申請日期	90 年 7 月 10 日
案號	90116898
類別	G06K 17/00

A4
C4

541486

（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	資料處理裝置、資料處理方法、及授權系統、以及程式提供媒體
	英文	
二、發明 創作 人	姓名	(1) 岡上拓己
	國籍	(1) 日本
	住、居所	(1) 日本國東京都品川區北品川六－七－三五 蘇妮股份有限公司
三、申請人	姓名（名稱）	(1) 蘇妮股份有限公司 ソニー株式会社
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都品川區北品川六丁目七番三五號
	代表人姓名	(1) 出井伸之

裝 訂 線

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
日本	2000 年 7 月 24 日	2000-222123	☑有主張優先權
日本	2000 年 8 月 17 日	2000-247463	☑有主張優先權

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　)

（本發明所屬之技術領域）

本發明係有關於資料處理裝置、資料處理方法，及授權系統以及程式提供媒體。特別是有關於藉由利用樹狀結構之階層的密碼配送方式，只針對具有洽法授權之裝置可以解碼地配送認證密碼，藉此，除了針對在階層的密碼配送樹之管理下的裝置可進行利用內容的授權管理外，即使對於利用未具有相互認證處理功能的記憶裝置來進行資料記錄或資料再生的情形，也可以根據授權來限制利用內容之資料處理裝置、資料處理方法、及授權系統，以及程式提供媒體。

（習知技術）

目前乃盛行以網際網路等的網路、或是記憶卡、ＤＶＤ、ＣＤ等之可流通的記憶媒體，而讓音樂資料、遊戲程式、畫像資料等之各種的軟體資料（以下將該稱之爲內容（Content））的內容流通。該些的流通內容，則藉由在使用者所擁有的ＰＣ（Personal Computer）、再生專用器、或是遊戲機器中接收到內容資料，或是藉由安裝記憶卡、ＣＤ、ＤＶＤ等的記憶媒體來執行內容再生處理。或是將來自外部的輸入內容儲存在內藏在再生器、ＰＣ等記錄裝置，例如記憶卡、硬碟等，而藉由再度從儲存媒體而再生等的方法而被利用。

在再生裝置、遊戲機器、ＰＣ等的資料機器，爲了要從網路接收到流通內容，或是對ＤＶＤ、ＣＤ等進行存取

五、發明說明(2)

的介面，更者，則具有對於內容之再生爲必要的控制機構、程式、作爲資料之記憶體領域所使用的ＲＡＭ、ＲＯＭ等。

音樂資料、畫像資料、或程式等的各種的內容，則根據來自當作再生機器而利用之再生機器、遊戲機器、ＰＣ等之資料機器本體的使用者指示，或是經由所連接之輸入機構而來的使用者的指示，而從內藏，或是可自由裝卸的記憶媒體而被呼出，經由資訊機器本體，或是被連接之顯示器、揚聲器等而被再生。

遊戲程式、音樂資料、畫像資料等許多的軟體內容，一般而言，由其製作者，販賣者保有散佈權。因此，在分配該內容時，則只針對一定的利用限制，亦即，正規的使用者允許使用軟體，而一般採用已考慮到不進行未允許之複製等，亦即，安全性的構成。

用於實現對於限制使用者使用的１個方法即是對於分配內容的編碼處理。亦即，除了分配例如經由網際網路等的經編碼的聲音資料、畫像資料、遊戲程式等之各種內容外，也只針對被確認爲正規使用者的人，才可針對所分配的編碼內容實施解碼的手段，亦即，是一賦予解碼密碼的構成。

編碼資料，則可以藉由一定手段之解碼處理而回復到可以利用的解碼資料。以往已知有一應用編碼密碼在如此之資訊的編碼處理，而應用解碼密碼在解碼處理的資料編碼、解碼方法。

五、發明說明(3　)

利用編碼密碼與解碼密碼之資料編碼、解碼方法的形態乃有各式各樣，其中1個例子即是被稱爲所謂的共同密碼編碼方式的方式。共同密碼編碼方式，則是將應用於資料之編碼處理的編碼密碼與應用於資料之解碼處理的解碼密碼設成共用，針對正規的使用者賦予應用在編碼處理、解碼處理上的共用密碼，而排除未具有密碼的非法使用者來存取資料。該方式的代表方式則有ＤＥＳ（資料編碼標準：Data encryption standard)。

應用在上述之編碼處理、解碼處理的編碼密碼、解碼密碼，則可以例如根據某個密碼（password）來利用hash函數等的單向性函數。所謂的單向性函數是一很難從其輸出反向地求出輸入乃非常困難的函數。例如將由使用者所決定的密碼（password）當作輸入而應用單向性函數，而根據其輸出產生編碼密碼、解碼密碼。如此般，實質上不可能從編碼密碼、解碼密碼反向地求出作爲原始之資料的密碼。

又，將根據在作編碼時所使用的編碼密碼而實施的處理，與在作解碼時所使用之解碼密碼而實施的處理設成不同算張（algorithm)的方式，則是一被稱爲所謂的公開密碼編碼方式。公開密碼編碼方式則是一使用不特定的使用者可以使用的公開密碼的方法，而利用由特定個人所發行的公開密碼，而針對對於特定個人的編碼文書進行編碼處理。根據公開密碼而經編碼的文書，則只有根據與在該編碼處理所使用的公開密碼呈對應的秘密密碼來實施解碼處

五、發明說明（4　）

理。由於秘密密碼只爲發行公開密碼的個人所擁有，因此，根據該公開密碼而編碼的文書，則只有擁有秘密密碼的個人才能實施解碼。公開密碼編碼方式的代表者則有RSA（Rivest-Shamir-Adleman）編碼。藉由利用該編碼方式，可實現只有正規使用者才能對編碼密碼實施解碼的系統。

（本發明所要解決的課題）

上述之內容配送系統，大多採用將內容編碼而經由網路，或是儲存在DVD、CD等的記錄媒體，提供給用者，而只將用於對編碼內容實施解碼的內容密碼提供給合法使用者的構成。此外，則提出一將用於防止內容密碼本身遭到非法複製的內容密碼實施編碼而提供給合法的使用者，利用只有合法的使用者才會有的解碼密碼，對編碼內容密碼實施解碼而能夠使用內容密碼的構成。

對於是否爲合法的使用者的判定，一般而言，則是在例如作爲內容之發送者的內容提供者與使用者裝置之間，在配送內容，或是內容密碼之前先執行認證處理來進行。在一般的認證處理中，除了確認對象外，也產生只對其通訊才會有效的通話密碼（session key），當認證成立時，則利用所產生的通話密碼，針對資料，例如內容或內容密碼實施編碼而進行通訊。認證方式則有利用共用密碼編碼之式的相互認證，與利用公開密碼方式的認證方式，但是在利用共用密碼進行認證時，則系統必須要有共用的密碼

五、發明說明 (5)

，因此，在作更新處理時會非常不方便。又，在公開密碼方式中，則占算負載會變大，且連必要的記憶體量也會變大，而不能說在各裝置設置如此的處理機構是很好。

在本發明中，其目的在於提供一不需要依賴如上述般資料在送出者、接收者之間的相互認證處理，利用樹狀結構之階層的密碼配送方式，在只有擁有合法授權的裝置才能夠進行解碼的情形下來配送認證密碼，除了針對在階層的密碼配送樹之管理下的裝置可進行利用內容的授權管理外，即使對於未具有相互認證處理功能的記憶裝置來進行資料記錄或資料再生的情形，也可以根據授權來限制利用內容之資料處理裝置、資料處理方法、及授權系統、以及程式提供媒體。

（解決課題的手段）

本發明之第 1 實施例如下。

本發明之資料處理裝置，其主要係針對一對來自記憶裝置的資料進行再生，或對記憶裝置進行資料記錄之資料處理裝置，其特徵在於：

上述資料處理裝置具有以在資料處理裝置與記憶裝置之間之相互認證之成立作爲條件，而執行對來自上述記憶裝置的資料進行再生處理，或對上述記憶裝置進行資料記錄處理的構成，

當上述記憶裝置未具有相互認證處理之執行功能時，則具有執行與構成上述資料處理裝置之假想記憶裝置之相

五、發明說明（6）

互認證處理，以在資料處理裝置與上述假想記憶裝置之間所執行之相互認證處理的成立爲條件，而執行對來自上述記憶裝置的資料進行再生處理，或對上述記憶裝置進行資記錄處理的構成。

更者，在本發明之資料處理裝置之一實施態樣中，上述資料處理裝置，具有進行資料再生或資料記錄的記憶裝置會判斷是否可進行相互認證，當可進行相互認證處理時，則在與該記憶裝置之間執行相互認證處理的構成。

更者，在本發明之資料處理裝置之一實施態樣中，上述資料處理裝置，具有根據包含有：在構成讓各密碼對應於在從以多個資料處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉之密碼樹之路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料在內之有效化密碼區塊（ＥＫＢ），而被編碼之認證密碼的ＥＫＢ配送認證密碼，

在上述資料處理裝置與上述假想裝置之間所執行之相互認證處理，則是一可應用上述ＥＫＢ配送認證密碼，與事先被儲存在上述假想記憶裝置的認證密碼來執行的構成。

更者，在本發明之資料處理裝置之一實施態樣中，上述包含ＥＫＢ配送認證密碼的有效化密碼區塊（ＥＫＢ），爲一在構成上述密碼樹之葉的資料處理裝置中，則只有在有正常執照的資料處理裝置中才可進行解碼，而在未具有正常執行之資料處理裝置中，則不能進行解碼之有效化

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ ）

密碼區塊（ＥＫＢ），

爲了要防止在違法資料處理裝置中發生與上述假想記憶裝置之間的認證成立，是一能夠排除法資料處理裝置的構成。

更者，在本發明之資料處理裝置之一實施態樣中，上述有效化密碼區塊（ＥＫＢ）所編碼而提供的ＥＫＢ配送認證密碼乃實施世代（version）管理，是一執行各世代之更新處理的構成。

更者，在本發明之資料處理裝置之一實施態樣中，上述資料處理裝置具有一根據以該資料處理裝置固有的儲存密碼（kstd），針對在讓各密碼對應於在從以多個情報處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉的密碼樹狀結構中，對應於本身的葉所設定的葉密碼進行編碼，且將之儲存在資料處理裝置內的記憶裝置內。

更者，在本發明之資料處理裝置之一實施態樣中，上述資料處理裝置，根據在讓各密碼對應於在從以多個資料處理裝置作爲葉而構成的樹的根到葉爲止之路徑上的根、節點，以及葉的密碼樹狀結構中，其中與本身葉對應而設定的葉密碼，將在從上述密碼樹之本身葉到上位之路徑上的多段的不同的節點密碼個別加以編碼，而作爲編碼密碼之集合的裝置密碼區塊（ＤＫＢ）儲存在資料處理裝置內的記憶機構。

更者，本發明之第２實施例如下。

五、發明說明（ ）

本發明之資料處理方法，其主要係針對一對來自記憶裝置的資料進行再生，或對記憶裝置進行資料記錄之資料處理方法，其特徵在於：

當上述記憶裝置未具有相互認證處理的執行功能者，則執行與構成爲資料處理裝置之假想記憶裝置之相互認證處理的步驟及；

以在上述資料處理裝置與上述假想記憶裝置之間所執行的相互認證處理的成立作爲條件，而對來自上述記憶裝置的資料進行再生處理或對上述記憶裝置進行資料記錄處理的步驟。

更者，在本發明之資料處理方法之一實施態樣中，上述資料處理方法，具有進行資料再生或資料記錄的記憶裝置會判斷是否可進行相互認證的步驟，當可進行相互認證處理時，則在與該記憶裝置之間執行相互認證處理的構成。

更者，在本發明之資料處理方法之一實施態樣中，上述資料處理方法，具有根據包含有：在構成讓各密碼對應於在從以多個資料處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉之密碼樹之路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料在內之有效化密碼區塊（ＥＫＢ），而被編碼之作爲認證密碼的ＥＫＢ配送認證密碼，

在上述資料處理裝置與上述假想裝置之間所執行之相互認證處理，則是一可應用上述ＥＫＢ配送認證密碼，與

五、發明說明（9）

事先被儲存在上述假想記憶裝置的認證密碼來執行的構成。

更者，本發明之第3實施例如下。

本發明之授權系統，其主要係一可對資料處理裝置賜予授權的授權系統，其特徵在於：

提供根據包含有：在構成讓各密碼對應於在從以多個資料處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉之密碼樹之路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料在內之有效化密碼區塊（ＥＫＢ），而被編碼之認證密碼的ＥＫＢ配送認證密碼，

資料處理裝置具有即使記憶裝置未具有相互認證處理之執行功能時，也會將與構成上述資料處理裝置之假想記憶裝置之相互認證處理的成立當作對來自上述記憶裝置之資料進行再生處理，或對上述記憶裝置進行資料記錄處理之執行條件的構成，

提供上述ＥＫＢ配送認證密碼的有效化密碼區塊（ＥＫＢ），爲一在構成上述密碼樹之葉的資料處理裝置中，則只有在有正當授權的資料處理裝置中才可進行解碼，而在未具有正當授權之資料處理裝置中，則不能進行解碼之有效化密碼區塊（ＥＫＢ），藉此可以防止在非法資料處理裝置中發生與上述假想記憶裝置之間的認證成立，是一能夠排除非法資料處理裝置利用內容的構成。

更者，本發明之第4實施例如下。

五、發明說明 (10)

本發明之程式提供媒體，其特徵在於：係針對一用來提供可以在電腦系統上執行對來自記憶裝置之資料進行再生，或對記憶裝置進行資料記錄之處理處理之電腦程式的程式提供媒體，上述電腦程式具有：

當上述記憶裝置未具有相互認證處理的執行功能者，則執行與構成爲資料處理裝置之假想記憶裝置之相互認證處理的步驟及；

以在上述資料處理裝置與上述假想記憶裝置之間所執行的相互認證處理的成立作爲條件，而對來自上述記憶裝置的資料進行再生處理或對上述記憶裝置進行資料記錄處理的步驟。

（發明之實施形態）

〔系統概要〕

圖１爲可適用本發明之資料處理系統之內容（content）配送系統的例子。內容配送機構１０，則將內容，或者內容密碼（content key)等其他之認證密碼等的資料加以編碼，而送到資料處理機構２０。在資料處理機構２０中，則將所收到之編碼內容，或是編碼內容密碼等加以解碼，而取得內容或是內容密碼等，進行畫像資料、聲音資料的再生，或是執行各種程式。在內容配送機構１０與資料處理機構２０之間的資料交換，則是經由網際網路（Internet）等之網路，或是ＤＶＤ、ＣＤ等其他之可流通的記憶媒體而被執行。

五、發明說明 (11)

資料處理機構２０，則將資料儲存在備有例如快閃記憶體等之記憶機構的記憶卡等的資料記憶機構３０而加以保存。資料記憶機構３０則包含有作爲具有編碼處理功能之記憶機構的例如記憶卡（具體例爲記憶條（Memory Stick：商標））。在從資料處理機構２０，將資料儲存在資料記憶機構３０，以及從資料記憶機構３０，將資料移動到資料處理機構之際，則執行相互認證處理，以及資料的編碼處理，以防止非法的資料複製。

此外，內容資料也可以在資料處理機構２０中的各機器之間移動。此時，也執行機器間的相互認證處理、資料的編碼處理。

內容配送機構１０則有網際網路（Internet）１１、衛星傳送１２、電話線路１３、ＤＶＤ、ＣＤ等的媒１４等，另一方面，資料處理機構２０的裝置則有個人電腦（ＰＣ）２１、攜帶型裝置（ＰＤ）２２、行動電話、ＰＤＡ（Personal Digital Assistants）等之攜帶機器２３、ＤＶＤ、ＣＤ播放機等之記錄再生器，遊戲終端機２４，利用記憶卡（例如 Memory Stick（商標））的再生裝置２５等。該些資料處理機構２０的各裝置，可以從Internet等之通訊方式，或是其他的資料處理機構，或是資料記憶機構３０來取得由內容配送機構１０所提供的內容。

圖２爲代表性的內容資料（content data）的移動處理例。圖２所示的系統則表示資料（內容）在個人電腦（

（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)

ＰＣ）１００、再生裝置２００以及記憶裝置３００之間移動之處理例的說明圖。ＰＣ　１００具有程式以及資料記憶用的硬帶（ＨＤ），更者，則具有可安裝作爲外部記憶體之ＣＤ、ＤＶＤ等的構造。

個人電腦（ＰＣ）１００可以連接到 Internet、公用線路等之各種網路，例如從提供ＥＭＤ（Electronic Music Distribution：電子音樂配送）等之服務之未圖示之提供服務者的主電腦，經由網路接收到音頻資料、畫像資料、程式等的各種資料，而因應所需，將所收到的資料加以解碼，而輸出到再生裝置２００。又，個人電腦（ＰＣ）１００，當接收內容資料時，則因應必要，在與提供服務者之主電腦之間進行認證處理以及收費處理。又，個人電腦（ＰＣ）１００會將例如從ＣＤ、ＤＶＤ所輸入的資料輸出到再生裝置２００。

記憶裝置３００是一可相對於再生裝置２００進行自由裝卸的裝置，例如記憶條（Memory Stick：商標），而內藏有快閃記憶體等之可更寫的半導體記憶體。

如圖２所示，在進行ＰＣ　１００、再生裝置２００、記憶裝置３００之間的資料移動，例如音樂資料、畫像資料等資料再生、資料記錄、資料複製的處理時，則在資料移動器之間執行相互認證處理，以防止利用非法的機器來移動資料。有關該些的處理請容後述。又，在內容資料經由網路或是各種記憶媒體來配送，以及內容在ＰＣ與再生裝置相互間，或再生裝置與記憶卡等之記憶裝置之間移

五、發明說明 (13)

動時，則藉由將內容實施編碼，可以維護資料的安全。

〔有關作爲密碼配送構成之樹狀結構〕

請參照圖3來說明將適用於上述內容之編碼處理的編碼密碼，例如適用於內容之編碼處理之內容密碼，或用於將內容密碼加以編碼之內容密碼編碼化之密碼等之各種的編碼處理密碼配送到擁有安全且合法授權的裝置的構造，亦即，階層密碼樹狀結構。

在圖3之最下段所示的號碼0～15則是一用於構成進行內容資料之再生、執行之資料處理機構20的各裝置，例如內容（音樂資料）再生裝置。亦即，圖3所示之階層樹狀結構的各葉（leaf）則相當於各裝置。

各裝置0～15，，則在製造時或出貨時，或是之後，將由被分配到圖3所示之階層樹狀結構中之從本身葉（leaf ）到根（root）爲止之節點密碼（node key）以及各葉的葉密碼（leaf key）所構成的密碼組（key set）儲存在記憶體內。圖3之最下段所示之K0000～K1111爲分別被分配給各裝置0～15的葉密碼，而從最上段的KR（根密碼）開始，將被記載在從最小段數來第2節點的密碼：KR～K111當作節點密碼（node key）。

在圖3所示的樹狀結構中，例如裝置0具有葉密碼K0000，與節點密碼：K000、K00、K0、KR。裝置5具有K0101、K010、K01、K0

五、發明說明（14）

、ＫＲ。裝置１５具有Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲ。此外，在圖３的樹中只記載了裝置０～１５共１６個，而連樹狀結構也採用４段構成之取得均衡之左右對稱結構，更多的裝置被構成在樹中，或是在樹的各部具有不同的段數構成。

又，在圖３之樹狀結構中所包含的各裝置，則包含有各種的記錄媒體，例如使用了裝置埋入型或構成爲可自由裝卸於裝置之快閃記憶體等的記憶卡、ＤＶＤ、ＣＤ、ＭＤ等之各種型式之記憶裝置的裝置。更者，可共同存在有各種的應用服務。作爲圖３所示之內容或密碼分配結構的階層樹狀結構可以應用在不同的裝置，不同應用的共存結構上。

在該些各種的裝置、應用程式（application）共存的系統中，例如圖３之以虛線所包圍的部分，亦即，裝置０、１、２、３，則設定爲利用同一個記錄媒體的１個群（group）。例如，執行將共通的內容實施編碼，而從提供者送至在以該虛線所包圍之群內的裝置而送出供各裝置共同使用的內容密碼（content key），或是從各裝置，將內容費用之支付資料實施編碼而輸出到提供者或是收費機關等的處理。內容提供者，或是收費處理機關等之進行與各裝置之資料送受訊的機關，則將圖３之以虛線所示的部分，亦即，裝置０、１、２、３當作１個群，而執行一次送出資料的處理。如此的群則有多個存在於圖３的樹中。內容提供者，或收費處理機構等之進行與各裝置之資料收發

五、發明說明（15）

的機關，則作爲訊息資料（message data）配送機構。

此外，節點密碼、葉密碼也可以藉由某一個密碼管理中心而加以統括管理，也可以是對各群進行各種之資料送受訊的提供者或根據收費機關等之訊息資料配送機構，而針對各群加以管理的結構。該些的節點密碼、葉密碼，則例如在密碼被洩露時會被執行更新處理，而該更新處理則是由密碼管理中心，提供者，收費機關等來執行。

在該樹狀結構中，由圖3可知，在1個群中所包含的3個裝置0、1、2、3則當作節點密碼，而保有共用的密碼K00、K0、KR。藉由利用該節點密碼共用結構，則只將例如共用的內容密碼提供給裝置0、1、2、3。例如，若將共同保有的節點密碼K00本身設定作爲內容密碼時，則不需要送出新的密碼，而只將共用的內容密碼設定在裝置0、1、2、3。又，若經由網路，或是儲存記錄媒體，將根據節點密碼對新的內容密碼Kcon實施編碼所得到的值EnC(K00,Kcon)分配至裝置0、1、2、3時，則只有裝置0、1、2、3，利用在各裝置所保有的共有節點密碼K00來解讀密碼EnC（K00，Kcon），而得到內容密碼：Kcon。此外，EnC（Ka，Kb）表示根據Ka對Kb實施編碼所得到的資料。

又，在某個時點t，當裝置3所擁有的密碼：K0011、K001、K00、K0、KR被駭客所解開而洩漏時，以後，系統（裝置0、1、2、3的群）爲

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明 (16)

了要維護被送受訊的資料，則必須將裝置3自系統切離。因此，分別將節點密碼：K001、K00、K0、KR更新爲新的密碼K(t)001、K(t)00、K(t)0、K(t)R，而必須將該更新密碼傳至裝置0、1、2。在此，K(t)aaa表示密碼Kaaa的世代(Cteneration：t的更新密碼。

以下說明更新密碼的分配處理。密碼的更新，則將根據如圖4(A)所示之被稱爲有效化密碼區塊(EKB:Enabling Key Block)的區塊資料(block data)所構成的表，藉由供給到網路，或是儲存在記錄媒體，而供給到裝置0、1、2而被執行。此外，有效化密碼區塊(EKB)，則是由用於將最新被更新的密碼分配到與構成圖3所示之樹狀結構之各葉呈對應的裝置的編碼化密碼而構成。有效化密碼區塊(EKB)有時也被稱爲密碼更新區塊(EKB：Key Renewal Block)。

圖4(A)所示之有效化密碼區塊(EKB)，則當作只有必須要更新節點密碼的裝置爲具有可更新資之資料結構的區塊資料而構成。圖4的例子，在圖3所示之樹狀結構中的裝置0、1、2中，爲一以分配世代t之更新節點密碼爲目的而形成的區塊資料。由圖3可知，裝置0，裝置1則必須將K(t)00、K(t)O、K(t)R當作更新節點密碼，而裝置2則必須將K(t)001、K(t)00、K(t)0、K(t)R當作更新節點密碼。

經濟部智慧財產局員工消費合作社印製

五、發明說明 (17)

如圖４（Ａ）之ＥＫＢ所示，ＥＫＢ包含多個的編碼化密碼。最下段的編碼化密碼爲Ｅｎｃ（Ｋ００１０、Ｋ（ｔ）００１）。而此爲根據裝置２所具有的葉密碼Ｋ００１０而被編碼的更新節點密碼Ｋ（ｔ）００１，裝置２則根據本身所具有的葉密碼，將該編碼化密碼加以解碼，而得到Ｋ（ｔ）００１。又，利用由解碼所得到的Ｋ（ｔ）００１，可以對從圖４（Ａ）之下方數來第２段的編碼化密碼ＥｎＣ（Ｋｃｔ）００１、Ｋ（ｔ）００）進行解碼，而能夠得到更新節點密碼Ｋ（ｔ）００。以下，則依序對從圖４（Ａ）之上方數來第２段的編碼化密碼ＥｎＣ（Ｋ（ｔ）００、Ｋ（ｔ）０）進行解碼而得到更新節點密碼Ｋ（ｔ）０，對從圖４（Ａ）之上方數來第１段的編碼化密碼ＥｎＣ（Ｋ（ｔ）０、Ｋ（ｔ）Ｒ進行解碼而得到Ｋ（ｔ）Ｒ。另一方面，裝置Ｋ０００００、Ｋ０００１，節點密碼Ｋ０００則不列入於更新的對象，而必須作爲更新節點密碼者則有Ｋ（ｔ）００、Ｋ（ｔ）Ｏ、Ｋ（ｔ）Ｒ。裝置Ｋ００００、Ｋ０００，則對從圖４（Ａ）之上方數來第３段的編碼化密碼ＥｎＣ（Ｋ０００、Ｋ（ｔ）００）進行解碼而得到Ｋ（ｔ）００，接著，則對從圖４（Ａ）之上方數來第２段的編碼化密碼ＥｎＣ（Ｋ（ｔ）００、Ｋ（ｔ）０）進行解碼而得到更新節點密碼Ｋ（ｔ）０，對從圖４（Ａ）的上方數來第１段的編碼化密碼ＥｎＣ（Ｋ（ｔ）０、Ｋ（ｔ）Ｒ）進行解碼而得到Ｋ（ｔ）Ｒ。如此一來，裝

五、發明說明 (18)

置０、１、２可以得到經更新的密碼Ｋ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒ。此外，圖４（Ａ）的索引則表示當作解碼密碼來使用之節點密碼、葉密碼的絕對位址。

圖３所示之樹狀結構之上位段的節點密碼，則不需要更新Ｋ（ｔ）０、Ｋ（ｔ）Ｒ，當只有必須進行節點密碼Ｋ００的更新處理時，藉由利用圖４（Ｂ）之有效化密碼區塊（ＥＫＢ），可將更新節點密碼Ｋ（ｔ）００分配給裝置０、１、２。

