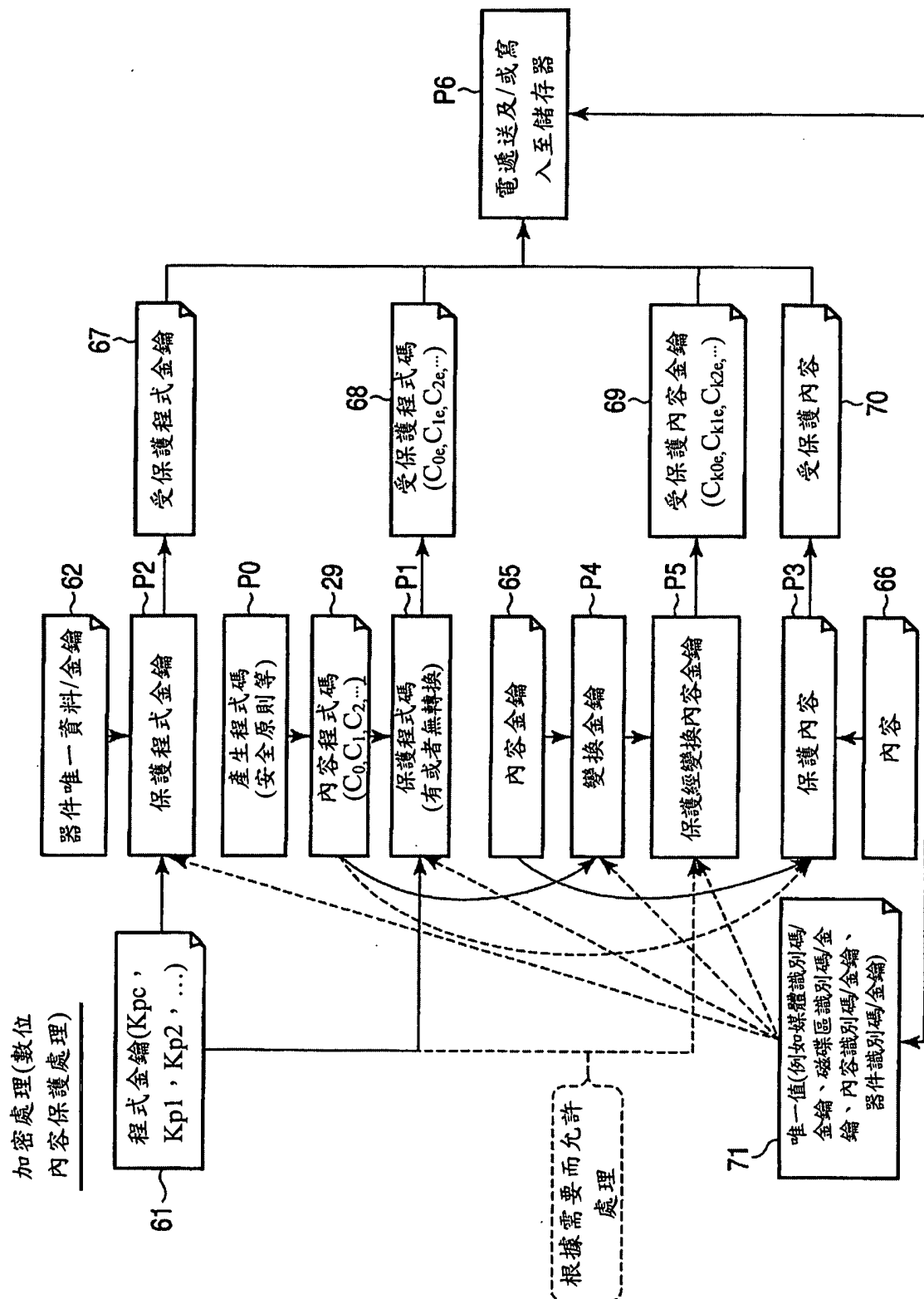


圖 16

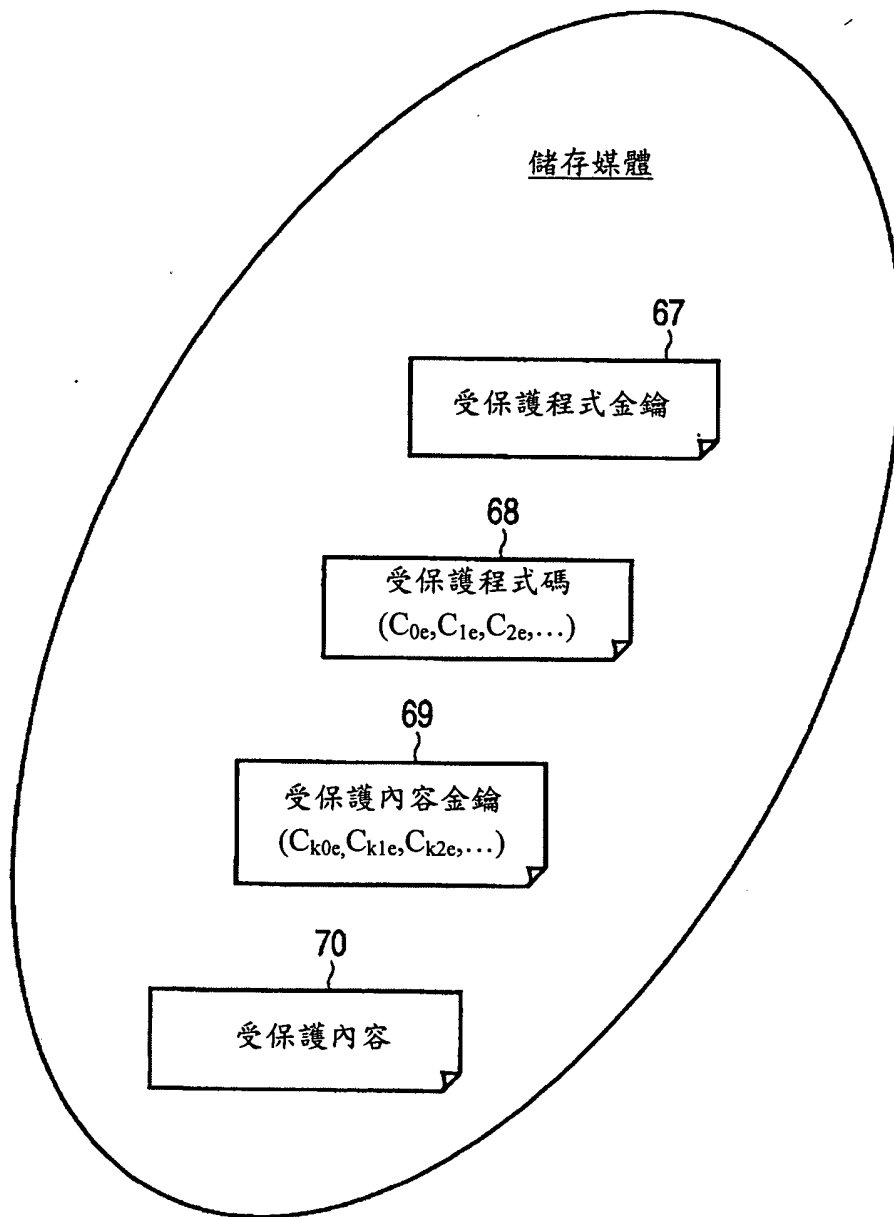


圖 17A