圖４（Ｂ）所示的ＥＫＢ則可以應用在分配可共用於特定的群的新的內容密碼的情形。具體例則是在圖３中以虛線所示之群內的裝置０、１、２、３利用某個記錄媒體，而必須要有新的共用的內容密碼Ｋ（ｔ）ｃｏｎ。此時，則利用已更新裝置０、１、２、３之共用的節點密碼Ｋ００的Ｋ（ｔ）００，將已對新的共用的更新內容密碼：Ｋ（ｔ）ｃｏｎ實施編碼的資料Ｅｎｃ（Ｋ（ｔ）、Ｋ（ｔ）ｃｏｎ，與圖４（Ｂ）所示的ＥＫＢ一起予以分配。藉由此分配，可以分配在裝置４等之其他的群的機器中未被解碼的資料。

亦即，裝置０、１、２，若是利用處理ＥＫＢ所得到的Ｋ（ｔ）００來對上述編碼文字進行解碼時，則可以得到在ｔ時刻時的內容密碼Ｋ（ｔ）ｃｏｎ。

〔分配使用ＥＫＢ的內容密碼〕

五、發明說明(19)

圖5表示一得到在t時刻時的內容密碼K(t)con的處理例，係表示利用K(t)00，將新的共用的內容密碼K(t)con編碼化所得的資料Enc(K(t)00、K(t)con)，與圖4(B)所示之EKB，經由記錄媒體而收到之裝置O的處理。亦即，是一將根據EKB所得到的編碼化訊息資料當作內容密碼K(t)con的例子。

如圖5所示，裝置O則利用被儲存在記錄媒體的世代：t時點的EKB，與本身事先儲存的節點密碼K000，藉由與上述同樣的EKB處理，而產生節點密碼K(t)00。更者，則利用經解碼的更新節點密碼K(t)00，對更新內容密碼K(t)con實施解碼，之後，爲了要使用，乃根據本身所具有的葉密碼K0000實施編碼而加以儲存。

〔EKB的格式〕

圖6爲表示有效化密碼區塊(EKB)的格式例。世代601爲一表示有效化密碼區塊(EKB)之世代的識別碼。此外，世代則具有識別最新之EKB的功能，與表示和內容之對應關係的功能。深度(depth)表示相對於有效化密碼區塊(EKB)之分配對象之裝置的階層樹的階層數。資料指標(data pointer)603則是一表示在有效化密碼區塊(EKB)中之資料部的位置的指標，標籤指標(tag pointer)604是一表示標籤部的位置的指標

五、發明說明(20)

，而署名指標６０５是一表示署名之位置的指標。

資料部６０６則儲存了例如已將作更新的節點密碼實施編碼的資料。而儲存有與例如圖５所示之被更新的節點密碼相關的各編碼密碼等。

標籤部６０７是一表示被儲存在資料部之經編碼的節點密碼，葉密碼之位置關係的標籤。利用圖７來說明該標籤的給予原則。在圖７中，則表示送出在圖４（Ａ）所述之有效化密碼區塊（ＥＫＢ）作爲資料的例子。此時的資料則成爲如圖７的表（ｂ）所示。將此時之編碼化密碼中的上節點（Top node)的位址設爲上節點位址。此時，由於包含了根密碼(root key)的更新密碼Ｋ（ｔ）Ｒ，因此，上節點位址成爲ＫＲ。此時，例如最上段的資料Ｅｎｃ（Ｋ（ｔ）０、Ｋ（ｔ）Ｒ，則位在如圖７的（ａ）所示之階層樹的位置。在此，接下來的資料爲Ｅｎｃ（Ｋ（ｔ）００、Ｋ（ｔ）０），在樹上，則位於前一個資料的左下方的位置。當有資料時，標籤爲０，而當沒有時，則設定爲１。標籤則設定爲｛左（Ｌ）標籤、右（Ｒ）標籤｝。由於在最上段之資料Ｅｎｃ（Ｋ（ｔ）０、Ｋ（ｔ）Ｒ）的左方有資料，因此，Ｌ標籤＝０，而由於在右方沒有資料，因此成爲Ｒ標籤＝１。以下，則針對全部的資料設定標籤，而構成圖７（Ｃ）所示的資料例，以及標籤列。

標籤是一用於表示資料Ｅｎｃ（Ｋｘｘｘ、Ｋｙｙｙ）要位在樹狀結構之何處而設者。儲存在資料部的密碼資

五、發明說明（21）

料Ｅｎｃ（Ｋｘｘｘ、Ｋｙｙｙ）……，由於只不過是單純地被編碼的羅列資料，因此，根據上述的標籤，可以判斷當作資料而被儲存的編碼化密碼在樹上的位置。在不利用上述的標籤的情形下，如先前的圖４中所示的結構般，使用與編碼化資料對應的節點索引(node index)，例如可以是以下的資料結構。

０：Ｅｎｃ（Ｋ（ｔ）０、Ｋ（ｔ）ｒｏｏｔ）

００：Ｅｎｃ（Ｋ（ｔ）００、Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（ｔ）０００、Ｋ（ｔ）００）

當設成採用如此的索引的結構時，則會成爲一冗長的資料，而導致資料量增加，而不適於經由網路來配送。相較於此，藉由使用表示上述標織之密碼位置的索引資料，可以根據少的資料量來判別密碼位置。

回到圖６再說明ＥＫＢ格式。簽名（Signature）是一由發出有效化密碼區塊（ＥＫＢ）之例如密碼管理中心，內容提供者，收費機關等所執行的電子簽名。乃根據簽名檢畫來確認收到ＥＫＢ的裝置爲一由合法之有效之有效化密碼區塊（ＥＫＢ）發生者所發出的有效化密碼區域（ＥＫＢ）。

〔配送已使用ＥＫＢ的內容密碼以及內容〕

在上述的例子中是說明只有內容密碼與ＥＫＢ一起送出的例子，但以下則說明將經內容密碼被編碼的內容，經內容密碼編碼密碼被編碼的內容密碼，與經ＥＫＢ被編碼

五、發明說明（22）

的內容密碼編碼一起送出的結構。

圖8表示該資料結構。在圖8（a）所示的結構中，Enc（Kcon.content）801是一根據內容密碼（Kcon）對內容（Content）實施編碼的資料，Enc（KEK，Kcon）802是一根據有效化密碼區塊對內容密碼編碼密碼KEK實施編碼的資料。

在此，內容密碼編碼密碼KEK可以是圖3所示的節點密碼（K000、K00……），或根密碼（KR）本身，或是根據節點密碼（K000、K00……）或根密碼（KR）而被編碼的密碼。

圖8（b）爲表示將多個的內容記錄在媒體，而分別利用相同的Enc（EKB、KEK）805時的結構例。該結構可以是一在對各資料不附加Enc（EKB、KEK）的情形下，將表示連續（link）到Enc（EKB、KEK）之連結對象的資料附加在各資料的結構。

圖9爲表示將內容密碼編碼密碼KEK當作將圖3所示之節點密碼K00更新而成之更新節點密碼K（t）00時的例子。此時，在圖3之以虛線框所包圍的群中，裝置3爲例如因爲密碼洩露而被排除者，藉由將圖9所示之（a）有效化密碼區塊，（b）根據內容密碼編碼密碼（KEK＝K（t）00）對內容密碼（Kcon）實施編碼所得到的資料，（c）根據內容密碼（Kcon）對內容（Content）實施編碼所得到的資料

五、發明說明 (23)

配送到其他群的會員，亦即，裝置０、１、２，因此，裝置０、１、２可以得到內容（content）。

在圖９的右側，則表示在裝置Ｏ中的解碼順序。裝置Ｏ，首先，藉由從所數到的有效化密碼區塊，利用本身所保有之葉密碼Ｋ０００實施解碼處理，可以取得內容密碼編碼密碼（ＫＥＫ＝Ｋ（ｔ）００）。接著，則根據Ｋ（ｔ）００的解碼而取得內容密碼Ｋｃｏｎ，更者，則根據內容密碼Ｋｃｏｎ進行內容的解碼。藉由該些處理，裝置Ｏ可利用內容。在裝置１、２，藉由各個不同的處理順序來處理ＥＫＢ，可以取得內容密碼編碼密碼（ＫＥＫ＝Ｋ（ｔ）００），同樣地可以利用內容。

圖３所示之其他群的裝置４、５、６，即使是收到同樣的資料（ＥＫＢ），利用本身所保有的葉密碼、節點密碼，並無法取得內容密碼編碼密碼（ＫＥＫ）＝Ｋ（ｔ）００）。即使同樣地排除的裝置３，利用本身所保有的葉密碼、節點密碼，也無法取得內容密碼編碼密碼（ＫＥＫ＝Ｋ（ｔ）００），而只有具有合法權利的裝置才能夠對內容實施解碼而加以利用。

如此般，若配送已利用ＥＫＢ的內容密碼時，可以減少資料量，且只有合法授權者則可以實施解碼而來配送編碼內容（content）。

此外，雖然有效化密碼區域（ＥＫＢ）、內容密碼、編碼化密碼等，可以經由網路而安全地加以配送，但是也可以將有效化密碼區塊（ＥＫＢ）、內容密碼、編碼內容

五、發明說明 (24)

儲存在ＤＶＤ、ＣＤ等之記錄媒體而提供給使用者。此時，在對被儲存在記錄媒體的編碼化內容實施解碼，乃使用藉由對被儲存在同一記錄媒體的有效化密碼區塊（ＥＫＢ）實施解碼所得到的內容密碼。因此，可以以簡單的方式來分配只有事先合法授權者所保有的葉密碼、節點密碼才可以使用之編碼化內容的處理，亦即，只分配已限定可以使用之使用者裝置的內容。

圖１０係表示將有效化密碼區塊（ＥＫＢ）與編碼化內容一起儲存在記錄媒體的構成例。在圖１０所示的例子中，將內容Ｃ１～Ｃ４儲存在記錄媒體，更者，則儲存有讓對應於各儲存內容的有效化密碼區塊（ＥＫＢ）賦予對應的資料，更者，則儲存有世代Ｍ的有效化密碼區塊（ＥＫＢ－Ｍ）。例如ＥＫＢ－１被使用在用來產生由內容Ｃ１編碼化而成的內容密碼Ｋｃｏｎ１，而例如ＥＫＢ－２被使用在用來產生由內容Ｃ２編碼化而成之內容Ｋｃｏｎ２。在本例中，世代Ｍ的有效化密碼區塊（ＥＫＢ－Ｍ）則被儲存在記錄媒體，由於內容Ｃ３、Ｃ４係對應於有效化密碼區域（ＥＫＢ－Ｍ），因此，藉由對有效化密碼區域（ＥＫＢ－Ｍ）實施編碼，可以取得內容Ｃ３、Ｃ４的內容密碼。由於ＥＫＢ－１、ＥＫＢ－２未被儲存在碟片內，因此，則必須要有在藉由新的提供方式，例如網路配送，或由記錄媒體來配送，對各自的內容密碼實施解碼爲必要的ＥＫＢ－１、ＥＫＢ－２。

五、發明說明 (25)

〔階層樹狀結構的範疇分類〕

將根密碼、節點密碼、葉密碼等設成圖3的階層樹狀結構而構成編碼密碼，而將內容密碼、證證密碼、ICV產生密碼，或程式碼、資料等與有效化密碼區塊（EKB）一起實施編碼而加以配送，以下則說明將用於定義節點密碼等的階層樹狀結構分類成各裝置的各範疇，而執行有效率的密碼更新處理、編碼密碼配送、資料配送的構成。

圖11係表示階層樹狀結構之範疇分類的一例。在圖11中，在階層樹狀結構的最上段設定有根密碼Kroot 1101，而在以下的中間段設定有節點密碼1102，在最下段則設定有葉密碼1103。各裝置則保有各自的葉密碼，與從葉密碼到根密碼之一連串的節點密碼、根密碼。

在此的一例則是將從最上段數來第M段的某個節點設定作爲範疇節點（category node）1104。亦即，將第M段的各節點設定作爲特定範疇的裝置設定節點。將第M段的1個節點當作頂點，而在M+1段以下的節點、葉則設成與該範疇中的裝置相關的節點以及葉。

例如，在圖11之第M段的1個節點1105設定有範疇〔Memory Stick（商標）〕，而在該節點以下相連的節點、葉則設定爲包含已使用 Memory Stick 之各種裝置在內的範疇專用的節點，或葉。亦即，將節點1105以下定義成被定義在 Memory Stick 之範疇之裝置的相關節點，以及葉的集合。

五、發明說明（26）

更者，可將從M段算來隔數段之位在下方的段設定成副範疇節點（Subcategory node）。如圖所示位於在範疇〔Memory Stick〕節點１１０５之下２段的節點，則設定成〔再生專用器〕節點以作爲包含於已使用 Memory Stick 之裝置之範疇中的副範疇。更者，則在作爲副範疇節點之再生專用器的節點１１０６以下，設定包含於再生專用器之範疇中的附音樂再生功能電話的節點１１０７，更者，則在其下方可以設定包含於附音樂再生功能電話之範疇中的〔ＰＨＳ〕節點１１０８，與〔行動電話〕節點１１０９。

更者，範疇、副範疇，則不只是裝置的種類，也可以由例如某個製造商、內容提供者、清賬機構等獨自管理的節點，亦即，處理單位、管轄單位、或提供服務單位等任意的單位（以下將該些總稱爲實體 Intity）來設定。例如若將１個範疇節點設定爲由遊戲機器製造商所販賣的遊戲機器ＸＹＺ專用的頂點節點時，則可將位在該頂點節點以下之下段的節點密碼、葉密碼儲存在由製造商所販賣的遊戲機器ＸＹＺ來加以販賣。之後，編碼內容的配送，或各種密碼之配送、更新處理，則產生由在該頂點節點密碼以下的節點密碼、葉密碼所構成的有效化密碼區塊（ＥＫＢ）來加以配送，而配送只有在頂點節點以下的裝置才可以利用的資料。

如此般，以１個節點作爲頂點，而將以下的節點設成爲該頂點節點所定義的範疇，或是副範疇的相關節點，藉

五、發明說明 (27)

此，管理範疇段，或是副範疇段之1個頂點節點的製造商，內容提供者等，則會獨自地產生以該節點作爲頂點的有效化密碼區塊（ＥＫＢ），而配送到屬於頂點節點以下的裝置，在完全不影響到屬於不屬於頂點節點之其他範疇之節點的裝置的情形下，可以執行密碼更新。

〔根據簡略ＥＫＢ的密碼配送結構〕

在先前所說明之例如圖3的樹狀結構中，當將密碼，例如內容密碼送到所設定裝置（葉）時，則利用密碼分配對象裝置之擁有的葉密碼、節點密碼，產生可以解碼之有效化密碼區塊（ＥＫＢ）來提供。例如在圖１２（ａ）的樹狀結構中，當將密碼，例如內容密碼送到構成葉(leaf)的裝置ａ、ｇ、ｈ時，則在ａ、ｇ、ｊ的各節點產生可解碼的有效化密碼區塊（ＥＫＢ）來加以配送。

例如考慮根據更新根密碼Ｋ（ｔ）ｒｏｏｔ，對內容密碼Ｋ（ｔ）ｃｏｎ實施編碼處理，而與ＥＫＢ一起加以配送的情形。此時，裝置ａ、ｇ、ｊ則分別利用圖１２（ｂ）所示的葉以及節點密碼來執行ＥＫＢ的處理，而取得Ｋ（ｔ）ｒｏｏｔ，根據所取得的更新根密碼Ｋ（ｔ）ｃｏｎ執行內容密碼Ｋ（ｔ）ｃｏｎ的解碼處理，而取得內容密碼。

此時所提供的有效化密碼區塊（ＥＫＢ）的構成，則如圖１３所示。圖１３所示之有效化密碼區塊（ＥＫＢ），則是根據在先前之圖6中所說明的有效化密碼區塊（

五、發明說明(28)

ＥＫＢ）的格式而構成，具有與資料（編碼化密碼）對應的標籤(tag)。標籤，如先前之圖７所示，若在左（Ｌ）、右（Ｒ）之各方向有資料時爲０，若沒有時則爲１。

收到有效化密碼區塊（ＥＫＢ）的裝置，則根據有效化密碼區塊（ＥＫＢ）的編碼化密碼與標籤，依序執行編碼化密碼的解碼處理，而取得上位節點的更新密碼。如圖１３所示，有效化密碼區塊（ＥＫＢ），當從根到葉爲止的段數（深度）愈多時，則其資料量愈增加。段數（深度）會隨著裝置（葉）的數目而增加，當成爲密碼之配送對象的裝置的數目多時，則ＥＫＢ的資料量會更增加。

以下則針對可以削減該有效化密碼區塊（ＥＫＢ）之資料量的結構來加以說明。圖１４爲將有效化密碼區塊（ＥＫＢ）對應於密碼配送裝置而簡化的結構例。

與圖１３同樣地來推測將密碼，例如內容密碼送到構成葉的裝置ａ、ｇ、ｊ的情形。如圖１４的（ａ）所示，構築出一只由密碼配送裝置所構成的樹狀結構。此時，則根據圖１２（ｂ）所示的結構來構築出圖１４（ｂ）的樹狀結構以作爲新的樹狀結構。也可以從Ｋｒｏｏｔ到Ｋｊ爲止完全沒有分歧，而只存在１條板從Ｋｒｏｏｔ到Ｋａ以及Ｋｇ爲止，只在Ｋ０構出分歧點，而構築出２分歧結構的圖１４（ａ）的樹狀結構。

如圖１４（ａ）所示，產生一只具有Ｋ０作爲節點之經簡化的樹狀結構。用於配送更新密碼的有效化密碼區塊（ＥＫＢ），則根據該些之簡化樹狀結構而被產生。圖

五、發明說明 (29)

１４（ａ）所示的樹狀結構則是一選擇時可對有效化密碼區塊（ＥＫＢ）實施解碼之末端節點或葉設成最下段，而構成２分歧型樹狀結構的路徑，且藉由省略掉不需要的節點而被再構築出來的再構築階層樹狀結構。用來配送更新密碼的有效化密碼區塊（ＥＫＢ），則只根據與該再構築階層樹狀結構的節點或葉對應的密碼而被構成。

在先前之圖１３所示的有效化密碼區塊（ＥＫＢ），雖然是儲存了由從各葉ａ、ｇ、ｊ到Ｋｒｏｏｔ爲止之所有的密碼編碼而成的資料，但經簡化的ＥＫＢ，則只會儲存針對構成已簡化的樹狀結構之節點的編碼化資料。如圖１４（ｂ）所示，標籤乃具有３位元結構。第１以及第２位元具有與圖１３的例子同樣的意義，在左（Ｌ）、右（Ｒ）的各方向，若有資料時爲０，而若沒有時則表示１。第３個位元是一表示編碼化密碼是否被儲存在ＥＫＢ內的位元，當儲存有資料時爲１，而當沒有資料時則爲０。

被提供給資料通訊網、或被儲存在記錄媒體，而提供給裝置（葉）的有效化密碼區塊（ＥＫＢ），則如圖１４（ｂ）所示，若相較於圖１３所示的結構，可以大幅地削減資料量。已收到圖１４所示之有效化密碼區塊（ＥＫＢ）的各裝置，則藉由依序針對在標籤的第３位元儲存了１的部分的資料實施解碼，可以對所定的編碼化密碼進行解碼。例如，裝置ａ會根據葉密碼Ｋａ對編碼化資料Ｅｎｃ（Ｋａ、Ｋ（ｔ）０）實施解碼，而取得節點密碼Ｋ（ｔ）０，根據節點密碼Ｋ（ｔ）０，針對編碼化資料

五、發明說明 (30)

Ｅｎｃ（Ｋ（ｔ）0、Ｋ（ｔ）ｒｏｏｔ實施解碼而取得Ｋ（ｔ）ｒｏｏｔ。裝置ｊ，則根據葉密碼編碼化資料Ｅｎｃ（Ｋｊ、Ｋ（ｔ）ｒｏｏｔ）實施解碼而取得Ｋ（ｔ）ｒｏｏｔ。

如此般，構築出一只由配送對象的裝置所構成之經簡化的新的樹狀結構，只利用構成樹狀結構的葉以及節點的密碼來產生有效化密碼區塊（ＥＫＢ），可以產生資料量少的有效化密碼區塊（ＥＫＢ），而能夠有效率地進行有效化密碼區塊（ＥＫＢ）的資料配送。

此外，經簡化的階層樹狀結構，則特別是對於在後段中所說明之實體單位的ＥＫＢ管理結構最爲有效。實體（entity)是一從構成作爲密碼配送結構之樹狀結構的節點(node)或葉(leaf)所選出之多個節點或葉的集合體區塊。實體(entity)是一根據裝置的種類所設定的集合，或是裝置提供製造商、內容提供者，清賬機關等之管理單位等之具有某個共通點的處理單位、管轄單位，提供服務單位等之各種形態的集合，在１個實體則集合了被分類到某個共同範疇的裝置，例如根據多個實體之頂點節點(subroot)再構築出與上述同樣之經簡化的樹而產生ＥＫＢ，藉此，在屬於所選出之實體的裝置中可產生，配送可以被解碼，且經簡化之有效化密碼區塊（ＥＫＢ）。

此外，該有效化密碼區塊（ＥＫＢ）可以儲存在光碟、ＤＶＤ等的資訊記錄媒體。例如在包含有：由上述編碼密碼資料所構成的資料部，與作爲在編碼密碼資料之階層

五、發明說明 (31)

樹狀結構中之位置識別資料的標籤部在內的有效化密碼區塊，將已儲存有已根據更新節點密碼實施編碼之內容等之訊息資料的資訊記錄媒體提供給各裝置。裝置，則會根據標籤部的識別資料依序抽出包含在有效化密碼區塊（ＥＫＢ）中的編碼密碼資料而加以解碼，取得對內容之解碼爲必要的密碼而利用該內容。當然，也可以經由網際網路(Internet)等的網路來配送有效化密碼區塊（ＥＫＢ）。

〔在具有編碼處理功能之記憶裝置與資料處理裝置之間的資料移動〕

接著，則針對利用藉由應用上述階層樹狀結構的有效化密碼區塊（ＥＫＢ）而被配送之編碼處理密碼的處理結構，以具有編碼處理功能的記憶裝置，例如 Memory Stick（商標）等之記憶卡，與資料再生裝置間的資料移動處理爲中心來加以說明。

圖１５爲可相互間執行內容資料之移動的再再生裝置與具有編碼處理功能之記憶卡等的記憶裝置之詳細構成的方塊圖。

如圖１５所示，記憶裝置３００例如具有主控制模組３１、通訊介面３２、控制模組３３、快閃記憶體３４、以及快閃記憶體管理模組３５。以下則說明各模組。

〔控制模組３３〕

如圖１５所示，控制模組３３例如具有亂數產生單元

五、發明說明 (32)

５０、記憶單元５１、密碼產生／演算單元５２、相互認證單元５３、編碼／解碼單元５４、以及控制單元５５。控制模組３３是一單晶片之編碼處理專用的積體電路，具有多層構造，而內部的記憶單元則爲鋁層等假（dummy）層所挾持。又，控制模組３３，則動作頻率的寬度窄，且爲了不會從外部非法地讀取資料，乃具有耐緩衝性。亂數產生單元５０，當接受到亂數產生指示時，則產生６４位元（８位元組）的亂數。

記憶單元５１例如是一 EEPROM(Electrically Erasable Programmable Read Only Memory）等的不揮發性記憶體，而記憶有對於認證處理爲必要之密碼資料等的各種的資料。圖１６爲被記憶在記憶單元５１之資料的說明圖。如圖１６所示，記憶單元５１乃記憶有認證密碼資料ＩＫ０～ＩＫ３１、裝置識別資料ＩＤｍ以及記憶用密碼資料 Kstm。

認證密碼資料ＩＫ０～ＩＫ３１，則是當記憶裝置３００在與再生裝置２００之間進行相互認證時所使用的密碼資料，如後所述，每次進相互認證時，會隨機地從認證密碼資料ＩＫ０～ＩＫ３１中選出一個認證密碼資料。此外，認證密碼資料ＩＫ０～ＩＫ３１以及記憶用密碼資料 Kstm，則無法從記憶裝置３００的外部被讀取。裝置識別資料ＩＤｍ是一針對記憶裝置３００獨特所賦予的識別資料，如後所述，當記憶裝置３００在與再生裝置２００之間進行相互認證時會被讀取，而被輸出到再生裝

五、發明說明 (33)

置２００。記憶用密碼資料Ｋｓｔｍ，如後所述，對在作內容編碼時所使用的內容密碼資料ＣＫ實施編碼，而在記憶在快閃記憶體３４時被使用。

密碼產生／演算單元５２，例如進行ＩＳＯ／ＩＥＣ９７９７之ＭＡＣ（Message Authentication Code）演算等的各種的演算而產生密碼資料。此時，ＭＡＣ演算則例如利用在ＦＩＰＳＰＵＢ４６－２所規定的ＤＥＳ（Data Encryption Standard)作爲〝Block cipher Algorithm〞。MAC演算是一用於將任意長度的資料壓縮成固定長度之單向性哈習函數演算，函數值則根據秘密密碼來決定。

相互認證單元５３，則在從再生裝置２００輸入音頻資料，進行寫入快閃記憶體３４之動作之前，會在與再生裝置２００之間先進相互認證處理。又，相互認證單元５３，則在從快閃記憶體３４讀取音頻資料，進行輸出到再生裝置２００之動作之前，會在與再生裝置２００之間先進行相互認證處理。又，相互認證單元５３，則在相互認證處理中進行上述ＭＡＣ演算。該相互認證處理則用被記憶在記憶單元５１的資料。

編碼１解碼單元５４，則根據ＤＥＳ、ＩＤＥＡ、ＭＩＳＴＹ等的區塊編碼算法來進行編碼。所使用的模式爲在ＦＩＰＳ　ＰＵＢ　８１〝DES MODES OF OPERATION〞所規定的ＥＣＢ（Electronic Cade Book）模式以及ＣＢＣ（Cipber Block Chaining)模式。又，編碼

五、發明說明 (34)

／解碼單元５４則根據以及ＤＥＳ、ＩＤＥＡ、ＭＩＳＴＹ等之區塊解碼算法進行解碼。所使用的模式爲上述ＥＣＢ模式以及ＣＢＣ模式。該ＥＣＢ模式以及ＣＢＣ模式的區塊編碼／解碼，則利用所指定的密碼資料，對所指定的資料實施編碼／解碼。控制單元５５，則會統括亂數產生單元５０、記憶單元５１、密碼產生／演算單元５２、相互認證單元５３，以及編碼／解碼單元５４的處理來加以控制。

〔快閃記憶體３４〕

快閃記憶體３４例如具有３２Ｍ位元組的記憶容量。在快閃記憶體３４則被寫入有當在相互認證單元５３，根據再生裝置２００與記憶裝置３００之間的相互認證處理爲雙方皆爲合法的裝置時，會從再生裝置２００所輸入的音頻資料或畫像資料等各種資料。又，從快閃記憶體３４，當相互認證單元５３，根據再生裝置２００與記憶裝置３００之間的相互認證處理認爲是合法的對象時，則音頻資料、畫像資料等會被讀取而被輸出到再生裝置２００。

以下則說明被記憶在快閃記憶體３４的資料以及其格式。圖１７爲被記憶在快閃記憶體３４的資料所說明圖。如圖１７所示，在快閃記憶體３４例如記憶有再生管理檔案，多個的軌道資（再生資料）。在此，再生管理檔案具有用來管理軌道資料檔案之再生的管理資料，軌道資料檔案則分別具有對應的軌道資料（音頻資料）。此外，在本

五、發明說明 (35)

實施形態中，軌道資料則例如意味著1個曲子的音頻資料。以下則說明將被記憶在快閃記憶體34的資料當作音頻資料時的例子。

圖18係再生管理檔案的結構，圖19係1個曲子之ATRAC3資料檔案的結構。再生管理檔案是一16KB固定長度的檔案。ATRAC3資料檔案則是曲單位，係由前頭的屬性標題（head）與接下來實際上經編碼的音樂資料所構成。屬性標題也被設成16KB固定長度，而具有與再生管理檔案類似的結構。

再生管理檔案係由標題，1位元組碼之記憶卡的名稱NM1－S、2位元組碼之記憶卡的名稱NM2－S、曲目順序之再生表TRKTBL、以及記憶卡整體的附加資訊INF－S所構成。資料檔案之前頭的屬性標題，則由標題、1位元組碼之曲名NM2、2位元組碼的曲名NM2、軌道之密碼資訊等的軌道資訊TRKINF、段落數（parts）資訊PRTINF、以及軌道之附加資訊INF所構成。標題則包含有總段落數、名稱的屬性、附加資訊的大小的資訊等。

屬性標題接下來即是ATRAC3的音樂資料。音樂資料則被分成16KB的各區塊，而在各區塊的前頭則附加了標題。在標題則包含有用於將密碼加以解碼的初始值。此外，接受編碼處理者，則只有在ATRAC3資料檔案中之音樂資料等的內容資料，至於其他的再生管理檔案、標題等的資料則未被編碼。

五、發明說明 (36)

圖２０爲表示再生管理檔案ＰＢＬＩＳＴ之詳細的資料結構。再生管理檔案ＰＢＬＩＳＴ是１個群集（１區塊＝１６ＫＢ）的大小。圖２０所示的標題是由３２個位元組所構成。圖２０Ｂ所示之標題以外的部分，則再度記錄有針對記憶卡整體的名稱ＮＭＩ－Ｓ（２５６個位元組）、名稱ＮＭ２－Ｓ（５１２個位元組）、經編碼的內容密碼（ＣＯＮＴＥＮＴＳＫＥＹ）、ＭＡＣ、Ｓ－ＹＭＤｈｍｓ、用來管理再生順序的表ＴＲＫＴＢＬ（８００個位元組）、針對記憶卡整體之附加資訊ＩＮＦ－Ｓ（１４７２０個位元組）、以及標題中之資訊的一部分。該些不同種類之資料群的各自的前頭，則被規定成在再生管理檔案內位於所設定之位置。

再生管理檔案，從以圖２０Ａ所示之（０×０００００）以及（０×００１０）所表示的前頭開始數來３２個位元組爲標題。此外，在檔案中，則從前頭開始，將以１６個位元組單位所切成的單位稱爲溝（slot）。在被配置在檔案之第１以及第２溝的標題，則從前頭開始依序配置有具有下列之意義、功能、值的資料。此外，被記成Reserved的資料則表示未定義的資料。通常雖然是寫成（０×００），但即使是如此，Reserved的資料也是被忽視。而在將來的世代，則可以有變更。又，禁此將資料寫入到該部分。連被寫成 Option 之部分未被利用時，也全部視爲保留（Reserved）。

ＢＬＫＩＤ－ＴＬＯ（４個位元組）

五、發明說明 (37)

意義：ＢＬＯＣＫＩＤ　ＦＩＬＥ　ＩＤ

功能：用來識別爲再生管理檔案之前頭的值

值：固定值＝〝ＴＬ＝０〞（例如

０×５４４Ｃ２Ｄ３０）

ＭＣｏｄｅ（２個位元組）

意味：ＭＡＫＥＲ　ＣＯＤＥ

功能：用來識別所記錄之機構之製造商、型號的碼。

值：上位１０個位元（製造商碼）、下位６位元（機種碼）

ＲＥＶＩＳＩＯＮ（４個位元組）

意義：ＰＢＬＩＳＴ的更寫次數

功能：在每次更寫再生管理檔案時則漸增（increment)

值：從０開始每次加１

ＳＮ１Ｃ＋Ｌ（２個位元組）

意義：表示被寫入到ＮＭ１－Ｓ領域之記憶卡之名稱（１個位元組）的屬性

功能：分別以１個位元組來表示所使用的文字碼與語言碼

值：文字碼Ｃ係以上位１個位元組如下述般地來區別文字

００：未設定文字碼，以單純的２進位數來處理

０１：ＡＳＣＩＩ（Amercian Standard Code for Information Interchange

０２：ＡＳＣＩＩ＋ＫＡＮＡ　０３：modified

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明 (38)

8859-1

８１：ＭＳ－ＪＩＳ　８２：ＫＤ　Ｃ　５６０１－１９８９　８３：ＧＢ（Great Britain)2312-80

９０：Ｓ－ＪＩＳ（Japanese Industrial Standard)(for voice)

語言碼（Ｌ）則是以下位１個位元組，如下述般，根據ＥＢＵ　Tech 3258規定來區分語言

００：未作設定　０８:German　０９:English

０Ａ:Spanish　０Ｆ:French　１５:Italian

１Ｄ:Dutch　６５:Korea　０９:Japanese

７５:Chinese

當沒有資料時則全部設爲０

ＳＮ２Ｃ＋Ｌ（２個位元組）

意義：表示被寫入到ＮＭ２－Ｓ領域之記憶卡之名稱（位元組的屬性）

功能：分別以１個位元組來表示所使用的文字碼與語言碼

值：與上述的ＳＮ１Ｃ相同

ＳＯＮＦＳＩＺＥ（２個位元組）

意義：表示由與被寫入到ＩＮＦ－Ｓ領域之記憶卡整體相關的附加資訊的全部合計而成的大小

功能：以１６位元組單位的大小來記述資料大小，當沒有時，則一定全部要設爲０

值：大小爲從０×０００１到）×３９Ｃ（９２４）

五、發明說明 (39)

Ｔ－ＴＲＫ（２個位元組）

定義：ＴＯＴＡＬ　ＴＲＡＣＫ　ＮＵＭＢＥＲ

功能：總軌道數

值：從１開始到０×０１９０（最大４００個軌道），當沒有資料時全部設爲０

ＶｅｒＮｏ（２個位元組）

意義：格式的世代編號

功能：上位爲較大世代（major version）編號，下位爲較小世代（minor version）編號。也可以當作表示是否爲著作權對應型，亦即，表示是否爲根據上述之階層樹狀結構之有效化密碼區塊（ＥＫＢ）來配送密碼之使用對象的資料來使用。

值：例如０×０１００（ｖｅｒ　１．０）

０×０２０３（ｖｅｒ　２．３）

以下說明被寫入到上述標題之接下來的領域的資料（圖２０Ｂ）。

ＮＭ１－Ｓ

意義：與記憶卡整體相關之１個位元組的名稱

功能：以１個位元組的文字碼來表示之可變長度的名稱資料（最大爲２５６）名

要結束前一個資料一定要寫入終端碼（０×００）

大小爲從該終端碼開始計算，當沒有資料時，則至以從開頭（０×００２０）開始記錄１個位元組以上的空白

五、發明說明(40)

（ｎｕｌ）（０×００）

值：各種文字碼

ＮＭ２－Ｓ

意義：與記憶卡整體相關之２位元組的名稱

功能：以２個位元組的文字碼來表示之可變長度的名稱資料（最大爲５１２）名。要結束前一資料一定要寫入終端碼（０×００）

大小爲從該終端碼開始計算，當沒有資料時，則至少從開頭（０×０１２０）開始記錄２個位元組以上的空白（０×００）

值：各種文字碼

ＥＫＢ－vevsion（４個位元組）

意義：表示由上述階層樹狀結構之有效化密碼區塊（ＥＫＢ）所提供之內容密碼的世代編號及／或有效化密碼區塊（ＥＫＢ）的檔案名

功能：表示用來求取由階層樹狀結構之有效化密碼區塊（ＥＫＢ）所提供之內容密碼的有效密碼區塊（ＥＫＢ）

值：從０到０×ＦＦ

Ｅ（Kstm、Kcon）（８個位元組）

意義：根據記憶卡的儲存密碼（storage key）針對作爲各內容之編碼處理用之密碼的內容密碼實施編碼而成的資料

五、發明說明 (41)

功能：被使用在內容之編碼處理

值：從0到0×FFFFFFFFFFFFFFFF

爲止

E（kEkn，Kcon）（8個位元組）

意義：根據由上述層樹狀結構之有效化密碼區塊（EKB）所提供的密碼編碼密碼kEkn，針對作爲各內容之編碼處理用之密碼的內容密碼實施編碼而成的資料

功能：被使用在內容之編碼處理

值：從0到0×FFFFFFFFFFFFFFFF

爲止

C－MAC〔0〕〔8個位元組〕

意義：著作權資訊改善檢查值

功能：是一根據在再生管理檔案內的資料，表示最終內容記錄等之內容處理時間的S－YMDhms等其他的資料所產生之竄改檢查用的值。當時間資；料S－YMDhms被竄改時，則判定爲在檢查C－MAC〔0〕時發現有竄改，而不執行內容的再生。

值：從0到0×FFFFFFFFFFFFFFFF

爲止

MGR：

意義：內容密碼的種類

功能：0×00爲同時具有內容密碼Kcon與E（kEKn，Kcon）兩者，0×01爲只有

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（42 ）

E（kEkn，Kcon）

S－YMDhms（4位元組）（選用）

意義：以具有可信賴的計時器的機器所記錄的年・月・日・時・分・秒

功能：用於識別內容之最終記錄時間等之內容最終處理時間的值。在內容作處理時會被更新

值：25－31位元　年0－99（1980－2079

21－24位元　月0－12

16－20位元　日0－31

11－15位元　時0－23

05－10位元　分0－59

00－04位元　秒0－29（2秒單位）

此外，S－YMDhms，則在作內容記錄時等之內容處理時會被更新，上述的C－MAC〔0〕也會根據被更新的資料而被更新且被儲存。

TRK－nnn

意義：已在再生之ATRAC3資料檔案的SQN（順序）編號

功能：用來記述TRKINF中的FNo

值：從1到400（0×190）

當未存在有軌道時，則全部設爲0

五、發明說明 (43)

ＩＮＦ－Ｓ

意義：與記憶卡整體相關的附加資訊資料（例如照片軌詞、解說等的資訊）

功能：伴隨有標題之可變長度的附加資訊資料

也有多個不同的附加資訊並存的情形，而分別賦予ＩＤ與資料大小、包含有各標題之附加資料資料最小在１６個位元組以上，而以４位元組的整數倍的單位來構成。其詳細的內容請容後述

值：請參照附加資訊資料結構

再生管理檔案的最後的溝（slot），則可被寫入與在標題內的東西相同的ＢＬＫＩＤ－ＴＬＯ、ＭＣｏｄｅ、以及ＲＥＶＩＳＩＯＮ。

民生用音頻機器則有記憶卡在記錄中被拔出，或是電源被切斷的情形。而在回復時，則必須要檢查出發生該些異常的情形。將ＲＥＶＩＳＩＯＮ寫入到區塊的開頭與結尾。在每次更寫該值時，則會＋１。若在區塊的中途發生異常結束情形時，則開頭與結尾之ＲＥＶＩＳＩＯＮ的值不會一致，而能夠檢查出異常結束情形。由於ＲＥＶＩＳＩＯＮ存在有２個，因此，能夠以高的機率檢查出異常結束情形。當檢查出異常結束的情形時，則發出錯誤訊息之顯示等的警告。

又，由於將固定值ＢＬＫＩＤ－ＴＬＯ插入到１個區塊（１６ＫＢ）的開頭部分，因此，當ＦＡＴ被破壞時，爲了修復，可以使用固定值。亦即，只要看各區塊之開端

五、發明說明 (44)

的固定值，即能夠判別檔案的種類。又，該固定值BLKID－TL0，由於是雙重地被記述在區塊的標題以及區塊的終端部分，因此，能夠有信賴性地進行檢查。此外，再生管理檔案PBLIST之同一者也可以雙重地被記錄。

ATRAC3資料檔案，相較於軌道資訊管理檔案，是一相當大的資料量，而針對ATRAC3資料檔案附加區塊編碼BLOCK SERIAL。但是ATRAC3資料檔案，由於通常多數的檔案是存在於記憶卡上，因此，除了以CUNNUM0來區分內容外，若未附加BLOCK SERIAL時，則當發生重複，而FAT被破壞時，則很難使檔案回復。換言之，單一的ATRAC3資料檔案，由於除了是以多個區塊（BLOCK）來構成外，也可能離散地被配置，因此，爲了要判別構成同一ATRAC3資料檔案的BLOCK，除了要利用CONNUM0外，也根據區塊編號BLOCK SERIAL來決定在同一ATRAC3資料檔案內的昇降順序。

同樣地，雖然是未達到破壞FAT的情形，但是當邏輯錯誤而檔案發生問題時，則將製造商碼（MCode）記錄在區塊的開頭與結尾，以特定出所寫入之製造商的機種。

圖20C表示附加資訊資料的結構。在附加資訊的開頭寫入下述的標題。在標題以後則寫入可變長度的資料。

五、發明說明 (45)

ＩＮＦ

意義：ＦＩＥＬＤ　ＩＤ

功能：表示附加資訊資料之開頭的固定值

值：０×６９

ＩＤ

意義：附加資訊密碼碼（Key Code）

功能：表示附加資訊的分類

值：從０到０×ＦＦ

ＳＩＬＥ

意義：個別之附加資訊的大小

功能：雖然資料大小是自由，但一定要是４位元組的整數倍。又，最小要在１６個位元組以上。當資料結束後仍有多餘的部分時，則以空白（０×００）予以去掉。

值：從１６到１４７８４（０×３９Ｃ０）

ＭＣｏｄｅ

意義：ＭＡＫＥＲ　ＣＯＤＥ

功能：用來識別所記錄之機器之製造商、機型的碼

值：上位１０位元（製造商碼）、下位６位元（機種碼）

五、發明說明 (46)

C + L

意義：表示被寫入到從開頭屬來第１２個位元組開始的資料領域內之文字的屬性

功能：分別以１個位元組來表示所使用之文字碼與語言碼

值：與上述的ＳＮＣ＋Ｌ相同

ＤＡＴＡ

意義：個別的附加資訊資料

功能：可變長度資料。在實際資料的開頭則是從第１２個位元組開始，長度（大小）最小是在４個位元組以上，而經常不得不是４個位元組的整數部。

當從資料的最後仍有剩餘時，則以空白（０×００）予以去掉。

值：根據內容個別地被定義

圖２１爲ＡＴＲＡＣ３資料檔案Ａ３Ｄｎｎｎｎ的資料配列的例子。圖２１表示資料檔案之屬性標題（１個區塊），與音樂資料檔案（１個區塊）。圖２１係表該２個區塊（１６×２＝３２Ｋ位元組）之各溝（slot）的開頭的位元組（０×０００００～０×７ＦＦ０）。如圖２２中分離表示般，從屬性標題的開頭算起３２個位元組爲標題，２５６個位元組爲曲名領域ＮＭ１（２５６個位元組），５１２個位元組爲曲名領域ＮＭ２（５１２個位元組）。將下述的資料寫入到屬性標題的標題。

五、發明說明（47 ）

ＢＬＫＩＤ－ＨＤ０（４個位元組）

意義；用於識別係ＡＴＲＡＣ３資料檔案之開頭的值

值：固定值＝〝ＨＤ＝０〞（例如０×４８４４２Ｄ３０）

ＭＣｏｄｅ（２位元組）

意義：ＭＡＫＥＲ　ＣＯＤＥ

功能：用於識別所記錄之機器的製造商、機型的碼

值：上位１０位元（製造商碼）下位６位元（機型碼）

ＢＬＯＣＫ　ＳＥＲＩＡＬ（４個位元組）

意義：針對各軌道所賦予之連續編號

功能：區塊的開頭是從０開始，接下來的區塊逐次＋１即使是被編輯，也不讓值發生變化

值：從０開始到０×ＦＦＦＦＦＦＦＦ

ＮＩＣ＋Ｌ（２個位元組）

意義：表示軌道（曲名）資料（ＮＭ１）的屬性

功能：分別以１個位元組來表示在ＮＭ１中所使用的文字碼與語言碼

值：與ＳＮＩＣ＋Ｌ相同

五、發明說明 (48)

ＮＲＣ＋Ｌ（２個位元組）

意義：表示軌道（曲名）資料（ＮＭ２）的屬性

功能：分別以１個位元組來表示在ＮＭ２中所使用的文字碼與語言碼

值：與ＳＮ１Ｃ＋Ｌ相同

ＩＮＦＳＩＺＥ（２個位元組）

意義：表示將與軌道相關之附加資訊全部合在一起的大小

功能：以１６位元組單位的大小來記述資料大小，當沒有時，則一定全部設成０。

值：大小從０×００００到０×３Ｃ６（９６６）

Ｔ－ＰＲＴ（２個位元組）

意義：全段落（parts）數

功能：表示軌道的段落數。通常爲１

值：從１到０×２８５（６４５ｄｅｃ）

Ｔ－ＳＵ（４個位元組）

意義：全部ＳＵ（Sound Unit)數，ＳＵ爲段落(parts)的最小單位，且是一在以ＡＴＲＡＣ３對音頻資料進行壓縮時之最小的資料單位。ＳＵ爲將以４４．１ＫＨｚ的取樣頻率所得到之１０２４個樣本單位（１０２４×１６位元×２通道）的音頻資料壓縮成約１／１０之數百位元組

五、發明說明(49)

的資料。１ＳＵ換算成時間，大約是２３ｍ秒。通常是由數千個ＳＵ構成１個段落（parts）。當１個群集（cluster）是由４２個的ＳＵ所構成時，則可以以１個群集表示大約１秒的音樂。構成１個軌道之段落（parts）的數目，則會受到附加資訊大小所影響。由於段落數是根據從１個區塊中除去標題，或曲名，附加資訊資料等的數目來決定，因此，以在完全沒有附加資訊的狀態下可以使用最大數目（６４５個）的段落（parts）爲條件。

功能：表示在１個軌道中之實際的總ＳＵ數，相當於曲子的演奏時間

值：從０×０１到０×０００１ＦＦＦＦＦ

ＩＮＸ（２個位元組）（Option）

意義：ＩＮＤＥＸ的相對位置

功能：表示在曲子之特徵部分之開頭的指標。以將ＳＵ的個數設成１／４的數來指定距曲子之開頭的位置。而此則相當於通常ＳＵ之４倍長度的時間（約９３ｍ秒）

值：從０到０×ＦＦＦＦ（最大約６０８４秒）

ＸＴ（２個位元組）

意義：ＩＮＤＥＸ的再生時間

功能：以將從以ＩＮＸ－ｍｍ所指定之開頭開始應再生之時間之ＳＵ的個數設成１／４的數加以指定。而此通常相當於ＳＵ之４倍長度的時間（約９３ｍ秒）

值：０×０００００：無設定　從０×０１到

五、發明說明 (50)

０×ＦＦＦＥ（最大６０８４秒）

０×ＦＦＦＦ：直到曲子結束

接著，則說明曲名領域ＮＭ１以及ＮＭ２。

ＮＭ１

意義：表示曲名的文字列

功能：表示以１個位元組的文字碼來表示之可變長度的曲名（最大爲２５６）

要結束名稱資料一定要寫入終端碼（０×００）

大小則是從該終端碼來計算，當沒有資料時，則至以從開頭（０×００２０）開始記錄１個位元組以上的空白（０×００）。

值：各種文字碼

ＮＭ２

意義：表示曲名的文字列

功能：以２個位元組的文字碼所表示之可變長度的名稱資料（最大爲５１２）

要結束名稱資料則一定要寫入終端碼（０×００）

大小則是從該終端來計算，當沒有資料時，則至以從開頭（０×０１２０）開始記錄２個位元組以上的空白（０×００）

值：各種文字碼

從屬性標題的固定位置（０×３２０）開始，將８０

五、發明說明(51)

個位元組的資料稱爲軌道資訊領域ＴＲＫＩＮＦ，主要則一次管理安全關係，複製控制關係的資訊。圖２３表示ＴＲＫＩＮＦ的部分。針對ＴＲＫＩＮＦ內的資料，根據配置順序說明如下o

ＥＫＩ（１個位元組）

意義：由上述之階層樹狀結構之有效化密碼區塊（ＥＫＢ）所提供的編碼化內容密碼：表示是否有Ｅ（ＫＥＫｎ，Ｋｃｏｎ）。

功能：ｂｉｔ７＝１表示有密碼、ｂｉｔ７＝０表示無密碼，當ｂｉｔ７＝０時，則不參照ＥＫＢ－ｖｅｒｓｉｏｎ、Ｅ（ＫＥＫｎ、Ｋｃｏｎ）。

值：從０到０×ＦＦ爲止

ＥＫＢ－version（４個位元組）

意義：由上述之階層樹狀結構之有效化密碼區塊（ＥＫＢ）所提供之內容密碼之世代編號及／或有效化密碼區塊（ＥＫＢ）的檔案名。

功能：表示用來求取由階層樹狀結構之有效化密碼區塊（ＥＫＢ）所提供之內容密碼的有效化密碼區塊（ＥＫＢ）

Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）（８個位元組）

意義：根據記憶卡的儲存密碼（Ｋｓｔｍ），針對作

五、發明說明 (52)

爲各內容之編碼處理用密碼之內容密碼編碼而成的資料

功能：被使用在內容的編碼處理

值：從０到０×ＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ爲止

Ｃ－ＭＡＣ〔ｎ〕（８個位元組）

意義：著作權資訊改善檢查值

功能：由包含內容累積編號的多個的ＴＲＫＩＮＦ的內容與隱藏順序編號所作成的值。所謂的隱藏順序編號是一被記錄在記憶卡之隱藏領域的順序編號。不是合法之著作權之記錄器（recorder)，則無法讀取隱藏領域。又，著作權合法專用的記錄器，或是已搭載了可讀取記憶卡之應用程式的個人電腦，則可以對隱藏領域進存取。

Ａ（１個位元組）

意義：段落（parts）的屬性

功能：表示在段落內之壓縮模式等的資訊

值：請參照圖２４說明如下

但是Ｎ＝０，１的標準晶片（monoral），ｂｉｔ７爲１，則將副（ｓｕｂ）信號規定爲０，而只將主信號（Ｌ＋Ｒ）之特別的 Joint 模式規定作爲標準晶片。

ｂｉｔ２，１的資訊，則被一般的再生機器忽視也沒有關係。

Ａ的位元０則形成加強(emphasize)的ＯＮ／ＯＦＦ的

五、發明說明 (53)

資訊，位元1則形成再生SKIP或一般再生的資訊，位於2則爲了要區分資料，例如形成音頻資料或FAX等的其他的資料。位元3則未定義。藉由組位元4、5、6，如圖所示般規定ATRAC3的模式資訊。亦即，N爲以該3個位元所表示之模式的值，針對mono（N＝0，1）、LP（N＝2）、SP（N＝4）、EX（N＝5）、HQ（N＝7）的5種的模式分別表示記錄時間（當爲64MB的記憶卡時），資料轉送速率，在1個區塊內的SU數。1個SU的位元組數爲（mono：136個位元組、LP：192個位元組、SP：304個位元組、EX：384個位元組、HQ；512個位元組）。更者，根據位元7來表示ATRAC3（0：Dual，1：Joint）。

以下則使用64MB的記憶卡，針對SP模式的情形加以說明。64MB的記憶卡具有3968個區塊（Block）。在SP模式下，由於1SU爲304個位元組，因此，在1個區塊存在有53個SU。1SU相當於（1024／44100）秒。因此，1個區塊成爲（1024／44100）×53×（3968－16）＝4863秒＝81分

轉送速率成爲（44100／1024）×304×8＝104737bps

LT（1個位元組）

五、發明說明 (54)

意義：再生限制旗標（位元7以及位元6）與安全世代（security version)（位元5－位元0）

功能：表示針對該軌道有限制事項

值：位元7：0＝無限制　　1＝有限制

位元6：0＝期限內　　1＝超出期限

位元5－位元0＝安全世代0（若爲0以外，則設爲禁止再生）

FN0（2個位元組）

意義：檔案編號

功能：在最初被記錄時之軌道編號，且該值用於特定出被記錄在記憶卡內之隱藏領域之MAC計算用的值的位置

值：從1到0×190（400）

MG（D）SERIAL－nnn（16個元位組（upper:8 、Lower:8))

意義：記錄機器之安全區塊（安全IC20）的序號

功能：對各記錄機器全部皆不同之固有的值

值：從0到0×FFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFF爲止

CONNUM（4個位元組）

功能：根據各曲所累積之固有的值，而爲記錄機器之安全區塊所管理。2的32次方則是準備了42億首曲子

五、發明說明 (55)