安全數位卡

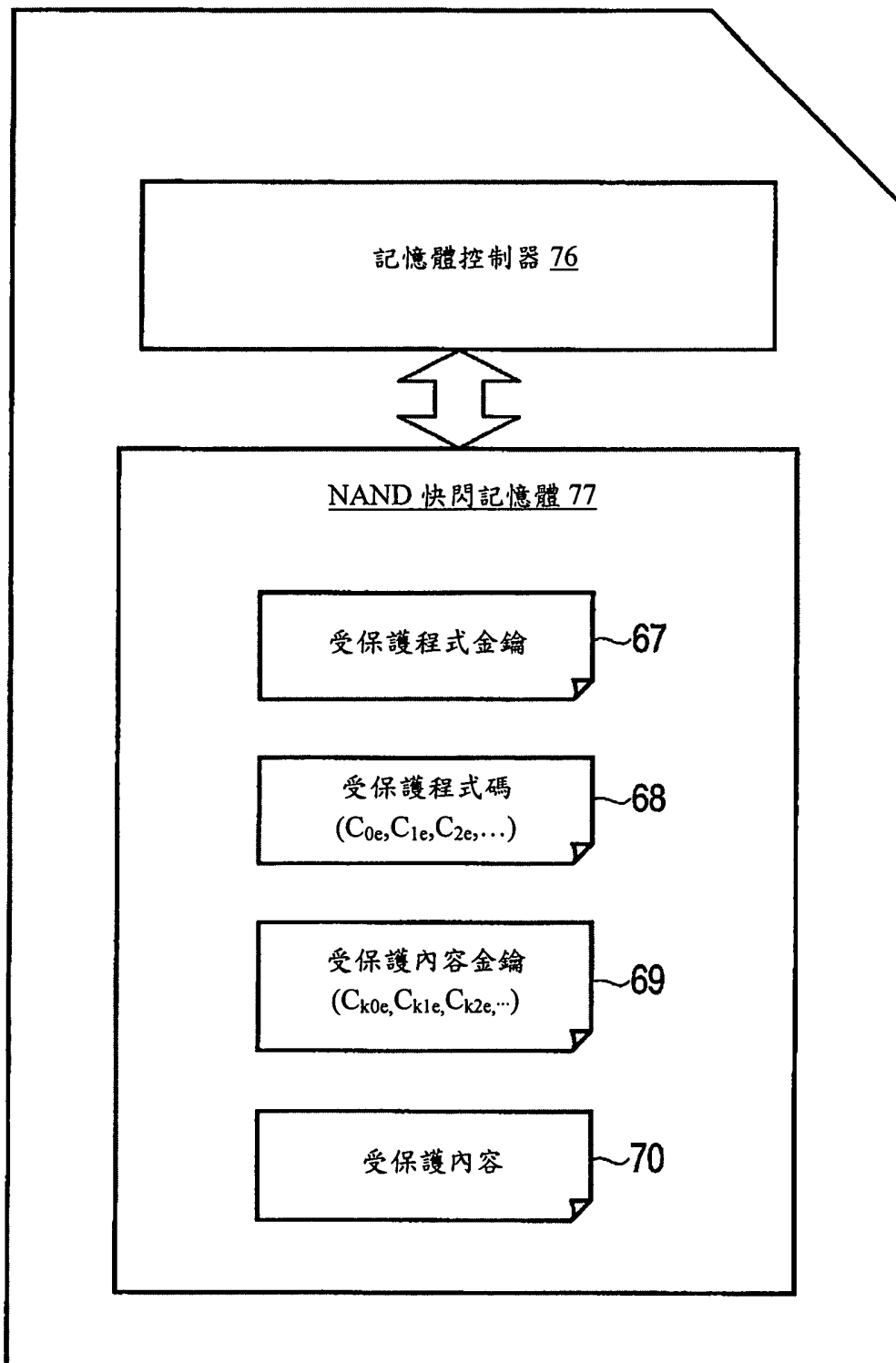


圖 17B

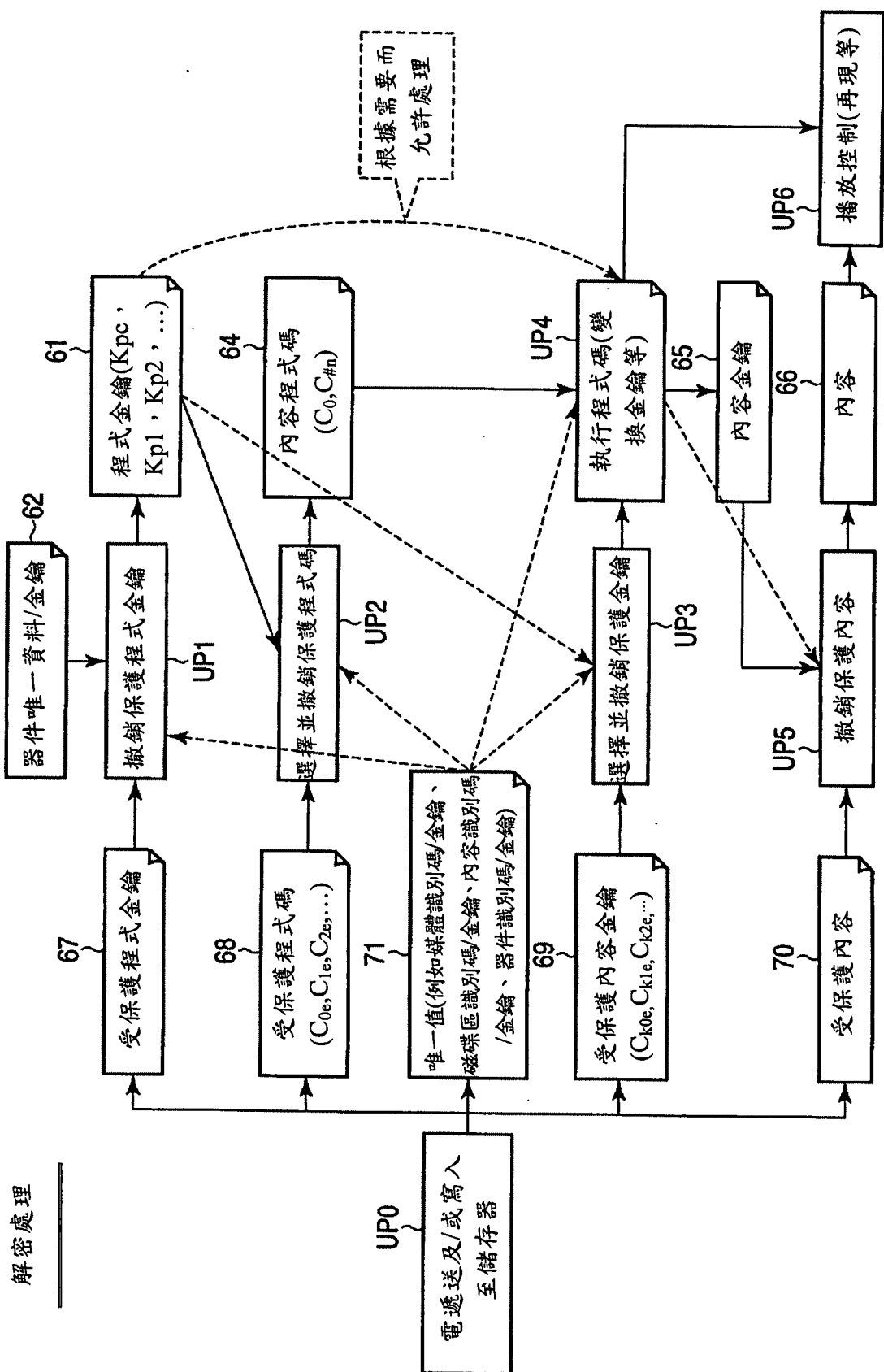


圖 18

四、指定代表圖：

(一)本案指定代表圖為：第 (16) 圖。

(二)本代表圖之元件符號簡單說明：

29	內容程式碼
61	金鑰
62	資訊
65	內容金鑰
66	內容
67	受保護程式金鑰
68	受保護程式碼
69	受保護內容金鑰
70	受保護內容
71	唯一值

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)