，而使用於辨識所記錄的曲子

值：從０到０ｘＦＦＦＦＦＦＦＦ

ＹＭＤｈｍｓ－Ｓ（４個位元組）（Option）

意義：附設再生限制之軌道的再生開始日期

功能：允許以ＥＭＤ所指定之再生開始的日期

值：與上述日期的記載相同

ＹＭＤｈｍｓ－Ｅ（４個位元組）（Option）

意義：附設再生限制之軌道之再生結束日期

功能：結束由ＥＭＤ所指定之再生許可的日期

值：與上述日期的記載相同

ＸＣＣ（１個位元組）

意義：以下所說明之ＣＣ的擴充部

功能：控制複製

ＣＴ（１個位元組）（Option）

意義：再生次數

功能：在允許再生的次數內，實際上可以再生的次數，再次再生時則漸減（decrement）

值：０ｘ００～０ｘＦＦ未使用時爲０ｘ００

當ＬＴ的ｂｉｔ７爲１，ＣＴ的值爲００時，則禁止再生

五、發明說明(56)

ＣＣ（１個位元組）

意義：ＣＯＰＹ　ＣＯＮＴＲＯＬ

功能：控制複製

值：如圖２５所示，位元６以及７表示複製控制資訊，位元４以及５表示與高速數位複製有關之複製控制資訊，位元２以及３表示安全區塊認證位準，位元０以及１則未定義

ＣＣ的例子：（ｂｉｔ７，６）、１１：允許無限制的複製、０１：禁止複製、００：允許複製１次、（ｂｉｔ３，２）００：來自類比乃至於數位的錄音、ＭＧ認證位準則設爲０

在來自ＣＤ的數位錄音中，（ｂｉｔ７，６）成爲００、（ｂｉｔ３，２）成爲００

ＣＮ（１個位元組）（Option）

意義：在高速數位複製ＨＳＣＭＳ（High Speed Serial Copy Management System）中的複製許可次數

功能：擴張是複製１次或自由複製的區別，以次數來指定。只有在複製第１代時才有效，而每次複製皆減去。

值：００：禁止複製，從０１到０ｘＦＥ：次數、０ｘＦＦ：次數無限制

接著上述軌道資訊軌道領域ＴＲＫＩＮＦ，則將從０ｘ０３７０開始算起２４個位元組的資料稱爲段落（parts）管理用之段落資訊領域ＰＲＴＩＮＦ，當由多個段落來

五、發明說明(57)

構成１個軌道時，則依時間軸的順序來排列ＰＲＴＩＮＦ。圖２６則表示ＰＲＴＩＮＦ的部分。針對在ＰＲＴＩＮＦ內的資料，根據配置順序說明如下。

ＰＲＴＳＩＺＥ（４個位元組）

意義：段落大小（pargs size）

功能：表示段落的大小。群集：２個位元組（最上位）、開始ＳＵ：１個位元組（上位）、結束ＳＵ：１個位元組（最下位）

值：群集：從１到０×１Ｆ４０（８０００）、開始ＳＵ：從０到０×Ａ０（１６０）、結束ＳＵ：從０到０×Ａ０（１６０）（但是ＳＵ的算法爲０、１、２從０開始）

ＰＲＴＫＥＹ（８個位元組）

意義：用於將段落編碼的值

功能：初始值＝０、編集時根據編集的規則

值：從０到０×ＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ

ＣＯＮＮＵＭ０（４個位元組）

意義：最初所制作之內容累積編號密碼

功能：用於使內容成爲獨特之ＩＤ的角色

值：設成與內容累積編號初始值密碼相同的值

回到圖２１。在ＡＴＲＡＣ３資料檔案的屬性標題中

五、發明說明(58)

，如圖２１所示，乃包含有附加資訊ＩＮＦ。ＩＮＦ爲與軌道相關之附加資訊資料，是一伴隨有標題之可變長度的附加資訊資料。有將多個不同的附加資訊並列的情形，而分別附加ＩＤ與資料大小。包含有各標題的附加資料，最小是在１６個位元組以上，爲４位元組之整數倍的單位。

接著上述的屬性標題則有ＡＲＡＣ３資料檔案之各區塊的資料。如圖２７所示，針對各區塊附加標題（beader）。以下則說明各區塊的資料。

ＢＬＫＩＤ－Ａ３Ｄ（４個位元組）

意義：ＢＬＯＣＫＩＤ　ＦＩＬＥ　ＩＤ

功能：用於識別爲ＡＴＲＡＣ３資料之開頭的值

值：固定值＝〝Ａ３Ｄ〞（例如０×４１３３４４２０）

ＭＣｏｄｅ（２個位元組）

意義：ＭＡＫＥＲ　ＣＯＤＥ

功能：用於識別記錄機器之製造商、機型的碼

值：上位１０位元（製造商碼）　下位６位元（機型碼）

ＣＯＮＮＵＭＯ（４個位元組）

意義：最初所製作之內容累積編號

功能：用於使內容成爲獨特之ＩＤ的角色，即使是被編輯，也不讓值發生變化

五、發明說明 (59)

值：設成與內容累積編號初始值密碼相同的值

BLOCK SERIAL（4個位元組）

意義：針對各軌道的賦予的連續編號

功能：區塊的開頭從0開始，接下來的區塊逐次＋1，即使是被編輯，也不讓值發生變化。

值：從0開始到0×FFFFFFFF

BLOCK－SEED（8個位元組）

意義：用於將1個區塊編碼的1個密碼（Key）

功能：區塊的開頭是一以記錄機器之安全區塊來產生亂數，而接下來的區塊則是＋1的值。當喪失該值時，則在相當於1個區塊的約1秒之期間，爲了要不發出聲音，則在標題與區塊結尾則重覆寫入相同的東西。即使是被編輯，也不讓值發生變化。

值：初期爲8個位元組的亂數

INITIALIZATION VECTOR（8個位元組）

意義：在針對各區塊對ATRAC3資料實施編碼、解碼時爲必要之初始值

功能：區塊的開頭從0開始，接下來的區塊是最後之SU之最後經編號的8個位元組。即使是被編輯，也不讓值發生變化。

五、發明說明 (60)

值：從０到０×ＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ

ＳＵ－ｎｎｎ

意義：音響單元（Sound Unit)的資料

功能：從１０２４個樣本被壓縮的資料，根據壓縮模式所輸出的位元組數並不同。即使是被編輯，也不讓值發生變化（一例則是在ＳＰ模式時，Ｎ＝３８４個位元組）

值：ＡＴＲＡＣ３的資料值

在圖２１中，由於Ｎ＝３８４，因此，將４２個ＳＵ寫入到１個區塊內。又，將１個區塊之開頭的２個溝（４個位元組）設爲標題，而在最後的１個溝（２個位元組），乃呈二層地將ＢＬＫＩＤ－Ａ３Ｄ、MCode CONNOM0、BLOCK SERIAL寫入。因此，１個區塊之剩下來的領域Ｍ位元組則成爲（１６,３８４－３８４×４２－１６×３＝２０８（位元組）。如上述般，８個位元組的ＢＬＯＣＫ　ＳＥＥＤ乃呈二層也被記錄。

在此，被記憶在快閃記憶體３４的資料，如後所述般，則以ＡＴＲＡＣ３方式被壓縮。壓縮的單位爲音響單位ＳＵ。因此，在從記憶裝置３００，將資料讀入再生裝置２００時，則讀取的最小單位成爲該音響單位ＳＵ。音頻資料的壓縮方式，則也可以是ＡＴＲＡＣ３等之ＡＴＲＡＣ方式以外的ＣＯＤＥＣ方式。

區塊種子資料（ＢＬＯＣＫ　ＳＥＥＤ　ＤＡＴＡ）ＢＳ，是一針對各區塊例如產生亂數所產生的資料。

五、發明說明 (61)

〔快閃記憶體管理模組３５〕

快閃記憶體管理模組３５則進行將資料寫入到快閃記憶體３４，或是從快閃記憶體３４讀取資料等的控制。

以下說明圖１５所示之再生裝置２００的構成。再生裝置２００例如具有主控制模組４１、通訊介面４２、控制模組４３、編輯模組４４、壓縮／解壓縮模組４５、揚聲器４６、Ｄ／Ａ轉換器４７以及Ａ／Ｄ轉換器４８。

〔主控制模組４１〕

主控制模組４１則總括地控制再生裝置２００的處理。

〔控制模組４３〕

如圖１５所示，控制模組４３例如具有亂數產生單元６０、記憶單元６１、密碼產生／密碼演算單元６２、相互認證單元６３、編碼／解碼單元６４、以及控制單元６５。控制模組４３、則與控制模組３３同樣地是一單晶片之編碼處理專用的積體電路，具有多層構造，內部的記憶單元則被鋁層等的假(dummy）層所挾持。又，控制模組４３則其動作電壓或動作頻率的寬度狹窄，爲了不會從外部非法地讀取資料，乃具有耐緩衝（damper）性。亂數產生單元６０，當接受到亂數產生指示時，則產生６４位元８位元組）的亂數。記憶單元６１則記憶對認證處理爲

五、發明說明 (62)

必要之各種的資料。

密碼產生／密碼演算單元６２，則進行例如利用ＩＳＯ／ＩＥＣ　９７９７之ＭＡＣ演算方式的演算等的各種的演算來產生密碼資料。此時，〝Block Cipber Algorithm〞則使用在ＦＩＰＳ　ＰＵＢ　４６－２中所規定的ＤＥＳ。

相互認證單元６３，則在進行將例如電腦所輸入的音頻資料輸出到記憶裝置３００之動作之前，先在與記憶裝置３００之間進行相互認證處理。又，相互認證單元６３，則在進行從記憶裝置３００輸入音頻資料之動作之前，先在與記憶裝置３００之間進行相互認證處理。又，相互認證單元６３，則在相互認證處理進行上述的ＭＡＣ演算。在該相互認證處理中，則使用被記憶在記憶單元６１的資料。此外，相互認證單元６３，則因應所需，在進行與在個人電腦（ＰＣ）１００，或網路上的電腦之間進行音頻資料之輸入的動作之前，會先在與個人電腦（ＰＣ）１００，或網路上之電腦之間進行相互認證處理。

編碼／解碼單元６４，如上述般，選擇性地使用由ＦＩＰＳ　ＰＯＢ８１中所規定的ＥＣＢ模式以及ＣＢＣ模式來進行區塊編碼。

編碼／解碼單元６４，則在ＦＩＰＳ８１的模式中選擇性地進行ＣＢＣ模式以及ＣＢＣ模式的解碼。在此，編碼／解碼單元６４，則在ＣＢＣ模式中使用例如５６位元的密碼資料Ｋ，以由６４位元所構成之密碼區塊作爲單位

五、發明說明 (63)

來針對編碼文字進行解碼成一般文字。

控制單元６５則總括地控制亂數產生單元６０、記憶單元６１、密碼產生／密碼演算單元６２、相互認證單元６３，以及編碼／解碼單元６４的處理。

〔編輯模組〕

編輯模組４４，例如如圖１６所示，則根據來自使用者的操作指示來編被記憶在記憶裝置３００之快閃記憶體３４內的軌道資料檔案，而產生新的軌道資料檔案。

〔壓縮／解壓縮模組〕

壓縮／解壓縮模組４５，例如在將由記憶裝置３００所輸入之經編碼的音頻資料解碼後再生之際，則將以ＡＴＲＡＣ３方式所壓的音頻資料加以壓縮，而將該經解壓縮的音頻資料輸出到Ｄ／Ａ轉換器４７。又，在將例如從ＣＤ、ＤＶＤ或ＰＣ１所輸入的音頻資料記憶在記憶裝置３００之際，則以ＡＴＲＡＣ３方式來壓縮該音頻資料。

〔Ｄ／Ａ轉換器４７〕

Ｄ／Ａ轉換器４７可將從壓縮／解壓縮模組４５所輸入之數位形式的音頻資料轉換成類比形式的音頻資料，而將其輸出到揚聲器４６。

五、發明說明 (64)

〔揚聲器４６〕

揚聲器４６會輸出與從Ｄ／Ａ轉換器４７所輸入之音頻資料對應的聲音。

〔Ａ／Ｄ轉換器４８〕

Ａ／Ｄ轉換器４８則將例如從ＣＤ播放器所輸入的類比形式的音頻資料轉換成數位資料，且將其輸出到壓縮／解壓縮模組４５。

〔記憶體４９〕

記憶體４９則例如是ＥＺＰＲＯＭ（例如快閃記憶體），乃儲存有上述的密碼有效化區塊（ＥＫＢ），或根據ＥＫＢ所產生之裝置密碼區塊（ＤＫＢ）等的密碼資料，作爲裝置識別碼的裝置ＩＣ等。

〔針對內容資料之記憶裝置的儲存處理以及再生處理〕

在圖１５所示的再生裝置２００與記憶裝置３００之間，則執行內容資料的移動，亦即，從再生裝置２００，將資料記錄到記憶裝置３００之快閃記憶體３４的處理，更者，則從記憶裝置３００的快閃記憶體３４，執行再生裝置２００的資料再生處理。

以下說明該資料記錄以型再生處理。首先，參照圖２８的流程來說明從再生裝置２００，將資料記錄到記憶裝置３００之快閃記憶體３４的處理。

五、發明說明 (65)

再生裝置以及記憶裝置，則在資料移動前，首先執行步驟Ｓ２７０１、Ｓ２７０２所示之相互認證處理。圖２９表示利用共用密碼編碼方式的相互認證方法（ＩＳＯ／ＩＥＣ　９７９８－２）。在圖２９中，雖然是使用ＤＥＳ作爲共用密碼編碼方式，但只要是共用密碼編碼方式，也可以是其他的方式。在圖２９中，首先Ｂ產生６４位元的亂數Ｒｂ，而將Ｒｂ以及作爲本身之ＩＤ的ＩＤ（ｂ）送到Ａ。接受到此的Ａ，則重新產生６４位元的亂數Ｒａ，而依據Ｒａ、Ｒｂ、ＩＤ（ｂ）的順序，在ＤＥＳ的ＣＢＣ模式下，使用密碼Ｋａｂ對資料實施編碼，且將之送回到Ｂ。此外，密碼Ｋａｂ是一在Ａ以及Ｂ中儲存在各自之記錄元件內，而作爲共用的秘密密碼的密碼。利用ＤＥＳ之ＣＢＣ模式的密碼Ｋａｂ的編碼處理，則在例如使用ＤＥＳ的處理中取初始值與Ｒａ之排他的邏輯和，在ＤＥＳ編碼部中，則利用密碼Ｋａｂ實施編碼而產生編碼文字Ｅ１，接著則取編碼文字Ｅ１與Ｒｂ的排他的邏輯和，而在ＤＥＳ編碼部中利用密碼Ｋａｂ實施編碼而產生編碼文字Ｅ２，更者則取編碼文字Ｅ２與ＩＤ（ｂ）的排他的邏輯和，而在ＤＥＳ編碼部中利用密碼Ｋａｂ實施編碼而產生編碼文字Ｅ３，藉此產生送信資料（Ｔｏｋｅｎ－ＡＢ）。

接受到的Ｂ，則還是將儲存在各自之記憶元件內的密碼Ｋａｂ（認證密碼）當作共用的秘密密碼，針對受信資料實施解碼。受信資料的解碼方法，首先，根據認證密碼

五、發明說明 (66).

Ｋａｂ對編碼文字Ｅ１實施解碼而得到亂數Ｒａ。接著，則根據認證密碼Ｋａｂ對編碼文字Ｅ２實施解碼，而取其結果與Ｅ１之排他的邏輯和而得到Ｒｂ。最後，則根據認證密碼Ｋａｂ對編碼文字Ｅ３實施解碼，取其結果與Ｅ２的排他的邏輯和而得到ＩＤ（ｂ）。在如此所得到之Ｒａ、Ｒｂ、ＩＤ（ｂ）中，Ｒ（ｂ）以及ＩＤ（ｂ）則檢查是否與Ｂ所送出者爲一致。當通過該檢查時，則Ｂ會將Ａ視爲合法者。

接著，Ｂ則產生在認證後才使用的通話密碼（Session key)(Kses)（產生方法爲利用亂數）。此外，則根據Ｒｂ、Ｒａ、Ｋｓｅｓ的順序，在ＤＥＳ的ＣＢＣ模式下利用認證密碼Ｋａｂ實施編碼，且將之送回到Ａ。

接受到此的Ａ，則根據密碼資料Ｋａｂ來對受信資料實施解碼。受信資料的解碼方法，由於與Ｂ的解碼處理相同，因此在此省略詳細說明。在如此所得到的Ｒｂ、Ｒａ、Ｋｓｅｓ中，Ｒｂ以及Ｒａ是用來檢查是否與Ａ所送出者成爲一致。當通過該檢查時，則Ａ會視Ｂ爲合法者。在互相對對手認證後，通話密碼Ｋｓｅｓ會當作用於認證後之秘密通訊的共同密碼來使用。

此外，在檢查受信資料時，在發現非法，不一致時，則當作相互認證失敗而結束處理（在Ｓ２７０３中爲Ｎｏ）。

而當相互認證成立（在Ｓ２７０３中爲Ｙｅｓ）時，則在步驟Ｓ２７０４中，再生裝置會執行內容密碼

五、發明說明 (67)

Ｋｃｏｎ的產生處理。該處理，則利用在圖１５之亂數產生單元６０中所產生的亂數，而在碼產生／密碼演算單元６２中被執行。

接著，在步驟Ｓ２７０５中，（１）利用從有效化密碼（ＥＫＢ）所取得的編碼密碼ＫＥＫ，針對內容密碼Ｋｃｏｎ實施編碼處理，而產生Ｅ（ＫＥＫ、Ｋｃｏｎ）、（２）、根據在認證處理中所產生的通話密碼（Ｋｓｅｓ），針對內容密碼Ｋｃｏｎ實施編碼處理而產生Ｅ（Ｋｓｅｓ、Ｋｃｏｎ），且將其送回到記憶裝置（記憶卡）。

在步驟Ｓ２７０６中，記憶裝置會根據通密碼，針對從再生裝置所收到的Ｅ（Ｋｓｅｓ、Ｋｃｏｎ）實施解碼而取得內容密碼Ｋｃｏｎ，更者，根據事先被儲存在記憶裝置的儲存密碼Ｋｓｔｍ，針對Ｋｃｏｎ實施編碼而產生Ｅ（Ｋｓｔｍ、Ｋｃｏｎ），且將其送到再生裝置。

接著，在再生裝置Ｓ２７０７中，則利用在步驟２７０５中所產生的Ｅ（ＫＥＫ、Ｋｃｏｎ），以及在步驟Ｓ２７０６中從記憶裝置所收到的Ｅ（Ｋｓｔｍ、Ｋｃｏｎ），而產生構成資料檔案（參照圖２１）的軌道資訊領域ＴＲＫＩＮＦ資料，在資料檔案的格式處理後，則將其送到記憶裝置（記憶卡）。

在步驟Ｓ２７０８中，記憶裝置（記憶卡）會將從再生裝置所收到的資料檔案儲存在快閃記憶體。

藉此處理，在資料檔案之軌道資訊領域ＴＲＫＩＮＦ

五、發明說明(68)

資料，則如先前所述之圖２１、圖２３所示般，儲存有利用從有效化密碼區塊（ＥＫＢ）所取得的編碼密碼ＫＥＫ，針對內容密碼Ｋｃｏｎ實施編碼處理而得到的Ｅ（ＫＥＫ、Ｋｃｏｎ），以及根據事先被儲存在記憶裝置的儲存密碼Ｋｓｔｍ，針對內容密碼Ｋｃｏｎ實施編碼之Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）的２個編碼內容密碼。

此外，音樂資料、畫像資料等的編碼處理，則是一可直接將內容密碼Ｋｃｏｎ當作內容的編碼密碼來使用而執行、或是將構成內容的段落（ｐａｒｔｓ），或區塊（ｂｌｏｃｋ）等當作單位，而根據內容密碼與其他的密碼產生資料，而個別地產生各段落單位，或區塊單位之編碼密碼，而進行各段落單位、或區塊單位之編碼處理的構成。

在利用該資料檔案之再生處理中，再生裝置則選擇地應用Ｅ（ＫＥＫ、Ｋｃｏｎ）、與Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）之其中任一者，而取得內容密碼Ｋｃｏｎ。

接著，則參照圖３０的流程圖來說明再生裝置２００針對被儲存在記憶裝置３００之快閃記憶體３４的資料執行讀取處理，亦即，再生處理時的處理。

再生裝置以及記憶裝置，在資料移動之前，首先，執行在步驟Ｓ２９０１、Ｓ２９０２中所示的相互認證處理。該處理則與先前所說明之圖２９的處理相同。當相互認證失敗時在Ｓ２９０３爲Ｎｏ），則結束處理。

當相互認證處理成立（在Ｓ２９０３中爲ＹＥＳ）時

五、發明說明 (69)

，則在步驟Ｓ２９０４中，記憶裝置會對再生裝置送出資料檔案。收到資料檔案的再生裝置，則會檢查在資料檔案中的軌道資訊領域ＴＲＫＩＮＦ資料，而判斷內容密碼（Ｋｃｏｎ）的儲存狀況。該判別處理則是一用來判別是否儲存有根據由密碼有效化區塊（ＥＫＢ）所取得的編碼化密碼ＫＥＫ而被編碼的內容密碼，亦即，Ｅ（ＫＥＫ、Ｋｃｏｎ）的處理。Ｅ（ＫＥＫ、Ｋｃｏｎ）的有無，則可以根據在先前之圖２１、２３所說明之在資料檔案中之軌道資訊領域ＴＲＫＩＮＦ資料的〔ＥＫＩ〕資料來加以判別。

當儲存有Ｅ（ＫＥＫ、Ｋｃｏｎ）時（在步驟Ｓ２９０６中爲ＹＥＳ），則前進到步驟Ｓ２９０７，藉由密碼有效化區塊（ＥＫＢ）的處理而取得編碼密碼ＫＥＫ，根據所取得的編碼ＫＥＫ對Ｅ（ＫＥＫ、Ｋｃｏｎ）實施解碼，而取得內容密碼Ｋｃｏｎ。

當未儲存有Ｅ（ＫＥＫ、Ｋｃｏｎ）時在步驟Ｓ２９０６中爲Ｎｏ），在步驟Ｓ２９０８，則在記憶裝置的控制模組３３，根據儲存密碼Ｋｓｔｍ，針對藉由事先被儲存在記憶裝置之儲存密碼Ｋｓｔｍ而經編碼的Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）實施解碼，更者，則在相互認證處理中，產生根據由再生裝置以及記憶裝置所共有的通話密碼(session key)Ｋｓｅｓ而編碼的資料Ｅ（Ｋｓｅｓ、Ｋｃｏｎ），且將其送到再生裝置。

再生裝置，在步驟Ｓ２９０９中，根據通話密碼

五、發明說明(70)

Ｋｓｅｓ，針對從記憶裝置所收到的Ｅ（Ｋｓｅｓ、Ｋｃｏｎ）實施解碼而取得內容密碼Ｋｃｏｎ。

在步驟Ｓ２９１０中，則根據在步驟Ｓ２９０７，或步驟Ｓ２９０９之其中任一者所取得的內容密碼Ｋｃｏｎ進行編碼密碼的解碼。

如此般，在編碼密碼的再生處理中，再生裝置會利用從有效化密碼區塊（ＥＫＢ）所取得的編碼密碼ＫＥＫ對Ｅ（ＫＥＫ、Ｋｃｏｎ）實施解碼，或是根據由事先被儲存在記憶裝置之儲存密碼Ｋｓｔｍ所編碼的Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）來執行處理，藉由執行任一處理可以取得內容密碼Ｋｃｏｎ。

此外，音樂資料、畫像資料等的解碼處理，則是一可直接將內容密碼Ｋｃｏｎ當作內容的解碼密碼來使用而執行、或是將構成內容的段落（ｐａｒｔｓ），或區塊（ｂｌｏｃｋ）等當作單位，而根據內容密碼與其他的密碼產生資料，而個別地產生各段落單位，或區塊單位之解碼密碼，而進行各段落單位、或區塊單位之解碼處理的構成。

〔已儲存了ＫＥＫ之ＥＫＢ的格式〕

之前雖然利用圖６來說明有效化密碼區塊（ＥＫＢ）之概略的格式，但以下則說明在將密碼編碼密碼（ＫＥＫ）儲存在有效化密碼區塊（ＥＫＢ）時之具體的資料結構

五、發明說明(71)

的例子。

圖３１係表示作爲將密碼編碼密碼（ＫＥＫ）儲存在有效化密碼區塊（ＥＫＢ）之資料之ＥＫＢ的配送密碼許可資訊檔案的構成例。裝置（再生裝置）則從該檔案因應所需而取出密碼編碼密碼（ＫＥＫ），根據，ＫＥＫ對Ｅ（ＫＥＫ、Ｋｃｏｎ）進行解碼，而取得內容密碼：Ｋｃｏｎ來執行內容的解碼。以下說明各資料。

ＢＬＫＩＤ－ＥＫＢ（４個位元組）

意義：ＢＬＯＣＫＩＤ　ＦＩＬＥ　ＩＤ

功能：用於識別是否是配送密碼資訊檔案之開頭的值

值：固定值＝〝ＥＫＢ〞（例如０×４５４Ｂ４２２０）

ＭＣｏｄｅ（２個位元組）

意義：ＭＡＫＥＲ　ＣＯＤＥ

功能：用於識別記錄機器之製造商、機型的碼

值：上位１０位元（製造商碼）、下位６位元（機型碼）

ＬＫＦ

意義：ＬＩＮＫ　ＦＩＬＥ　ＩＮＦＯＲＭＡＴＩＯＮ

功能：用於識別作爲由該ＥＫＢ所取得之ＫＥＥ而應

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明 (72)

用之內容資料的連結檔案

值：0～0×FF

bit7：再生管理檔案（PBLIST） 使用：1、未使用：0

bit6：竄改檢查值（ICV） 使用：1、未使用：0

bit5～0：保留

LINK Cont

意義：LINK COUNT

功能：作連結之檔案（例如ATRACK3檔案）數

值：0～0×FFFFFFFF

Version

意義：VERSION

功能：表示配送密碼允許資訊檔案的世代

值：0～0×FFFFFFFF

EA

意義：Encryption Algorithm

功能：表示配送密碼允許資訊檔案之追蹤（trace）處理算法

值：0～0×FF

00h：3DES：根據3種（triple）DES模式

五、發明說明 (73)

的處理

０１ｈ：ＤＥＳ：根據單種ＤＥＳ模式的處理

此外，根據３ＤＥＳ模式的處理是一利用２種以上之編碼處理的編碼處理，而ＤＥＳ模式是一利用１個密碼的處理。

ＫＥＫ１

意義：Key Encrypting Key

功能：根據密碼有效化區塊（ＥＫＢ）中之根據密碼（最上位）密碼而經編碼的內容密碼編碼密碼

值：０～０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ

ＫＥＫ２

意義：Key Encrypting Key

功能：根據密碼有效化區塊（ＥＫＢ）中之根據密碼（最上位）密碼而經編碼的內容密碼編碼密碼

值：０～０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ

Ｅ（Version)

意義：Encyrpted Version

功能：根據密碼有效化區塊（ＥＫＢ）中之根密碼（最上位）密碼而經編碼的世代編號。在解碼時的下４個位元組則保留。

值：０～０ｘＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明 (74)

Size of tag part

意義：Size of tag part

功能：構成配送密碼允許資料檔案之資料的Tag（標籤）部分的大小(Byte)

值：0～0×FFFFFFFF

Size of Key part

意義：Size of Key part

功能：構成配送密碼允許資訊檔案之資料之Key（密碼）部分的大小(Byte)

值：0～0×FFFFFFFF

Size of Sign part

意義：Size of Sign part

功能：構成配送密碼允許資訊檔案之資料之Sign（簽名）部分的大小(Byte)

值：0～0×FFFFFFFF

Tag part

意義：Tag part

功能：構成配送密碼允許資訊檔案之資料之Tag（標籤）部分的值

值：全部的值，當未滿8位元組時，則填入0而設成

五、發明說明(75)

8位元組

Key part

意義：Key part

功能：配送密碼允許資訊檔案之資料之Key（密碼）部分的資料

值：全部的值

Signature part

功能：構成配送密碼允許資料檔案之資料之簽名（Signature)段落的資料

值：全部的值

如上述之說明以及圖31所示，在被提供給裝置之配送密碼允許資訊檔案，則儲存有用來識別作爲能應用從該配送密碼資訊檔案所取得之KEK之內容資料之連結檔案的識別資料〔LKF〕，更者，則儲存有作爲在連結之檔案（例如ATRACK3檔案）數的資料〔Link Count〕。再生裝置則參照〔LKF〕、〔Link Count〕，即可以知道是否存在有可應用從該配送密碼允許資訊檔案所取得之KEK的資料以及其數目。

〔利用連結資訊之資料解碼、再生處理〕

以下則說明利用用於識別包含在上述配送密碼允許資訊檔案之連結檔案的識別資料〔LKF〕、作爲正在連結

五、發明說明(76)

之檔案（例如ＡＴＲＡＣＫ３檔案）數之資料〔LinK Count〕，有效率地執行資料的解碼，再生的處理形態。

圖３２係表被儲存在記憶裝置之資料儲存領域，例如圖１５所示之記憶裝置３００之快閃記憶體３４的資料檔案結構例。在此，雖然只表示音樂資料（ＨＩＦＩ）的目錄（directory）結構，但也可以存在畫像檔案等的目錄。

在圖３２所示之音樂資料的目錄，則包含有再生管理檔案（ＰＢＬＩＳＴ），作爲編碼內容之多個的ＡＴＲＡＣＫ３資料檔案（Ａ３Ｄ）。更者，在記憶裝置則儲存有多個的有效化密碼區塊檔案（ＥＫＢｎ）。用來取得應用在ＡＴＲＡＣＫ３資料檔案（Ａ３Ｄ）之解碼處理中之內容密碼的有效化密碼區塊（ＥＫＢｎ），則可以根據ＡＴＲＡＣＫ３資料檔案（Ａ３Ｄ）中的指標來判別。如圖３２所示，１個有效化密碼區塊檔案（ＥＫＢ１）３１０１則被應用在多個（３個）ＡＴＲＡＣＫ３資料檔案（Ａ３Ｄ）的解碼處理上。

此時，則在與有效化密碼區塊檔案（ＥＫＢ１）３１０１對應之配送密碼允許資訊檔案的〔LinK Count〕，儲存有表示可應用在３個內容（Content)的資料。

圖３３即表示從作爲儲存了圖３２所示之多個的內容檔案，多個的有效化密碼區塊檔案之記憶裝置的記憶卡，針對內容實施解碼而再生時的處理流程。

圖３３的處理是一在將例如作爲記憶裝置之記憶卡設置在再生裝置時，或是將已安裝有記憶卡之再生裝置的電

五、發明說明 (77)

源設爲ＯＮ時，由再生裝置所執行的處理。

首先，在步驟Ｓ３２０１中，再生裝置會讀取各個ＥＫＢ檔案的軌道資訊，而檢查〔LinK Count]。更者，則從[Link Count]之計數多者開始依序選擇事先所決定之個數〔ｎ〕的ＥＫＢ檔案。個數〔ｎ〕則設定爲相當於可儲存在再生裝置之所定記憶領域，亦即，用來儲存保持密碼編碼密碼：ＫＥＫ之領域之個數的個數。

接著，在步驟Ｓ３２０２中，根據的選擇之ＥＫＢ的處理來取得多個〔ｎ〕的密碼編碼密碼：ＫＥＫ，而將該些儲存在設定成作爲再生裝置之密碼儲存領域之ＲＡＭ的所定領域。

接著，再生裝置，在步驟Ｓ３２０３中，則選擇要進行解碼、再生的內容。更者，在步驟Ｓ３２０４中，則判斷應用在該選擇內容之解碼上的ＫＥＫ是否被儲存在ＲＡＭ，當爲Ｙｅｓ時，則前進到步驟Ｓ３２０５，根據該對應的ＫＥＫ，針對Ｅ（ＫＥＫ、Ｋｃｏｎ）實施解碼而取得內容密碼，在步驟Ｓ３２０９中，則執行再生、亦即，根據所取得的內容密碼實施資料的解碼、再生處理。

在步驟Ｓ３２０４中，當應用在選擇內容之解碼上的ＫＥＫ未被儲存在ＲＡＭ時，則在步驟Ｓ３２０６中判定有無存在根據儲存密碼而被編碼的內容密碼，亦即，Ｅ（Ｋｓｔｍ、Ｋｃｏｎ），當存在時，則藉由Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）的解碼處理而取得內容密碼，而在步驟Ｓ３２０９中執行再生、亦即，根據所取得的內

五、發明說明(78)

容密碼來執行資料的解碼，再生處理。

此外，在步驟Ｓ３２０６中，當判定爲沒有Ｅ（Ｋｓｔｍ、Ｋｃｏｎ）時，則從記憶裝置取得要應用在該解碼對象內容之ＥＫＢ，而根據所取得的ＥＫＢ的解碼處理而取得ＫＥＫ，根據所取得的ＫＥＫ執行Ｅ（ＫＥＫ、Ｋｃｏｎ）的解碼處理，而取得內容密碼，在步驟Ｓ３２０９中執行再生，亦即，根據所取得之內容密碼進行資料的解碼再生裝置。

如此般，再生裝置則檢查事先儲存在記憶裝置之多個的密碼有效化區塊（ＥＫＢ）的〔ＬｉｎＫ　Ｃｏｕｎｔ〕，而針對〔ＬｉｎＫ　Ｃｏｕｎｔ〕的計數值多的ＥＫＢ進行解碼，而儲存密碼編碼密碼：ＫＥＫ，藉此，在作內容再生處理時，可以以高的機率來使用儲存在ＲＡＭ的ＫＥＫ，而有效率地執行內容的再生。

〔根據密碼有效化區塊（ＥＫＢ）來配送認證密碼〕

以下則說明在配送使用上述之有效化密碼區塊（ＥＫＢ）的密碼時，藉由配送在執行認證處理時所使用的認證密碼ＩＫｎ，來提供作爲安全之秘密密碼之共用的認證密碼，而根據共用密碼方式來執行認證處理。

利用共用密碼編碼方式的相同認證方法（ＩＳＯ／ＩＥＣ　９７８２－２），則是先前一利用圖２９來說明的處理，作爲執行資料收發的前處理，則是執行用來確認雙方之正常性的處理。在認證處理中，則進行資料收發之

五、發明說明 (79)

例如再生裝置與記憶裝置會共用認證密碼Ｋａｂ。該共用密碼Ｋａｂ則使用上述的有效化密碼區塊（ＥＫＢ），且將其配送到再生裝置。

圖３４以及圖３５則表示藉由有效化密碼區塊（ＥＫＢ），將共用的認證密碼ＩＫｎ配送到多個裝置的構成例。圖３４爲將可以解碼的認證密碼ＩＫｎ配送到裝置０、１、２、３的例子，圖３５表示排除裝置０、１、２、３中的裝置３，而只將可以解碼的認證密碼配送到裝置０、１、２的例子。

在圖３４的例子中，除了根據更新節點密碼Ｋ（ｔ）００，而將認證密碼ＩＫｎ編碼而成的資料（ｂ）外，在裝置０、１、２、３中，則產生可針對利用各自所擁有之節點密碼、葉密碼而被更新的節點密碼Ｋ（ｔ）００實施解碼的有效化密碼區塊（ＥＫＢ）而加以配送。各自的裝置，則如圖３４的右側所示，首先藉由對ＥＫＢ實施處理（解碼），而取得經更新的節點密碼Ｋ（ｔ）００，接著，則針對利用所取得的節點密碼Ｋ（ｔ）００而經編碼的認證密碼：Ｅｎｃ（Ｋ（ｔ）００，ＩＫｎ）而得到認證密碼ＩＫｎ。

其他的裝置４、５、６、７，則即使是收到同一個的有效化密碼區塊（ＥＫＢ），由於在本身所擁有的節點密碼、葉密碼，由於無法取得藉處理ＥＫＢ而被更新的節點密碼Ｋ（ｔ）００，因此，只可以將認證密碼送到安全且

五、發明說明（80 ）

合法的裝置。

另一方面，圖３５的例子，裝置3例如因爲洩漏密碼而遭到排除，而只產生只能對其他群的成員，例如裝置０、１、２實施解碼之有效化密碼區塊（ＥＫＢ）而加以配送的例子。將圖３５所示之（ａ）有效化密碼區塊（ＥＫＢ），與認證密碼（ＩＫｎ）根據節點密碼（Ｋ（ｔ）００）而經編碼的資料加以配送。

圖３５的右側則表示解碼順序。裝置０、１、２，首先，從所收到之有效化密碼區塊，利用本身所擁有的葉密碼或節點密碼來實施解碼處理而取得更新節點密碼Ｋ（ｔ）００。接著，則根據Ｋ（ｔ）００來解碼而取得認證密碼ＩＫｎ。

其他群的裝置，例如裝置４、５、６，即使是收到該同樣的資料（ＥＫＢ），也無法利用本身所擁有的葉密碼、節點密碼來取得更新節點密碼Ｋ（ｔ）００。同樣地，即使是被排除的裝置３，本身所擁有的葉密碼、節點密碼，則無法取得更新節點密碼（Ｋ（ｔ）００），而只有具有合法的權利的裝置才能夠對認證密碼實施解碼來加以利用。

如此般，若利用ＥＫＢ來配送認證密碼，可以減少資料量，且可以安全地配送出只有合法權利者才可以進行解碼的認證密碼。又，藉由有效化密碼區塊（ＥＫＢ）而被編碼所提供的ＥＫＢ配送認證密碼，則進行世代（evsion）管理，針對每個世代進行更新處理，而在任意的時間可以

五、發明說明(81)

排除裝置。

根據上述ＥＫＢ提供認證密碼的處理而被排除的裝置（再生裝置），則其與記憶裝置（例如記憶卡）的認證處理不會成立，而不可能對資料進行非法的解碼。

更著，若是利用ＥＫＢ來配送認證密碼，則也可以針對記憶卡以外的記憶媒體，例如內藏在再生裝置之硬碟等的記憶媒體進行資料儲存、再生處理的控制。

如利用先前的圖２８～圖３０所說明般，在利用記憶裝置進行內容的記錄・再生處理時，則執行相互認證處理，而以相互認證處理成立爲條件，而來進行資料的記錄以及再生。該認證處理程式，雖然對於在與如記憶卡般之可進行相互認證處理之記憶裝置之間的處理中可以有效地作用，但是對於再生裝置爲硬碟、ＣＤ－Ｒ等不具有編碼處理功能，亦即，不能執行相互認證的記憶媒體，則在作資料儲存、資料再生時並不有意義。但是在本發明中，則是一即使是利用不能認證的機器來進行資料儲存，或資料再生處理時，也能夠執行認證處理程式的構成。由於硬碟、ＣＤ－Ｒ等不可能進行相互認證，因此，將假想的記憶卡（Memory Stick)構成爲再生裝置，而在假想記憶卡與再生裝置之間執行認證處理，以認證成立作爲條件，可以針對未具有認證功能的記憶媒體進行資料儲存處理，或是從記錄媒體來再生資料。

圖３６表示使用該些假想記憶卡之資料記錄，再生處理流程。首先，再生裝置會在與再生裝置內之假想記憶卡

五、發明說明（82 ）

之間執行相互認證處理。在步驟Ｓ３５０２中判定認證是否成立，以成立作爲條件而前進到步驟Ｓ３５０３，而利用未具有認證功能的記錄媒體，例如硬碟、ＣＤ－Ｒ、ＤＶＤ等來執行資料記錄、再生處理。

在步驟Ｓ３５０２中，當判定爲認證不成立時，則無法利用步驟Ｓ３５０３之未有認證處理的記錄媒體，例如硬碟、ＣＤ－Ｒ、ＤＶＤ等來執行資料記錄、再生處理。

在此，則事先將在先前之圖１６中所說明之認證資料儲存在假想記憶卡，而如上所述般，由密碼有效化區塊來提供再生裝置所使用的認證密碼。

如此般，藉著由密碼有效化區塊（ＥＫＢ）來提供再生裝置的認證密碼，可只將能與假想記憶卡進行相互認證之認證密碼配送給擁有合法授權的裝置（再生裝置）。因此，可進行不會將有效的認證密碼送到非法的機器，亦即，被排除的再生裝置的處理。未被提供有效的認證密碼的再生裝置，則相互認證會不成立，不只是擁有認證功能的記憶卡，連利用未具有認證功能的記錄媒體，例如硬碟、ＣＤ－Ｒ、ＤＶＤ等也無法執行資料記錄、再生處理，而能夠排除非法的機器進行資料記錄、再生。

亦即，在由提供認證密碼的有效化密碼區塊（ＥＫＢ）構成密碼樹（Key tree）的葉（leaf）的資料處理裝置中，乃提供一只有在擁有合法授權的資料處理裝置中才可進行解碼，而在未擁有合法授權的非法的資料處理裝置中，則無法進行解碼的有效化密碼區塊（ＥＫＢ），以防止

五、發明說明（83 ）

在非法的資料處理裝置中與假想記憶體裝置的認證成立，而實現一具有可排除非法的資料處理裝置利用內容之構成的授權系統。

〔檢查值（ICV:Integrity Check Value）儲存構成〕

接著則說明爲要要竄改內容，乃產生一內容的Integrity・Check值（ＩＣＶ），對應於內容，根據ＩＣＶ的計算來判定有無竄改內容的處理構成。

內容的Integrity・Check值（ＩＶＣ），則例如利用對內容的hash函數來計算，根據ＩＣＶ＝hash（Kicv、Ｃ１、Ｃ２，……）來計算。Ｋｉｃｖ爲ＣＩＶ產生密碼，Ｃ１、Ｃ２爲內容的資訊，乃使用內容之重要資訊的訊息認證（ＭＡＣ：Message authentication Code）。如上所述，〔ＭＡＣ〕也包含於圖２１中所說明之ＡＴＲＡＣ３資料檔案。使用該些來計算Integrity・Check值（ＩＣＶ）。

圖３９表示利用ＤＥＳ編碼處理構成的ＭＡＣ值產生例。如圖３７之構成所示，將成爲對象的訊息分割成８位元組單位（以下將所分割的訊息設爲Ｍ１、Ｍ２、……、ＭＮ）。首先取初始值（Initial Value)（以下稱爲ＩＶ）與Ｍ１的排他性的邏輯和（將其結果設爲Ｉ１）。接著，則將Ｉ１輸入ＤＥＳ編碼部，利用密碼（以下稱爲Ｋ１）而實施編碼（將輸出設爲Ｅ１）。接著則取Ｅ１以及Ｅ２的排他的邏輯和，將其輸出Ｉ２輸入到ＤＥＳ編碼部，利

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明（84）

用密碼Ｋ１來實施編碼（輸出Ｅ２）。以下，則反覆該過程直到對全部的訊息實施完編碼處理。最後出來的ＥＮ則成爲訊息認證碼（ＭＡＣ（Message Authentication Code））。此外，訊息可以使用構成成爲檢查對象的內容以及標題資訊等之內容相關資料的部分資料。

將nash函數應用在該內容的ＭＡＣ值與ＩＣＶ產生密碼Ｋｉｃｖ，而產生內容之Integrity・Check值（ＩＣＶ）。比較已保證沒有竄改之例如在產生內容時所產生的ＩＣＶ，與重新根據內容所產生的ＩＣＶ，若是得到相同的ＩＣＶ，則保證內容沒有竄改，若ＩＣＶ不同時，則判定爲竄改。

上述之Integrity・Check值（ＩＣＶ），則根據針對各內容所產生之多個的內容ＭＡＣ，而產生１個的Integrity・Check值（ＩＣＶ）。根據多個的ＭＡＣ所進行之ＩＣＶ的計算，則例如藉由

ＩＣＶ＝ＭＡＣ（Ｋｉｃｖ、Ｃ＿ＭＡＣ〔０〕１１Ｃ＿ＭＡＣ〔１〕１１Ｃ＿ＭＡＣ〔２〕１１……）而產生。

儲存在產生內容時所產生的ＩＣＶ，而在作檢查處理時，則進行產生ＩＣＶ與儲存ＩＣＶ的比較處理。當２個ＩＣＶ爲一致時，則判定爲無竄改，而當ＩＣＶ爲不一致時，則判定爲竄改，而限制資料再生等的處理。

在記憶卡等的記憶裝置，則不只是音樂內容，也儲存有畫像資料、遊戲程式資料等之不同領域的內容。爲了要防止各領域的內容遭到竄改，則針對各領域產生Integrity

五、發明說明（85 ）

・Check 值（ＩＣＶ）而加以儲存是一檢查內容是否遭受竄改的有效的手段。

然而，當儲存在記憶體的內容數增加時，則很難根據正規的內容資料來產生、儲存、以及管理檢查用的檢查值。特別是對於使用快閃記憶體之記憶卡等之容量大的媒體而言，則是將音樂資料、畫像資料、程式資料等之各種領域的內容資料儲存在記憶體內。在此環境下，則檢查值的產生處理、儲存處理、竄改檢查處理的管理會變得困難。當產生針對整個儲存資料的檢查值時，則必須要執行針對成爲檢查對象之資料整體的檢查值產生處理。當根據在ＤＥＳ－ＣＢＣ模式中所產生的訊息認證碼（ＭＡＣ）來求取檢查值ＩＣＶ時，則必須要執行針對資料整體之ＤＥＳ－ＣＢＣ的處理。該計算量則會隨著資料長度變而增加，在處理效率方面會有問題。

在可當作記憶裝置來使用的記憶卡則儲存了許多領域之不同的內容。藉由將該些領域之不同內容之竄改檢查管理設成爲一針對各領域產生獨立的 Integrity・Value 值（ＩＣＶ）而執行的構成，則在ＩＣＶ的檢查時，或ＩＣＶ的變更時，例如在資料變更時之新的 Integrity・Check 值（ＩＣＶ）的產生處理，可將在 1 個領域內的資料當作對象來執行，而不會影響到其他的領域。以下則說明用來儲存針對各領域之多個的 Integrity・Check 值（ＩＣＶ）的構成。

圖３８表示被儲存在記憶裝置之資料結構，以及各自

五、發明說明（86）

方 Integrity・Check 值（ＣＩＶ）的儲存構成例。在記憶卡等的記憶部（快閃記憶體），則如圖３８所示，在音樂資料的目錄包含有再生管理檔案（ＰＢＬＩＳＴ），作爲編碼內容之多個的ＡＴＲＡＣＫ３資料檔案（Ａ３Ｄ），更者，則在記憶體儲存屬於多個領域的內容資料（＃１～＃ｎ）。所謂的領域是指例如音樂資料、畫像資料、遊戲程式等。更者，即使是同樣的畫像資料，也可以針對各自的資料提供來源，當作另外的目錄，或獨立的領域來加以管理。

又，也可以將上述之有效化密碼區塊（ＥＫＢ）的管理單位（實體 entity）設定作爲１個領域。亦即，可將能應用根據某個有效化密碼區塊（ＥＫＢ）所取得的密碼編碼密碼：ＫＥＫ而經解碼的內容密碼Ｋｃｏｎ的內容集合設定作爲１個的領域。

再生管理檔案（ＰＢＬＩＳＴ）、作爲編碼內容之多個的ＡＴＲＡＣＫ３資料檔案（Ａ３Ｄ）則分別包含有用於檢查竄改的訊息認證碼（ＭＡＣ（Message Authentication Code）），根據該些值而產生 Integrity・Check 值（ＩＣＶ（ｃｏｎ））。多個的內容的ＭＡＣ值，則當作ＭＡＣ表被儲存在快閃記憶體之循序表（sequence list）而加以管理，且儲存保存根據該些的ＭＡＣ表，而應用ＩＣＶ產生密碼Ｋｉｃｖ所得到的 Integrity・Check 值（ＩＣＶ（ｃｏｎ））。

圖３９則表示用於儲存內容ＭＡＣ值的循序頁格式（

五、發明說明(87)

Sequence Page List)。循序頁領域是一被設定作爲一般內容資料禁止寫入領域的領域。以下則說明圖３９之循序頁結構。

Ｅ(ＫＳＴＲ、Ｋｃｏｎ)爲根據記憶卡的儲存密碼而經編碼的內容密碼。ＩＤ(upper)、(lower)爲記憶卡之識別碼(ＩＤ)的儲存領域。Ｃ＿ＭＡＣ〔０〕爲根據再生管理檔案(ＰＢＬＩＳＴ)的構成資料所產生的ＭＡＣ值。Ｃ＿ＭＡＣ〔１〕爲根據內容，例如ＡＴＲＡＣＫ３資料檔案＃１的資料所產生的ＭＡＣ值，以下，則針對各內容儲存ＭＡＣ值。根據該些的ＭＡＣ值而產生 Integrity・Check 值(ＩＣＶ(ｃｏｎ))，而所產生的ＩＶＣ(ｃｏｎ)則根據串列協定(serial protocol)而被寫入到記憶體。此外，爲了要因應不同的密碼系統，則最好分別將由各自密碼系統所產生的ＩＣＶ儲存在不同之區域(area)。

又，針對各範疇(category)所產生用來檢查竄改之各範疇的 Integrity・Check 值(ＩＣＶ)，則被記錄在記憶卡的記憶部(快閃記憶體)的輪詢頁(poll page)。該輪詢頁也被設定作爲一般資料之禁止寫入領域。

圖４０則表示用來儲存各範疇之 Integrity・Check 值(ＩＣＶ的 pool page 格式。０＿revision 則被設定領域＃０的更新資料，當被更新時則被漸增(increment)。０＿version 表示爲範疇＃０的世代(version)、＃０＿Ｅ(ＫＥＫ、Ｋｉｃｖ)爲根據範疇＃０的密碼編碼密碼(

五、發明說明（88）

ＫＥＫ）而經編碼的ＩＣＶ產生密碼（Ｋｉｃｖ）、ＩＣＶＯ爲範疇＃０之 Integrity・Check 值（ＩＣＶ）。以下，同樣的資料，則針對各範疇儲存到ＥＫＢ＃１５爲止。

ＩＣＶ的檢查，則是以電源接通時，或是將記憶卡等的記憶裝置設置在再生裝置爲條件而開始。圖４１則表示包含ＩＣＶ檢查在內的處理流程。

又，當檢測到再生裝置的電源接通，或是已安裝好新的記憶卡等時，則在步驟Ｓ４００１中判定在再生裝置與記憶裝置之間是否可以進行相互認證，當可以時，則在步驟Ｓ４００２中執行記憶裝置與再生裝置的相互認證處理（參照圖２９）。又，在步驟Ｓ４００１中，當判定爲在再生裝置與記憶裝置之間不能進行相互認證時，則在步驟Ｓ４００３中執行上述假想記憶卡與再生裝置之間的相互認證處理。

在步驟Ｓ４００４中，則判定相互認證是否成立，當不成立時，則不執行以下的處理而直接結束。當相互認證成立時，則在步驟Ｓ４００５中執行ＩＣＶ的計算。ＩＣＶ，如上所述，係根據各檔案的ＭＡＣ值被算出。

接著，在步驟Ｓ４００６中，則將藉由試算所出的產生ＩＣＶ，與事先所儲存之儲存ＩＣＶ進行比較。當２個ＩＣＶ爲一致時，則判定爲沒有竄改資料，而在步驟Ｓ４００７中執行資料再生等之各種的處理。另一方面，當ＩＣＶ爲不一致時，則判定爲資料遭到竄改，而不進行

五、發明說明（89 ）

資料的再生等即直接結束處理。藉由執行該處理，可以防止竄改資料，以及排除遭到竄改的資料被再生。

如此般，針對領域之不同的內容產生針對各範疇爲獨立的 Integrity・Check 值（ＩＣＶ）而加以管理，藉此，在作ＩＣＶ的檢查時，或ＩＣＶ的變更時，例如資料變更時之新的 Integrity・Check 值（ＩＣＶ）的產生處理，則以在１個範疇內的資料作爲對象來執行，而不致於影響到其他的領域。

〔擴充ＭＡＣ結構〕

以下則針對在上述之再生管理檔案，或ＡＴＲＡＣＫ３資料檔案之資料內容欄中所說明之資料竄改檢查用的ＭＡＣ(Message Authentication Code）的產生，以及針對各檔案之儲存處理的變形例，亦即，擴充ＭＡＣ的產生、儲存處理來加以說明。

圖４２表示擴充ＭＡＣ的產生、儲存處理例。圖４２則表示在先前之圖２１～圖２３所示之ＡＴＲＡＣＫ３資料檔案的一部分。資料竄改檢查用的ＭＡＣ（Message Authentication Code），則是一根據在例如ＡＴＲＡＣＫ３的資料檔案中之數個資料項目的資料，藉由在先前之圖３７所說明之處理所產生的值，藉由比較事先被儲存在檔案的ＭＡＣ、與在檢查時的產生ＭＡＣ，而判定有無竄改資料。

例如，被儲存在圖４２所示之ＡＴＲＡＣＫ３資料檔

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（90 ）

案的ＭＡＣ，則將該ＭＡＣ之竄改檢查對象資料設定在「ＩＮＦ－Ｓｅｑ＃」之多個的資料項目，而事先根據該些之ＭＡＣ對象資料項目所產生的ＭＡＣ則被儲存在檔案內。亦即，爲ＭＡＣ（ＩＮＦ－Ｓｅｑ＃｜｜Ａ｜｜ＬＴ｜｜……）。（　）內的資料是一成爲ＭＡＣ的對象，亦即，成爲有無竄改之判定對象的資料。

然而，會有在ＡＴＲＡＣＫ３資料檔案中儲存有各種的資訊資料，而導致竄改檢查對象資料增加的情形。包含所增加的檢查對象資料在內產生新的ＭＡＣ，而將此當作擴充ＭＡＣ而儲存在檔案中，針對只以以往之竄改檢查對象資料作爲對象所產生的原始ＭＡＣ，而基本上以竄改檢查對象領域設定成不變的結構來加以說明。

在圖４２中，係將先前所說明之ＩＮＦ－Ｓｅｑ＃以下的資料設定作爲竄改檢查對象資料，而將所產生的原始ＭＡＣ　７０１儲存在ＡＴＲＡＣＫ３資料檔案中。

更者，當在被記錄在ＡＴＲＡＣＫ３資料檔案中之ＩＮＦ空間的數個資訊中存在有應成爲竄改檢查對象的資料時，則包含構成原始ＭＡＣ７０１的ＭＡＣ產生對象資料的資料，在此爲「ＩＮＦ－Ｓｅｑ＃」在內，根據在其他ＩＮＦ空間內的竄改檢查對象資料而產生新的ＭＡＣ，將此當作擴充ＭＡＣ而儲存在資料檔案中。

在圖４２中，擴充ＭＡＣ〔ＭＡＣ（ＩＮＦ）〕７０２係根據ＭＡＣ（ＩＮＦ－Ｓｅｑ＃｜｜path｜｜MAC (profile)｜｜Others……）而產生。如此般，擴充

（請先閱讀背面之注意事項再填寫本頁）

裝　訂　線

五、發明說明（91 ）

ＭＡＣ包含原始ＭＡＣ的ＭＡＣ產生對象資料的一部分，而根據與其他之竄改檢查對象合併的資料而產生。

又，在更寫擴充ＭＡＣ時，亦即，藉由更寫擴充ＭＡＣ的對象資料，亦即，ＩＮＦ領域之〔ｐａｔｈ〕以下的資料，在根據該更寫資料而再產生新的擴充ＭＡＣ而執行再儲存之處理時，則對包含於擴充ＭＡＣ，且作爲原始ＭＡＣ之對象資料的〔ＩＮＦ－Ｓｅｑ＃〕進行更寫，而執行新的擴充ＭＡＣ的產生、儲存處理。

此時，由於連針對原始ＭＡＣ，也執行作爲其對象資料〔ＩＮＦ－ｓｅｑ＃〕的更寫，因此重新計算原始ＭＡＣ。亦即，在作擴充ＭＡＣ的更新時，則同時執行原始ＭＡＣ的再產生、再儲存處理。

〔ＩＮＦ－ｓｅｑ＃〕的更寫，則可以根據例如產生新的亂數的更寫處理，或是ＩＮＦ－ｓｅｑ＃資料的增數處理等來執行。

如此般，在對應於竄改檢查對象資料的增加而產生的擴充ＭＡＣ的ＭＡＣ產生對象資料中，則包含有原始ＭＡＣ之ＭＡＣ對象資料的一部分，而存在有由雙方之ＭＡＣ共用的ＭＡＣ對象資料，由於是一在作擴充ＭＡＣ的更新時會同時執行原始ＭＡＣ的再生的構成，因此，可以在不擴大原始ＭＡＣ的ＭＡＣ對象資料領域的情形下，即可經常讓作爲新的竄改檢查用資料之例如ＩＮＦ內的資料的更寫處理能夠反映原始ＭＡＣ。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（92）

〔在記憶裝置以及再生裝置間的ＫＥＢ處理〕

接著，則針對利用應用上述樹狀結構之密碼配送系統的有效化密碼區塊（ＥＫＢ），來取得適用於編碼內容之解碼處理的內容密碼(content key)的具體的處理結構加以說明。

圖４３表示已儲存有ＡＴＲＡＣＫ３資料等之編碼內容的例如 Memory Stick 等的記憶裝置１００、用來執行內容再生之再生裝置Ａ２００、再生裝置Ｂ３００。

在記憶裝置１００則儲存有利用圖２１等所說明之ＡＴＲＡＣＫ３資料檔案，爲了要在再生裝置中將內容予以再生，則必須要取得對於內容之解碼爲必要的內容密碼Ｋｃｏｎ。

首先，藉由圖４３所示的記憶裝置８００與再生裝置８１０來說明再生裝置，從記憶裝置直接取得內容密碼的處理形態。首先，記憶裝置８００，與再生裝置Ａ８１０，在執行認證處理功能之相互的控制模組８０１、８１１間執行相互認證處理。相互認證則利用例如之前所說明之圖８的共用密碼編碼方式，或是公開密碼編碼方式來執行相互認證處理。此時，記憶裝置８００與再生裝置Ａ８１０，其中各自的控制處理模組８０１、８１１則具有認證處理執行算法，更者，則必須要儲存對於認證處理爲必要的密碼。

記憶裝置８００，則在與再生裝置Ａ８１０之相互認證後，會在記憶裝置８００內的控制模組８０１中，從儲

五、發明說明（93）

存在快閃記憶體801的ATRACK3資料檔案，取出根據記憶裝置的儲存密碼Kstm而經編碼的內容密碼：E（Kstm、Kcon）、或是根據之前所說明之EKB檔案的處理所取得的密碼編碼密碼（KEK）而經編碼的內容密碼：E（KEK、Kcon）的其中任一者，而執行解碼處理而取得內容密碼Kses。

記憶裝置800，則利用在與再生裝置A810作相互認證時所產生之通話密碼Kses，而執行內容密碼Kcon的再編碼，將所產生的編碼資料：E（Kses、Kcon）送到再生裝置A810。再生裝置A810，則在控制模組811，根據通話密碼Kses，對所收到的編碼內容密碼E（Kses、Kcon）實施解碼而取得內容密碼。

以上所說明的方法是一在記憶裝置側，針對內容密碼實施解碼而取出，而再度根據通話密碼對其實施編碼而送到再生裝置的方法。

接著，則說明在記憶裝置側未實施解碼處理，而在再生裝置側取得內容密碼的處理的實施形態。

該處理形態爲一位於圖43之記憶裝置800與再生裝置B830之間的處理。記憶裝置800，則從在ATRACK3資料檔案中的有效化密碼區塊（EKB）世代，特定出對於取得內容密碼爲必要的對應有效化密碼區塊（EKB），而將所特定出來的EKB送到再生裝置B830。

五、發明說明（94 ）

再生裝置Ｂ８３０則從記憶裝置取得ＥＫＢ，而利用事先儲存在再生裝置內的記憶體，例如Ｅ２ＰＲＯＭ（如快閃記憶體）內的裝置密碼區塊（ＤＫＢ）來執行接受ＥＫＢ的處理，而取得密碼編碼密碼（ＫＥＫ）。

在此則說明裝置密碼區塊（ＤＫＢ）。利用圖４４來說明裝置密碼區塊（ＤＫＢ）的結構。如上所述，內容再生裝置等的各裝置，則具有從圖４４（ａ）所示之樹狀結構之密碼配送結構的末端，亦即，葉連到上位的根的各節點的密碼。而與例如圖４４（ａ）所示之末端節點的設定５（ＳＥＴ５）呈對應的裝置，則保有從作爲葉密碼之Ｋ１０１，作爲節點密碼的Ｋ１０、Ｋ１開始到根密碼Ｋｒｏｏｔ爲止的密碼設定（Ｋｅｙ　Ｓｅｔ），或是到副領域節點密碼爲止的密碼設定，或是到領域節點爲止的密碼設定。

各密碼則在裝置中被編碼，而被儲存在裝置內的記憶體，例如Ｅ２ＰＲＯＭ。而與從被保存在各裝置的葉到特定節點（如副領域節點）或是根爲止的密碼呈對應的密碼設定（Ｋｅｙ　Ｓｅｔ）的編碼密碼設定則是裝置密碼區塊（ＤＫＢ）。

圖４４（ｂ）則表示裝置密碼區塊（ＤＫＢ）的資料結構例。如圖４４（ｂ）所示，ＤＫＢ是一編碼密碼區塊，其具有根據葉密碼，針對節點密碼，以及根據密碼編碼而成的資料，以及根據裝置（如再生裝置）的儲存密碼：Ｋｓｔｄ，針對葉密碼實施編碼而成的資料。裝置（如再

五、發明說明（95）

生裝置），則利用本身的儲存密碼：Ｋｓｔｄ針對該裝置密碼區塊（ＤＫＢ）中的Ｅｎｃ（Ｋｓｔｄ、Ｋｌｅａｆ）實施解碼而取得葉密碼Ｋｌｅａｆ，更者，則利用所取得的葉密碼Ｋｌｅａｆ，直接對上位的編碼節點密碼、編碼根密碼，因此，可以省略掉從ＥＫＢ的下位密碼開始依序解碼而最得上位密碼的處理。此外，裝置密碼區塊（ＤＫＢ）則包含了作爲葉的識別碼的葉ＩＤ。

裝置固有的儲存密碼，則是一針對各設定（裝置）皆不同的密碼，可事先儲存在裝置中的安全記憶體（如ＳＡＮ）中，或是可根據葉ＩＤ而求得。亦即，在裝置的控制模組（編碼處理部）中，也可以根據葉ＩＤ來產生。具體地說，根據依所定的設定（ｓｅｔ）單位而共同被儲存的主密碼(master key)kmas，可針對葉ＩＤ應用ｈａｓｈ函數，而求得 kstd=hash(Kmas、葉ＩＤ）。

以下則回到圖４３繼續說明內容密碼的取得處理。從記憶裝置８００收到有效化密碼區塊（ＥＫＢ）的再生裝置Ｂ８３０，則在控制模組８３１中，利用根據對儲存在記憶體８３２之裝置密碼區塊（ＤＫＢ）實施解碼而得到的節點密碼、根密碼等，而取得根據ＥＫＢ而被編碼的密碼編碼密碼（ＫＥＫ）。ＥＫＢ的處理方法則是一與之前利用圖５、或圖９所說明者同樣的方法。

再生裝置Ｂ８３０，則利用由有效化密碼區塊（ＥＫＢ）的處理所取得的密碼編碼密碼（ＫＥＫ），針對從記憶裝置８００所收到的編碼內容密碼：Ｅ（ＫＥＫ、

五、發明說明（96 ）

Ｋｃｏｎ）實施解碼處理，而取得內容密碼。

此外，被儲存在圖４３之再生裝置Ｂ８３０的記憶體（Ｅ２ＰＲＯＭ）８３２的起始（initial）ＥＫＢ，則是一最初即被儲存在裝置（再生裝置Ｂ８３０）之經簡化的ＥＫＢ檔案，例如在上述圖１１所述之範疇節點（category node)中，是一共同被儲存在與被連接到１個範疇節點（例如，Category=Memory Stick）之下位的葉呈對應之裝置的編碼密碼區塊。

例如，若範疇節點所擁有的密碼爲ｋ０１時，則將經編碼的根密碼：Ｅｎｃ（Ｋｏｌ、Ｋｒｏｏｔ）儲存作爲起始ＥＫＢ。而裝置則藉由處理起始ＥＫＢ，而可取得根密碼。當收到已儲存有例如根據根密碼而經編碼的密碼編碼密碼（ＫＥＫ）的ＫＥＢ時，則利用從起ＥＫＢ所取得的根密碼，可以取得密碼編碼密碼（ＫＥＫ）。

此外，起始ＥＫＢ並不限於共同提供給屬於１個範疇節點的裝置的形態，也可以是由多個領域節點所共用。例如，當例如將 Memory Stick 的範疇節點的節點密碼設爲Ｋ０１，將具有內容再生功能之ＰＣ的範疇節點的節點密碼設爲Ｋ１０，將網路對應型之再生裝置的範疇節點的節點密碼設爲Ｋ１１時，則事先針對各裝置設定好已儲存了Ｅｎｃ（Ｋｏｌ、Ｋｒｏｏｔ）、ＥｎＣ（Ｋ１０、Ｋｒｏｏｔ）、Ｅｎｃ（Ｋ１１、Ｋｒｏｏｔ）之３種的編碼根密碼的起始ＥＫＢ而出貨，可以配送可爲不同的裝置所共用的編碼內容。

五、發明說明（97）

圖４５則表示將裝置密碼區塊（ＤＫＢ），以及當作始起ＥＫＢ之自己錄音，自己再生用的有效化密碼區塊（ＥＫＢ）儲存在再生裝置的記憶體（如Ｅ２ＰＲＯＭ）的構成例。又，圖４６則表示利用該些密碼區塊的內容密碼的取得處理例。

以下說明圖４５的構成。裝置（如記錄再生器）是一對應於圖４５（ａ）的葉的裝置，是一屬於被構成樹狀結構之第８段的領域節點Ｋｎ８的領域的裝置。在裝置則儲存有（ｂ）所示之ＥｎＣ（Ｋｓｔｄ、Ｋｌｅａｆ）～Ｅｎｃ（Ｋｌｅａｆ、Ｋｎ８）的裝置密碼區塊（ＤＫＢ）。其結構雖然是與先前所說明之ＤＫＢ相同，但是根據葉密碼直接被編碼而所儲存的資料，則是一從位於葉密碼之正上方的節點密碼Ｋｎ４７到作爲領域節點密碼之Ｋｎ８爲止的密碼。

更者，裝置則擁有自己錄音，再生用的有效化密碼區塊（ＥＫＢ），在藉由本身的裝置進行內容錄音、再生時，則根據處理再生用的有效化密碼區塊（ＥＫＢ）與裝置密碼區塊（ＤＫＢ）而取得內容密碼Ｋｃｏｎ，執行內容的解碼、編碼。

圖４６係表示在擁有圖４５（ｂ）之ＤＫＢ、ＥＫＢ的裝置的內容的取得處理中所執行的步驟。首先，在步驟Ｓ４００１中，裝置會根據葉ＩＤ而抽出儲存密碼Ｋｓｔｄ，該儲存密碼Ｋｓｔｄ，可以根據葉ＩＤ，而從裝置中的安全記憶體（secare memory）而抽出，或是如

五、發明說明（98）

上所述般地根據至密碼Ｋｍａｓ與葉ＩＤ而算出。

接著，則在Ｓ４６０２中，根據儲存密碼Ｋｓｔｄ而執行裝置密碼區塊（ＤＫＢ）的處理，亦即，ＥｎＣ（Ｋｓｔｄ、Ｋｌｅａｆ）的解碼而求得葉密碼。接著，則在Ｓ４６０３中，根據葉密碼Ｋｌｅａｆ來執行裝置密碼區塊（ＤＫＢ）的處理，亦即，ＥｎＣ（Ｋｌｅａｆ、Ｋｎ８）的解碼而求得範疇節點密碼（Category Node Key)。ＤＫＢ由於儲存有根據葉密碼直接被編碼的節點密碼，因此，可以直接藉由葉密碼實施解碼處理而取得上位的節點密碼。

接著，在步驟Ｓ４６０４中，則從節點密碼Ｋｎ８執行ＥＫＢ處理，而依序求得上的節點密碼，算出作爲最上位密碼之根密碼。接著，在步驟Ｓ４６０５中，則利用藉由有效化密碼區塊（ＥＫＢ）的處理所求得的根密碼Ｋｒｏｏｔ來執行Ｅｎｃ（Ｋｒｏｏｔ、ＫＥＫ）的解碼處理，而求得密碼編碼密碼ＫＥＫ。最後，則在步驟Ｓ４６０６中，利用所取得的密碼編碼密碼ＫＥＫ，來執行被儲存在附隨於內容資料之資料中的ＥｎＣ（ＫＥＫ、Ｋｃｏｎ）的解碼處理，而取得內容密碼Ｋｃｏｎ。

圖４５（ｂ）所示的有效化密碼區塊（ＥＫＢ）雖然是一自己錄音用的ＥＫＢ，但是當在將各種的內容下載到裝置時，則會同下載與該內容對應的ＥＫＢ，而對應於內容，將ＥＫＢ儲存在記憶體，而在內容再生時，則可針對與所下載的內容對應的ＥＫＢ執行圖４６的處理。又，圖

五、發明說明（99）

４５（ｂ）所示的裝置密碼區塊（ＤＫＢ），則將直接根據葉密碼，針對從上位開始算來８段的節點Ｋｎ８的節點密碼爲止實編碼而成的資料當作ＤＫＢ的編碼密碼資料，但是所儲存的節點密碼也可以是到上位或下位爲止的節點密碼。

以上是針對參考特定的實施例，來詳細地說明本發明。然而當然在不脫離本發明之要旨的範圍內可以修正或取代該實施例。亦即，所舉例的形態是用於揭露本發明，但並非是用以限定加以解釋。爲了要判斷本發明的主旨，則應參照申請專利範圍中所記載的內容。

（發明的效果）

如上所述，根據本發明的資料處理裝置以及方法，乃提供一根據包含有：在構成讓各密碼對應於在從以多個裝置作爲葉而構成之樹的根開始到葉爲止之路徑上的根、節點、以及葉之密碼樹的路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料的有效化密碼區塊而編碼的認證密碼，而實現一只有在所選出的合法的裝置才可以取得認證密碼之安全性高的認證密碼配送系統。

更者，根據本發明仄資料處理裝置以及方法，資料處理裝置，即使記憶裝置未擁有相互認證處理的執行功能，也將與構成上述資料處理裝置之假想記憶體裝置的相互認證處理的成位作爲從記憶裝置再生資料或對記憶裝置記錄資料處理的執行條件。由於是根據只有具有合法授權之資

五、發明說明（100）

料處理裝置才能夠實施解碼的有效化密碼區塊（ＥＫＢ）來提供認證密碼，因此，在非法的資料處理裝置中並無法取得合法的認證密碼，而與假想記憶裝置的認證不可能成立，而實現一可限制利用內容的系統。

圖面之簡單說明

圖１爲本發明之資料處理裝置之使用概念的說明圖。

圖２爲本發明之資料處理裝置之系統構成例以及資料路徑例的說明圖。

圖３爲針對本發明之資料處理裝置中的各種密碼、資料之編碼處理加以說明之樹狀結構圖。

圖４爲表示在分配本發明之資料處理裝置中之各種密碼、資料時所使用之有效化密碼區塊（key block）（ＥＫＢ）的例子的說明圖。

圖５爲已使用本發明之資料處理裝置中之內容密碼之有效化密碼區塊（ＥＫＢ）的分配例與解碼處理例的說明圖。

圖６爲表示本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ）的格式例的說明圖。

圖７爲本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ）之標籤（ｔａｇ）之構成的說明圖。

圖８爲表示在將本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ），與內容密碼（content Key)內容(content)合在一起加以配送時之資料構成例的說明圖。

五、發明說明（101）

圖９爲表示將本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ），與內容密碼內容合在一起加以配送時之裝置中的處理例的說明圖。

圖１０爲針對在將本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ）與內容儲存在記錄媒體時的說明圖。

圖１１爲本發明之資料處理裝置中之階層樹狀結構之範疇分類之例子的說明圖。

圖１２係表在本發明之資料處理裝置中之簡略化有效化密碼區塊（ＥＫＢ）之生成過程的說明圖。

圖１３係表在本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ）之生成過程的說明圖。

圖１４係表在本發明之資料處理裝置中之簡略化有效化區塊（ＥＫＢ）的說明圖。

圖１５係表在本發明之資料處理裝置中之再生裝置與記憶裝置之構成的方塊圖。

圖１６係表被記憶在本發明之資料處理裝置中之記憶裝置內之記憶單元的資料的說明圖。

圖１７係表被記憶在本發明之資料處理裝置中之記憶裝置之快閃記憶體的資料的說明圖。

圖１８係概略地表示在本發明之資料處理裝置中之再生管理檔案之資料結構的說明圖。

圖１９係概略地表示在本發明之資料處理裝置中之資料檔案之資料結構的說明圖。

圖２０係更詳細地表示在本發明之資料處理裝置中之

五、發明說明（102）

再生管理檔案之資料結構的說明圖。

圖２１係更詳細地表示在本發明之資料處理裝置中之資料檔案之資料結構的說明圖。

圖２２係表示在本發明之資料處理裝置中之資料檔案之屬性標題（header）之一部分的說明圖。

圖２３係表示在本發明之資料處理裝置中之資料檔案之屬性標題（header）之一部分的說明圖。

圖２４係表在本發明之資料處理裝置中之模式的種類、與在各模式中之錄音時間等的說明圖。

圖２５係表在本發明之資料處理裝置中之複製控制資訊的說明圖。

圖２６係表在本發明之資料處理裝置中之資料檔案之屬性標題之一部分的說明圖。

圖２７係表在本發明之資料處理裝置中之資料檔案之各資料區塊之標題的概略圖。

圖２８係表在本發明之資料處理裝置中之資料記錄處理流程的說明圖。

圖２９係表在可適用在本發明之資料處理裝置中之相互認證處理的說明圖。

圖３０係表在本發明之資料處理裝置中之資料再生處理流程的說明圖。

圖３１係表在本發明之資料處理裝置中之配送密碼允許資訊檔案之格式的說明圖。

圖３２係表在本發明之資料處理裝置中之資料儲存情

五、發明說明（103）

形的說明圖。

圖３３係表已使用在本發明之資料處理裝置中之密碼有效化區塊（ＥＫＢ）之資料解碼處理流程的說明圖。

圖３４係表示在本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ），與認證密碼合在一起加以配送的資料結構，以及在裝置中之處理例的說明圖（之１）。

圖３５係表示在本發明之資料處理裝置中之有效化密碼區塊（ＥＫＢ），與認證密碼合在一起加以配送的資料結構，以及在裝置中之處理例的說明圖（之２）。

圖３６係表示應用本發明之資料處理裝置中之假想記憶卡之認證處理順序的說明圖。

圖３７係表示在產可應用在本發明之資料處理裝置之Integrity・Check值（ＩＣＶ）時所使用之ＭＡＣ值產生例的說明圖。

圖３８係本發明之資料處理裝置之Integrity・Check值（ＩＣＶ）之儲存形態的說明圖。

圖３９係表示用於儲存本發明之資料處理裝置之ＭＡＣ值的循序頁格式（sequence page Format）的說明圖。

圖４０係表示用於儲存本發明之資料處理裝置之ＩＣＶ的輪詢格式（Poll Page Format）的說明圖。

圖４１係表示本發明之資料處理裝置之ＩＣＶ檢查處理流程的說明圖。

圖４２係表在本發明之資料處理裝置中之擴充ＭＡＣ

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（104）

的產生、儲存處理的說明圖。

圖４３係表利用本發明之資料處理裝置中之密碼有效化區塊（ＥＫＢ）的內容密碼的取得處理形態的說明圖。

圖４４係表在本發明之資料處理裝置中所使用之裝置密碼區塊（ＤＫＢ）的構成的說明圖。

圖４５係表在本發明之資料處理裝置中之裝置密碼區塊（ＤＫＢ）、密碼有效化區塊（ＥＫＢ）的儲存構成例的說明圖。

圖４６係表利用本發明之資料處理裝置中之裝置密碼區塊（ＤＫＢ）、密碼有效化區塊（ＥＫＢ）之內容密碼的取得處理態樣的說明圖。

主要元件對照表

１０　內容配送機構

１１　網際網路（Internet）

１２　衛星傳送

１３　電話線路

１４　媒體

２０　資料處理機構

２１　個人電腦（ＰＣ）

２２　攜帶型裝置（ＰＤ）

２３　行動電話、ＰＤＡ

２４　記錄再生器、遊戲終端

２５　再生裝置

五、發明說明（105）

30　記憶機構

100　個人電腦（ＰＣ）

200　再生裝置

300　記憶裝置

601　世代

602　深度（depth）

603　資料指標

604　標籤指標

605　簽名指標

606　資料部

607　標籤部

608　簽名

33、43　控制模組

50、60　亂數產生單元

51、61　記憶單元

52、62　密碼產生／演算單元

53、63　相互認證單元

54、64　編碼／解碼單元

55、65　控制單元

34　快閃記憶體

44　編輯模組

45　壓縮／解壓縮模組

46　揚聲器

49　記憶體

五、發明說明（106）

800　記憶裝置

801　控制模組

802　快閃記憶體

810　再生裝置A

811　控制模組

830　再生裝置B

831　控制模組

832　記憶體

A5
B5

四、中文發明摘要（發明之名稱：資料處理裝置、資料處理方法、及授權系統、以及程式提供媒體）

本發明係提供一種可以確實地執行認證處理，只有擁有合法授權的裝置才能夠利用內容的系統。

藉由有效化密碼區塊（ＥＫＢ），將認證密確提供給資料處理裝置。即使記憶裝置未具有相互認證處理的執行功能時，則以與構成資料處理裝置之假想記憶體裝置之相互認證處理成立作爲從記憶裝置實施資料再生處理，或是對記憶裝置實施資料記錄處理的執行條件。根據在非法的資料處理裝置中不能進行解碼的有效化密碼區塊（ＥＫＢ）來提供認證密碼，藉此，只有合法的資料處理裝置與假想記憶體裝置的認證成立，才能夠利用內容。

英文發明摘要（發明之名稱：）

（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

1．一種資料處理裝置，其主要係針對一對來自記憶裝置的資料進行再生，或對記憶裝置進行資料記錄之資料處理裝置，其特徵在於：

上述資料處理裝置具有以在資料處理裝置與記憶裝置之間之相互認證之成立作爲條件，而執行對來自上述記憶裝置的資料進行再生處理，或對上述記憶裝置進行資料記錄處理的構成，

當上述記憶裝置未具有相互認證處理之執行功能時，則具有執行與構成上述資料處理裝置之假想記憶裝置之相互認證處理，以在資料處理裝置與上述假想記憶裝置之間所執行之相互認證處理的成立爲條件，而執行對來自上述記憶裝置的資料進行再生處理，或對上述記憶裝置進行資記錄處理的構成。

2．如申請專利範圍第1項之資料處理裝置，上述資料處理裝置，具有進行資料再生或資料記錄的記憶裝置會判斷是否可進行相互認證，當可進行相互認證處理時，則在與該記憶裝置之間執行相互認證處理的構成。

3．如申請專利範圍第1項之資料處理裝置，上述資料處理裝置，具有根據包含有：在構成讓各密碼對應於在從以多個資料處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉之密碼樹之路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料在內之有效化密碼區塊（ＥＫＢ），而被編碼之作爲認證密碼的ＥＫＢ配送認證密碼，

六、申請專利範圍

在上述資料處理裝置與上述假想裝置之間所執行之相互認證處理，則是一可應用上述ＥＫＢ配送認證密碼，與事先被儲存在上述假想記憶裝置的認證密碼來執行的構成。

４．如申請專利範圍第３項之資料處理裝置，其中上述包含ＥＫＢ配送認證密碼的有效化密碼區塊（ＥＫＢ），爲一在構成上述密碼樹之葉的資料處理裝置中，則只有在有正常執照的資料處理裝置中才可進行解碼，而在未具有正常執行之資料處理裝置中，則不能進行解碼之有效化密碼區塊（ＥＫＢ），

爲了要防止在違法資料處理裝置中發生與上述假想記憶裝置之間的認證成立，是一能夠排除法資料處理裝置的構成。

５．如申請專利範圍第３項之資料處理裝置，由上述有效化密碼區塊（ＥＫＢ）所編碼而提供的ＥＫＢ配送認證密碼乃實施世代（version）管理，是一執行各世代之更新處理的構成。

６．如申請專利範圍第１項之資料處理裝置，其中上述資料處理裝置具有一根據以該資料處理裝置固有的儲存密碼（kstd），針對在讓各密碼對應於在從以多個情報處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉的密碼樹狀結構中，對應於本身的葉所設定的葉密碼進行編碼，且將之儲存在資料處理裝置內的記憶裝置內。

六、申請專利範圍

7．如申請專利範圍第1項之資料處理裝置，其中上述資料處理裝置，根據在讓各密碼對應於在從以多個資料處理裝置作爲葉而構成的樹的根到葉爲止之路徑上的根、節點，以及葉的密碼樹狀結構中，其中與本身葉對應而設定的葉密碼，將在從上述密碼樹之本身葉到上位之路徑上的多段的不同的節點密碼個別加以編碼，而作爲編碼密碼之集合的裝置密碼區塊（ＤＫＢ）儲存在資料處理裝置內的記憶機構。

8．一種資料處理方法，其主要係針對一對來自記憶裝置的資料進行再生，或對記憶裝置進行資料記錄之資料處理方法，其特徵在於：

當上述記憶裝置未具有相互認證處理的執行功能者，則執行與構成爲資料處理裝置之假想記憶裝置之相互認證處理的步驟及；

以在上述資料處理裝置與上述假想記憶裝置之間所執行的相互認證處理的成立作爲條件，而對來自上述記憶裝置的資料進行再生處理或對上述記憶裝置進行資料記錄處理的步驟。

9．如申請專利範圍第8項之資料處理方法，上述資料處理方法，具有進行資料再生或資料記錄的記憶裝置會判斷是否可進行相互認證的步驟，當可進行相互認證處理時，則在與該記憶裝置之間執行相互認證處理的構成。

10．如申請專利範圍第8項之資料處理方法，上述資料處理方法，具有根據包含有：在構成讓各密碼對應於

六、申請專利範圍

在從以多個資料處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉之密碼樹之路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料在內之有效化密碼區塊（ＥＫＢ），而被編碼之作爲認證密碼的ＥＫＢ配送認證密碼，

在上述資料處理裝置與上述假想裝置之間所執行之相互認證處理，則是一可應用上述ＥＫＢ配送認證密碼，與事先被儲存在上述假想記憶裝置的認證密碼來執行的構成。

１１．一種授權系統，其主要係一可對資料處理裝置賜予授權的授權系統，其特徵在於：

提供根據包含有：在構成讓各密碼對應於在從以多個資料處理裝置作爲葉而構成之樹的根到葉爲止之路徑上的根、節點、以及葉之密碼樹之路徑上的更新密碼，以及根據下位密碼所實施之上位密碼的編碼處理資料在內之有效化密碼區塊（ＥＫＢ），而被編碼之作爲認證密碼的ＥＫＢ配送認證密碼，

資料處理裝置具有即使記憶裝置未具有相互認證處理之執行功能時，也會將與構成上述資料處理裝置之假想記憶裝置之相互認證處理的成立當作對來自上述記憶裝置之資料進行再生處理，或對上述記憶裝置進行資料記錄處理之執行條件的構成，

提供上述ＥＫＢ配送認證密碼的有效化密碼區塊（ＥＫＢ），爲一在構成上述密碼樹之葉的資料處理裝置中

六、申請專利範圍

，則只有在有正當授權的資料處理裝置中才可進行解碼，而在未具有正當授權之資料處理裝置中，則不能進行解碼之有效化密碼區塊（ＥＫＢ），藉此可以防止在非法資料處理裝置中發生與上述假想記憶裝置之間的認證成立，是一能夠排除非法資料處理裝置利用內容的構成。

１２．一種程式提供媒體，其特徵在於：係針對一用來提供可以在電腦系統上執行對來自記憶裝置之資料進行再生，或對記憶裝置進行資料記錄之處理處理之電腦程式的程式提供媒體，上述電腦程式具有：

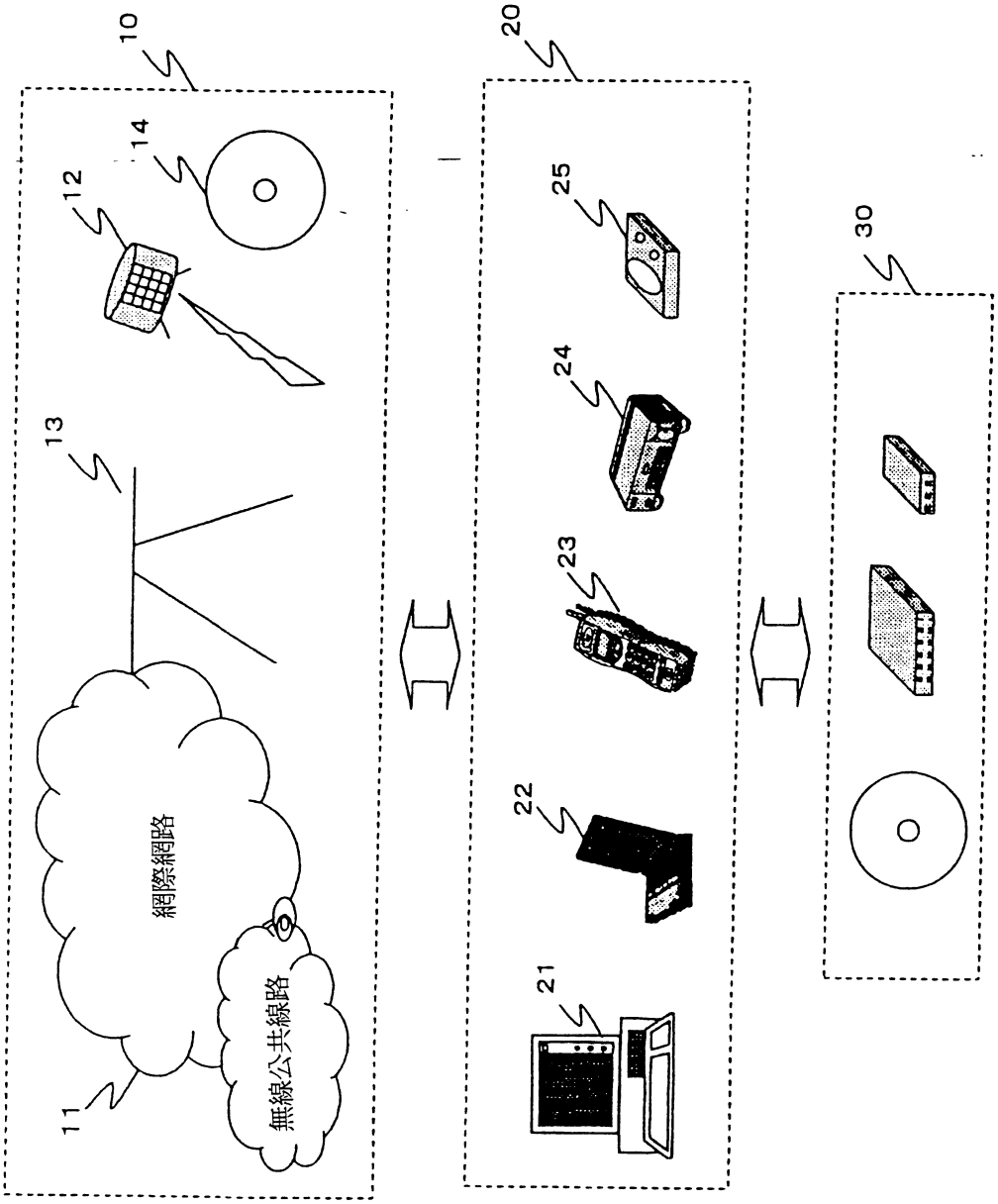
當上述記憶裝置未具有相互認證處理的執行功能者，則執行與構成爲資料處理裝置之假想記憶裝置之相互認證處理的步驟及；

以在上述資料處理裝置與上述假想記憶裝置之間所執行的相互認證處理的成立作爲條件，而對來自上述記憶裝置的資料進行再生處理或對上述記憶裝置進行資料記錄處理的步驟。

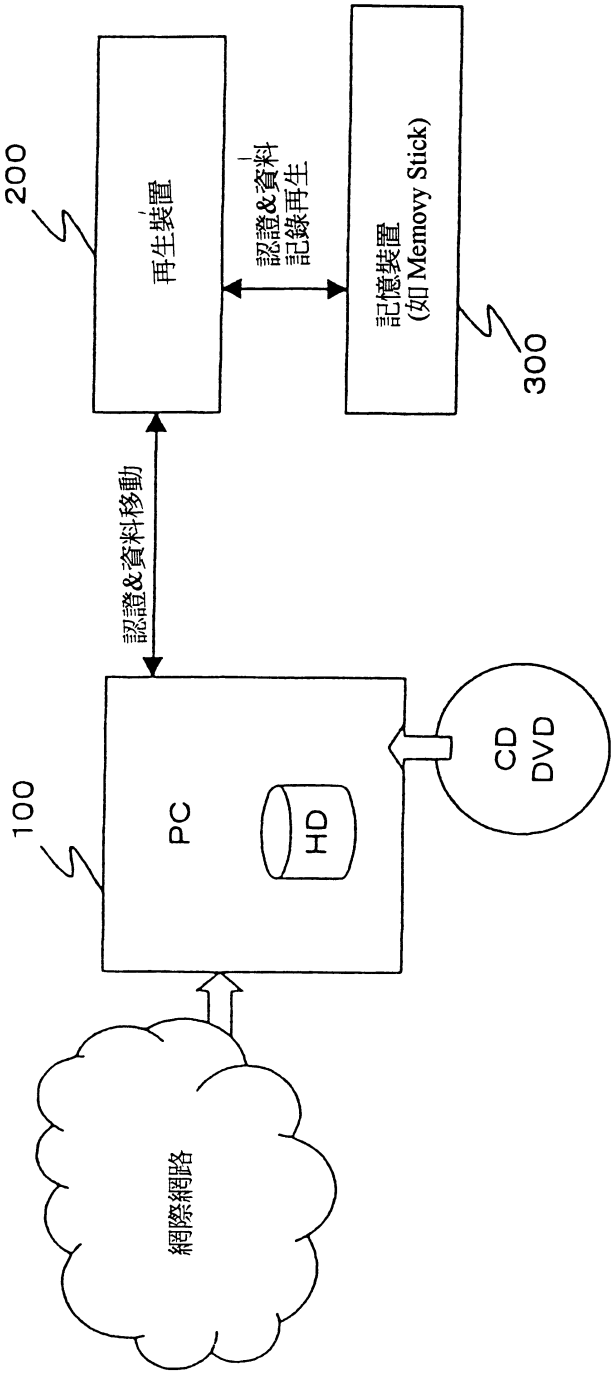
90116898

741531

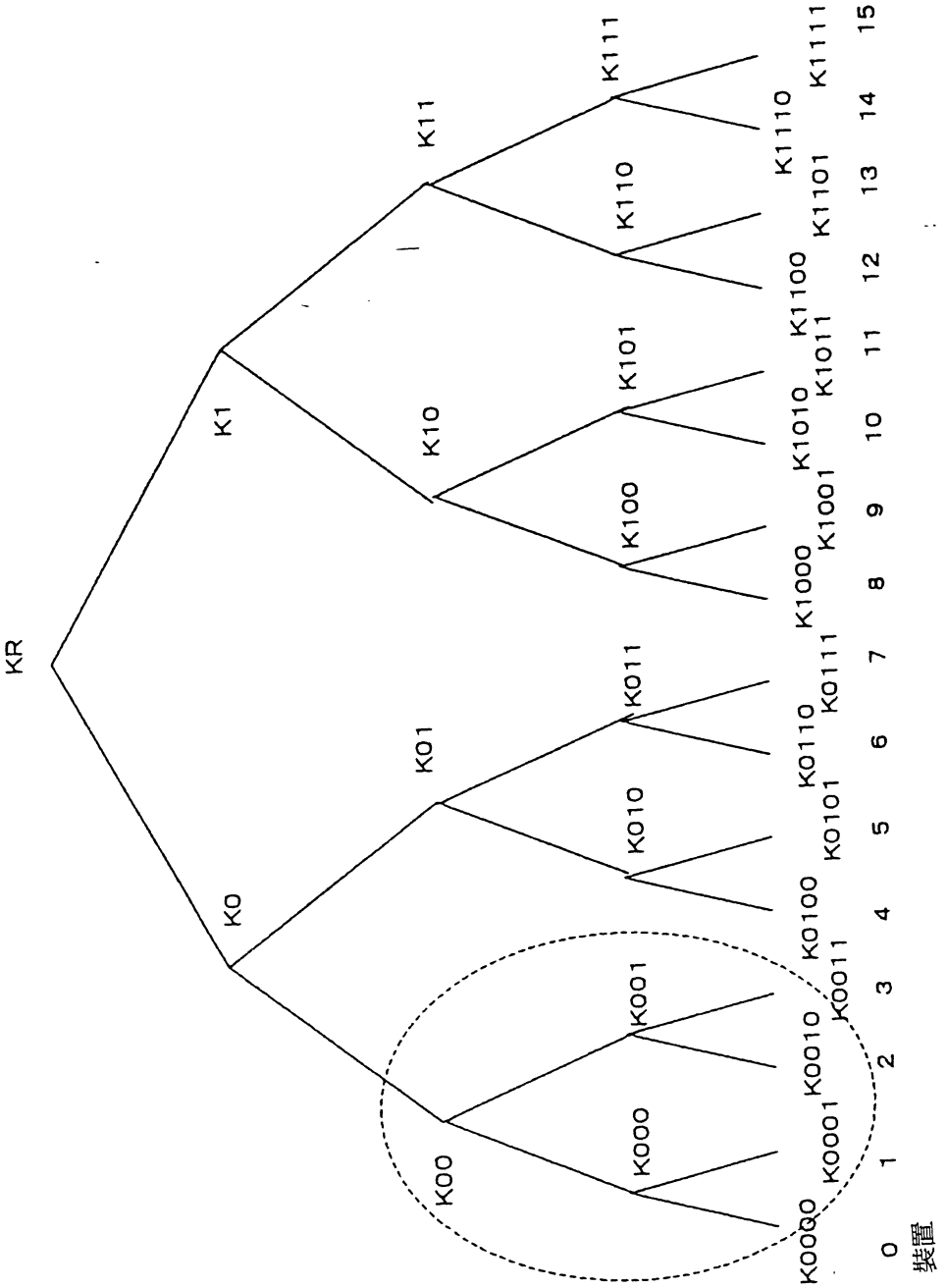
第1圖



第 2 圖


200
再生裝置
認證&資料
記錄再生
記憶裝置
(如 Memovy Stick)
300
認證&資料移動
100
PC
HD
CD
DVD
網際網路

第3圖


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
裝置

第 4 圖

(A)有效化密碼區塊(EKB:Enabling Key Block)例 1

將世代:t 的節點密碼送到裝置 0,1,2

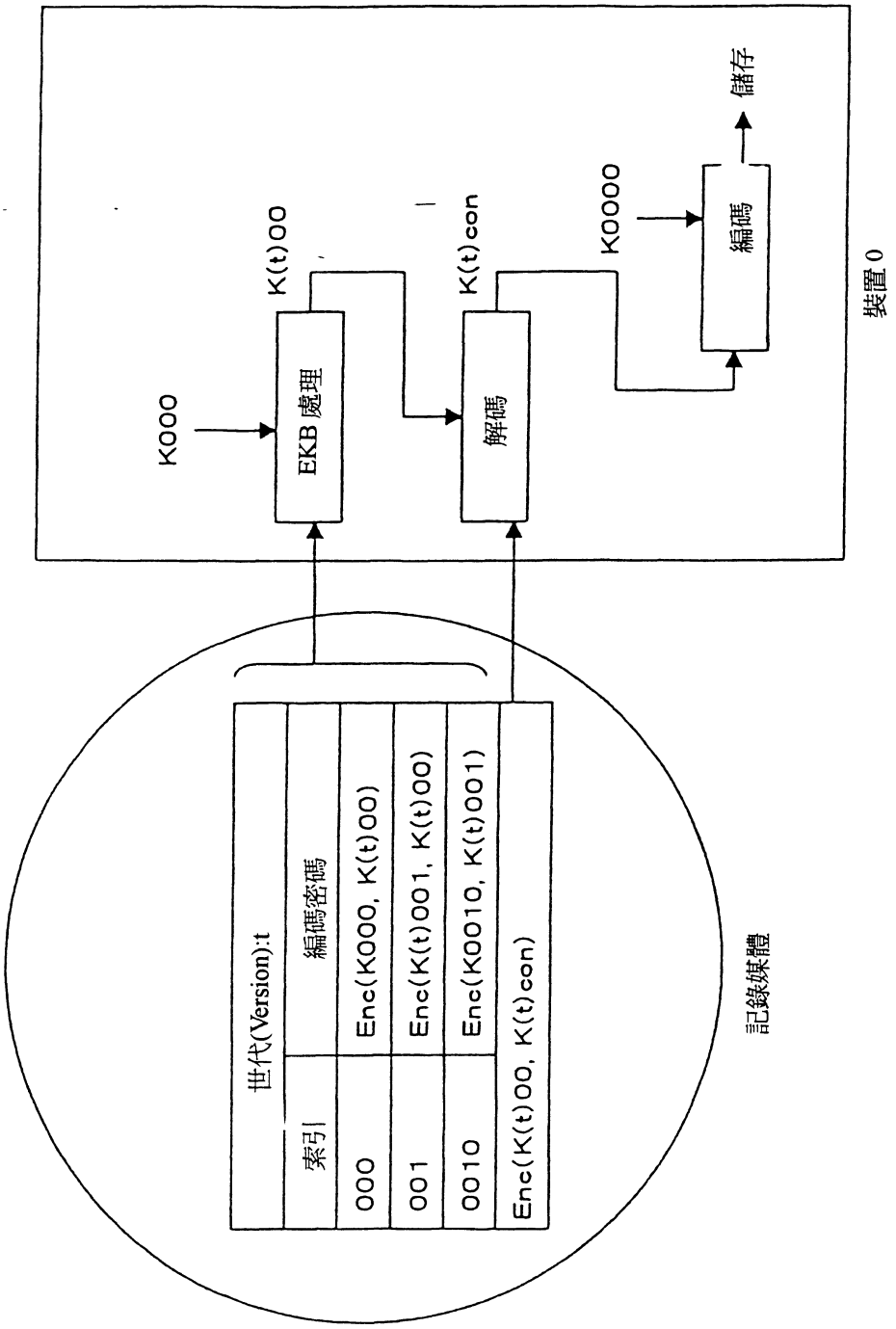
世代(Version):t	
索引	編碼密碼
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有效化密碼區塊(EKB:Enabling Key Block)例 2

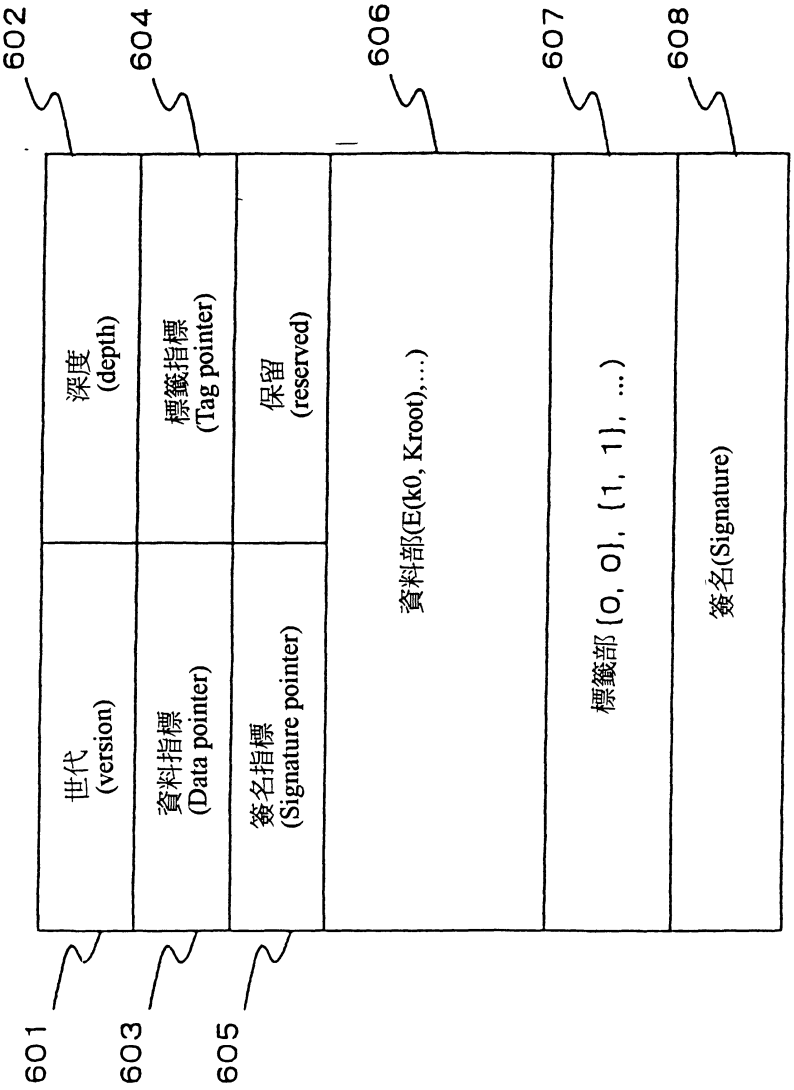
將世代:t 的節點密碼送到裝置 0,1,2

世代(Version):t	
索引	編碼密碼
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

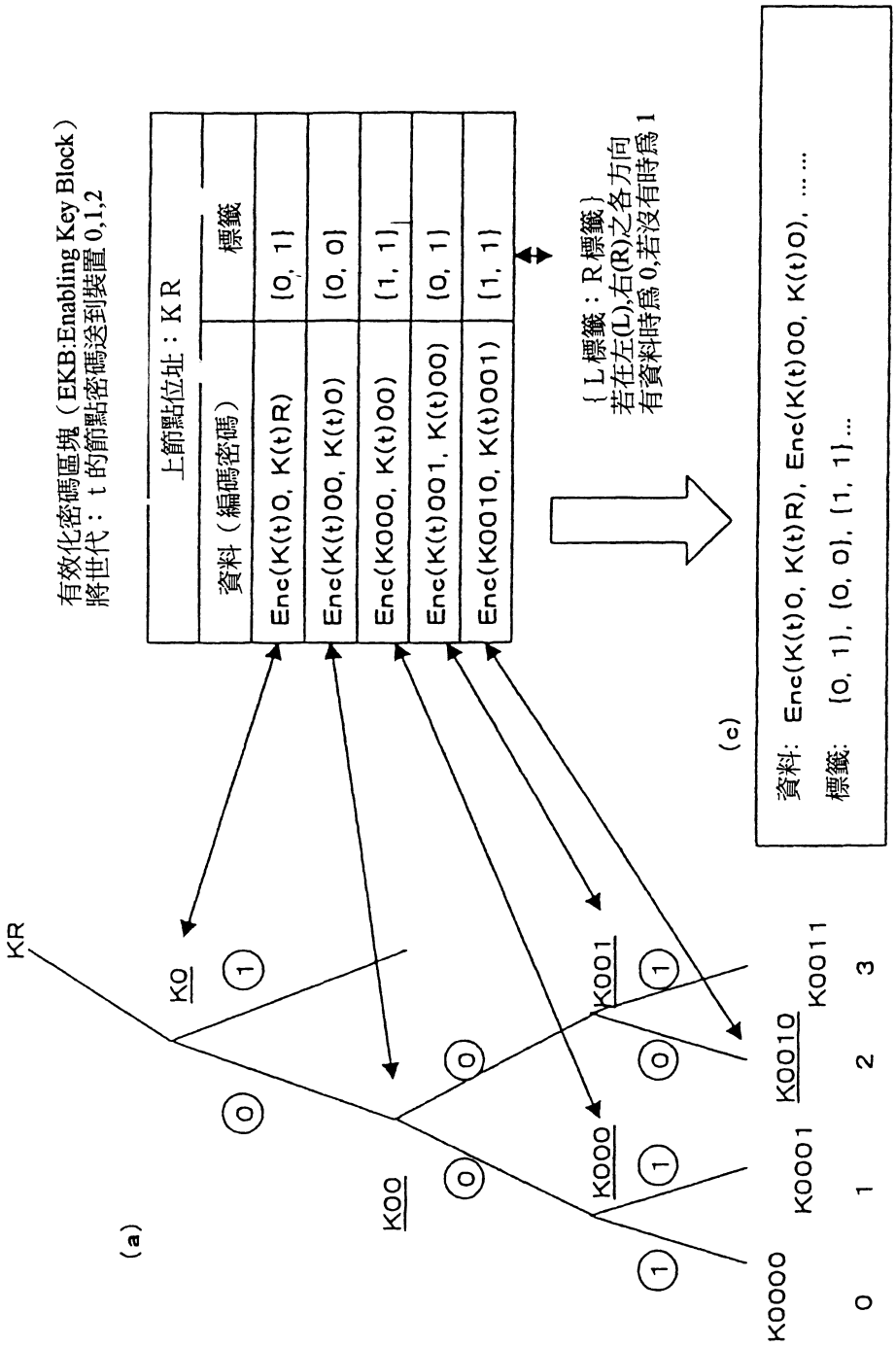
第 5 圖


K000
EKB 處理
K(t)00
解碼
K(t)con
K0000
編碼
儲存
裝置 0
世代(Version):t
索引
編碼密碼
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)
記錄媒體

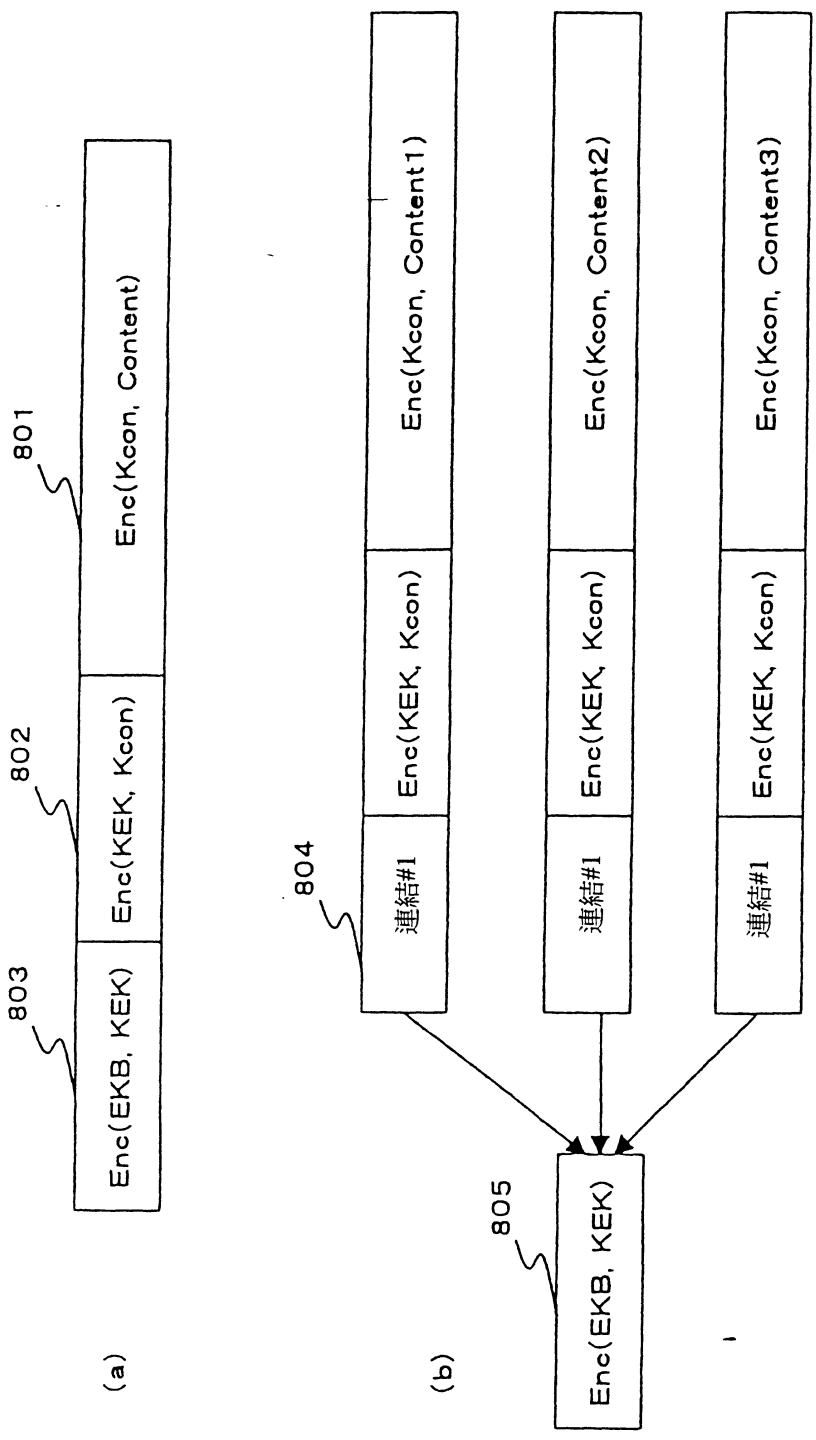
第 6 圖


602
604
606
607
608
深度
(depth)
標籤指標
(Tag pointer)
保留
(reserved)
資料部(E(k0, Kroot),...)
標籤部 {0, 0}, {1, 1}, ...)
簽名(Signature)
世代
(version)
資料指標
(Data pointer)
簽名指標
(Signature pointer)
601
603
605

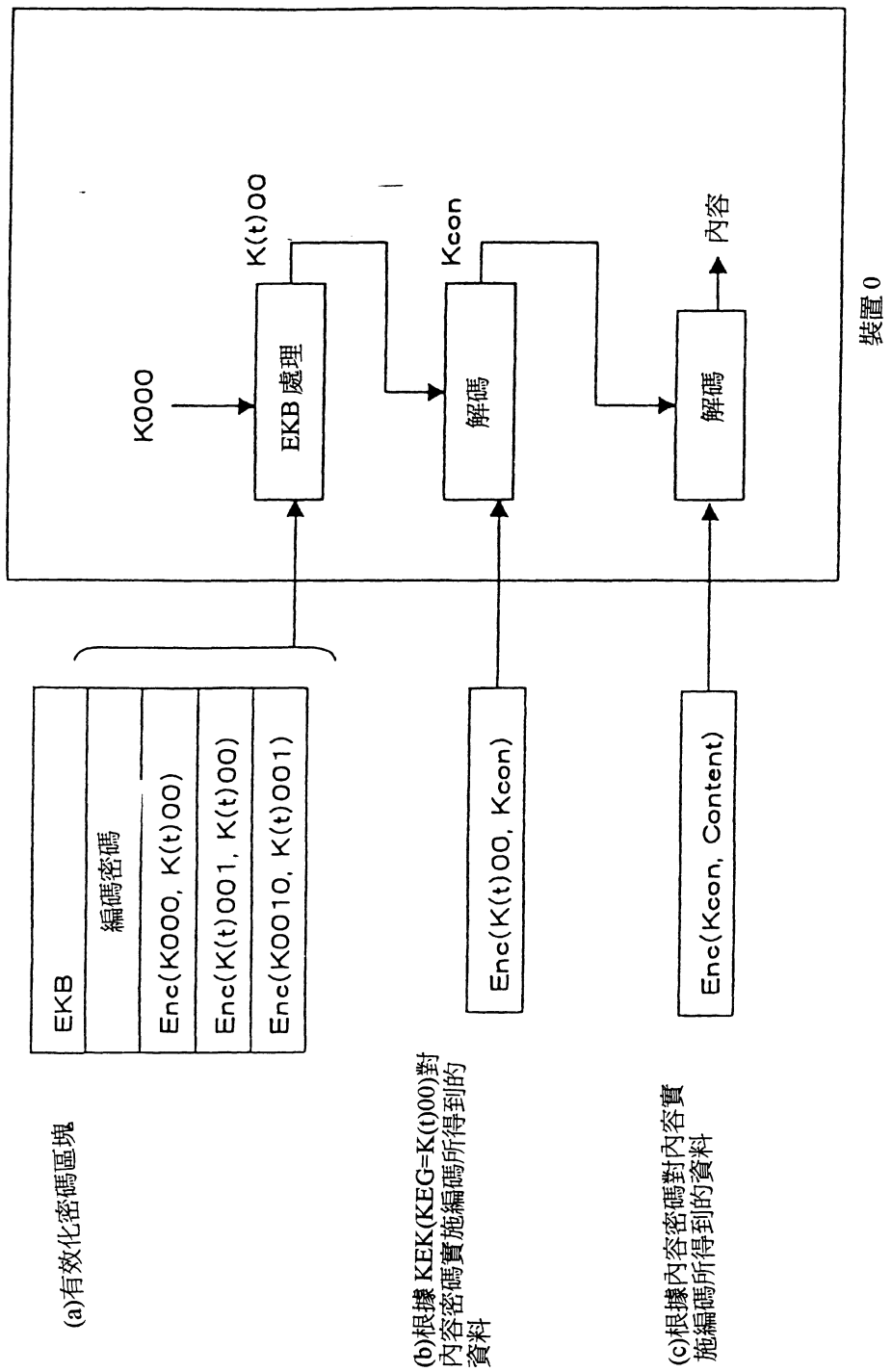
第 7 圖


(a)
KR
K0
K00
K000
K001
K0010
K0011
K0000
K0001
0
1
2
3
(b)
有效化密碼區塊（EKB:Enabling Key Block）
將世代：t 的節點密碼送到裝置 0,1,2
上節點位址：K R
資料（編碼密碼）
標籤
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{ L 標籤：R 標籤 }
若在左(L),右(R)之各方向
有資料時爲 0,若沒有時爲 1
(c)
資料: Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ……
標籤: {0, 1}, {0, 0}, {1, 1}…

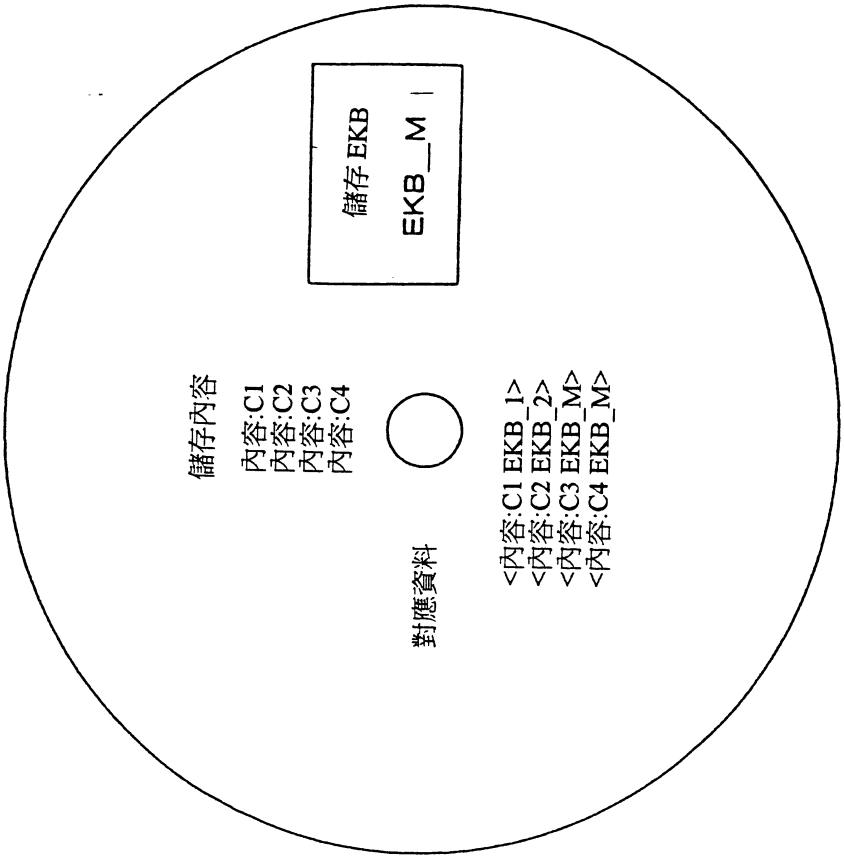
第 8 圖


(a)
801
802
803
Enc(EKB, KEK)
Enc(KEK, Kcon)
Enc(Kcon, Content)
(b)
804
805
連結#1
Enc(KEK, Kcon)
Enc(Kcon, Content1)
Enc(Kcon, Content2)
Enc(Kcon, Content3)
Enc(EKB, KEK)

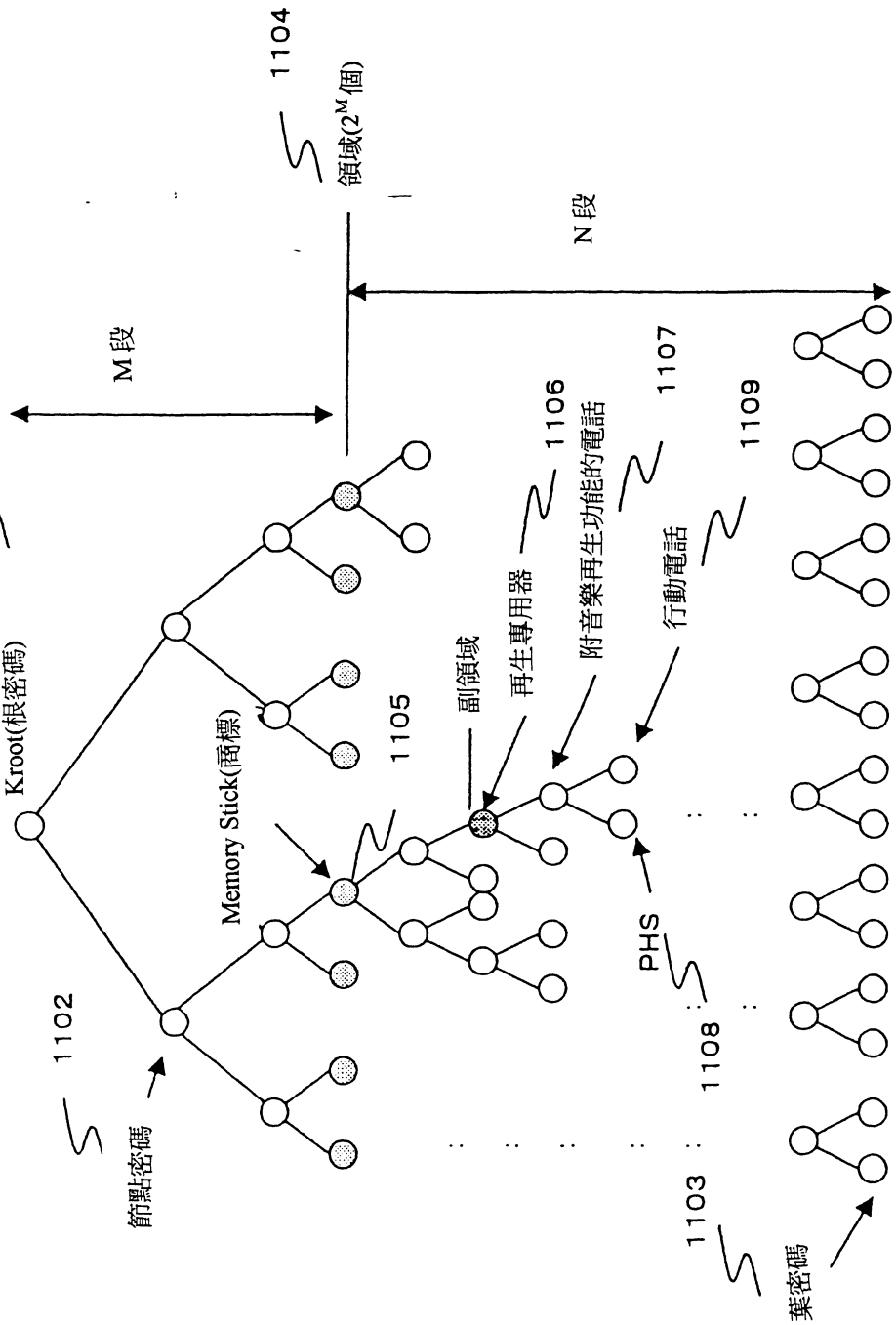
第 9 圖


EKB
編碼密碼
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
(a)有效化密碼區塊
Enc(K(t)00, Kcon)
(b)根據 KEK(KEG=K(t)00)對內容密碼實施編碼所得到的資料
Enc(Kcon, Content)
(c)根據內容密碼對內容實施編碼所得到的資料
K000
EKB 處理
K(t)00
解碼
Kcon
解碼
內容
裝置 0

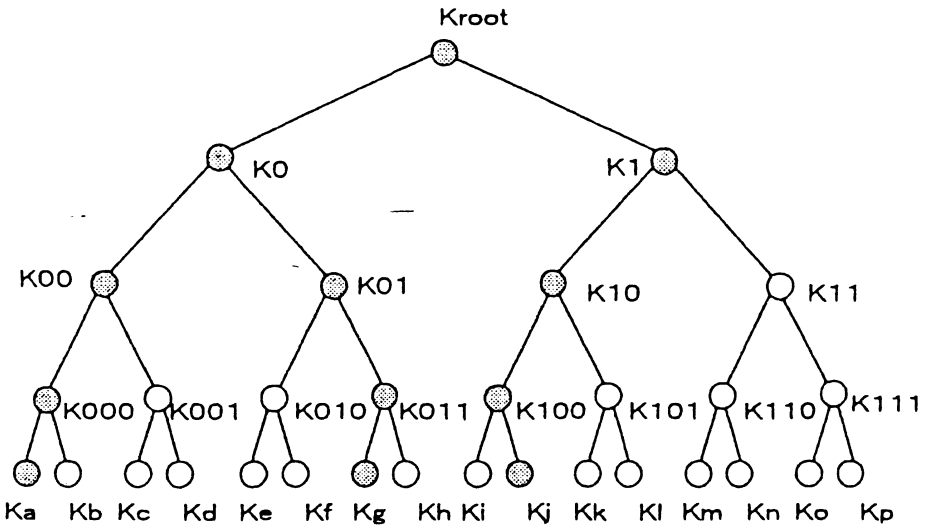
第 10 圖


儲存內容
內容:C1
內容:C2
內容:C3
內容:C4
儲存 EKB
EKB_M
對應資料
<內容:C1 EKB_1>
<內容:C2 EKB_2>
<內容:C3 EKB_M>
<內容:C4 EKB_M>
記錄媒體

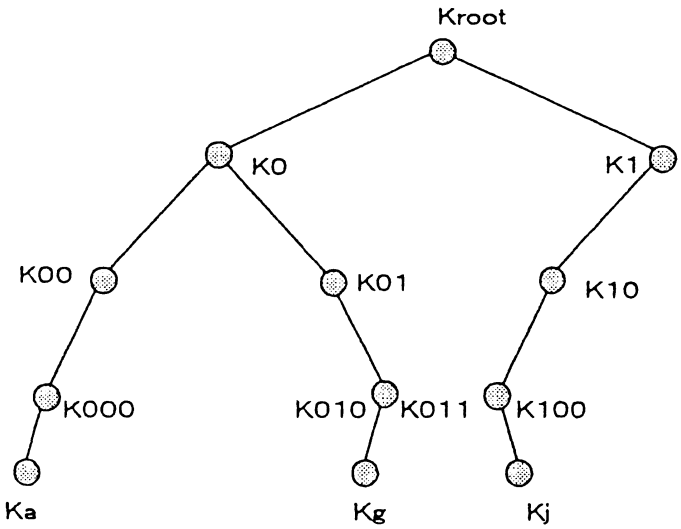
第 11 圖


1101
M 段
1104
領域(2^M個)
N 段
Kroot(根密碼)
1102
節點密碼
Memory Stick(商標)
1105
副領域
再生專用器
1106
附音樂再生功能的電話
1107
行動電話
1109
PHS
1108
1103
葉密碼

第 12 圖


Kroot
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
Ka
Kb
Kc
Kd
Ke
Kf
Kg
Kh
Ki
Kj
Kk
Kl
Km
Kn
Ko
Kp

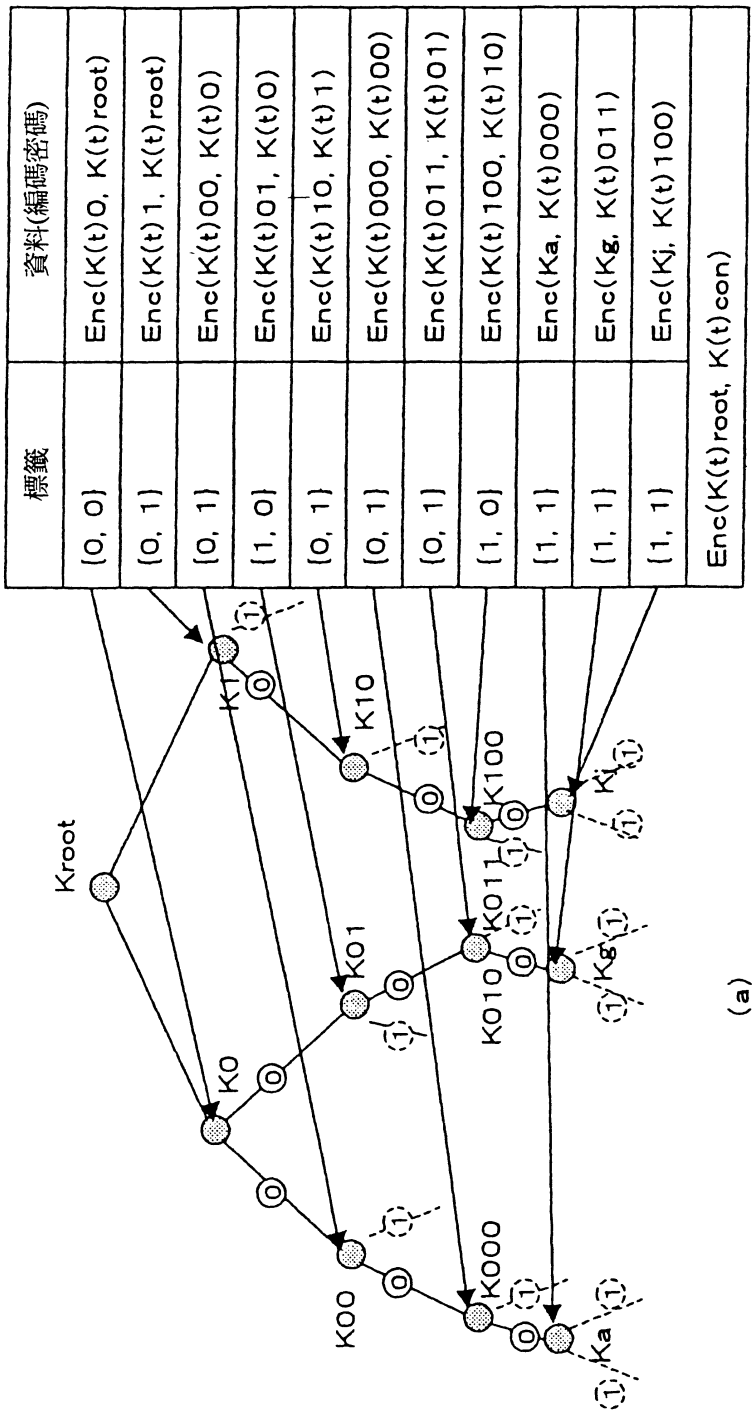
(a)


Kroot
K0
K1
K00
K01
K10
K000
K010
K011
K100
Ka
Kg
Kj

(b)

第 13 圖

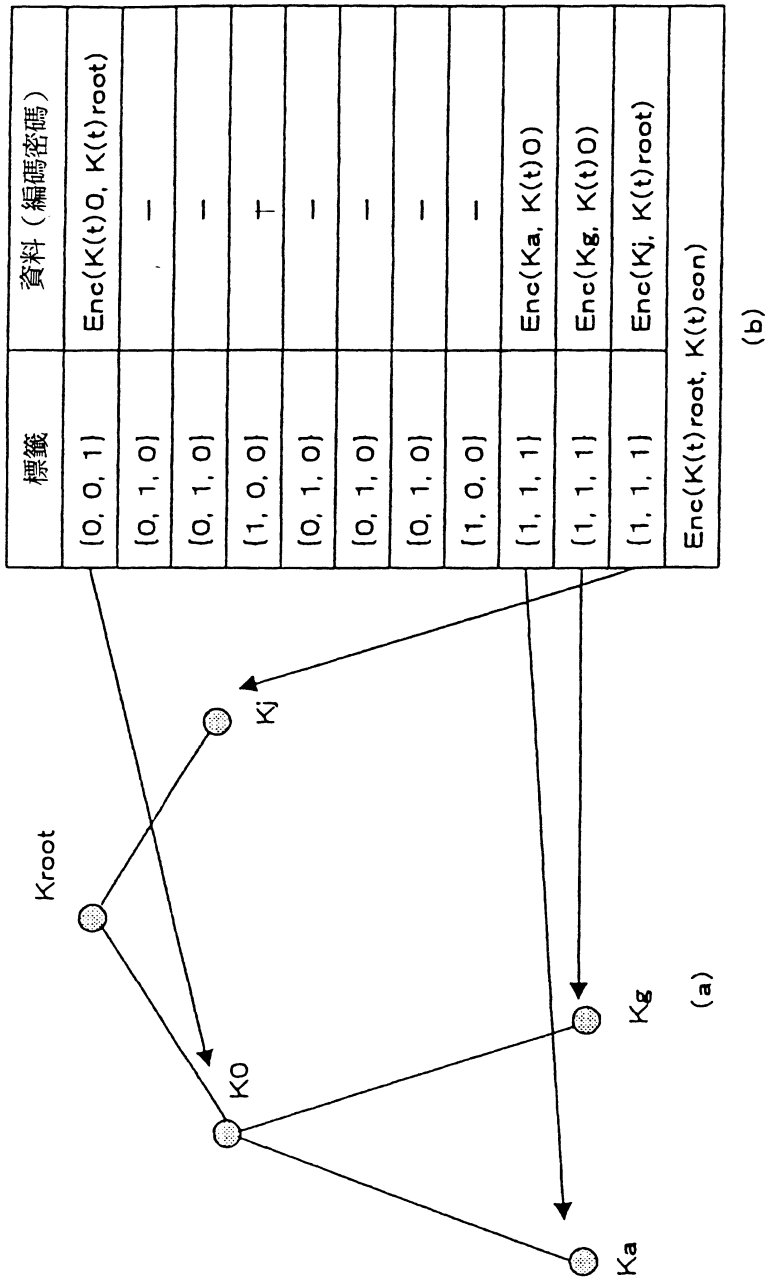
利用有效化密碼區塊(EKB:Enabling Key Block)，將世代 t 的內容密碼送到裝置 Ka,Kg,Kj)



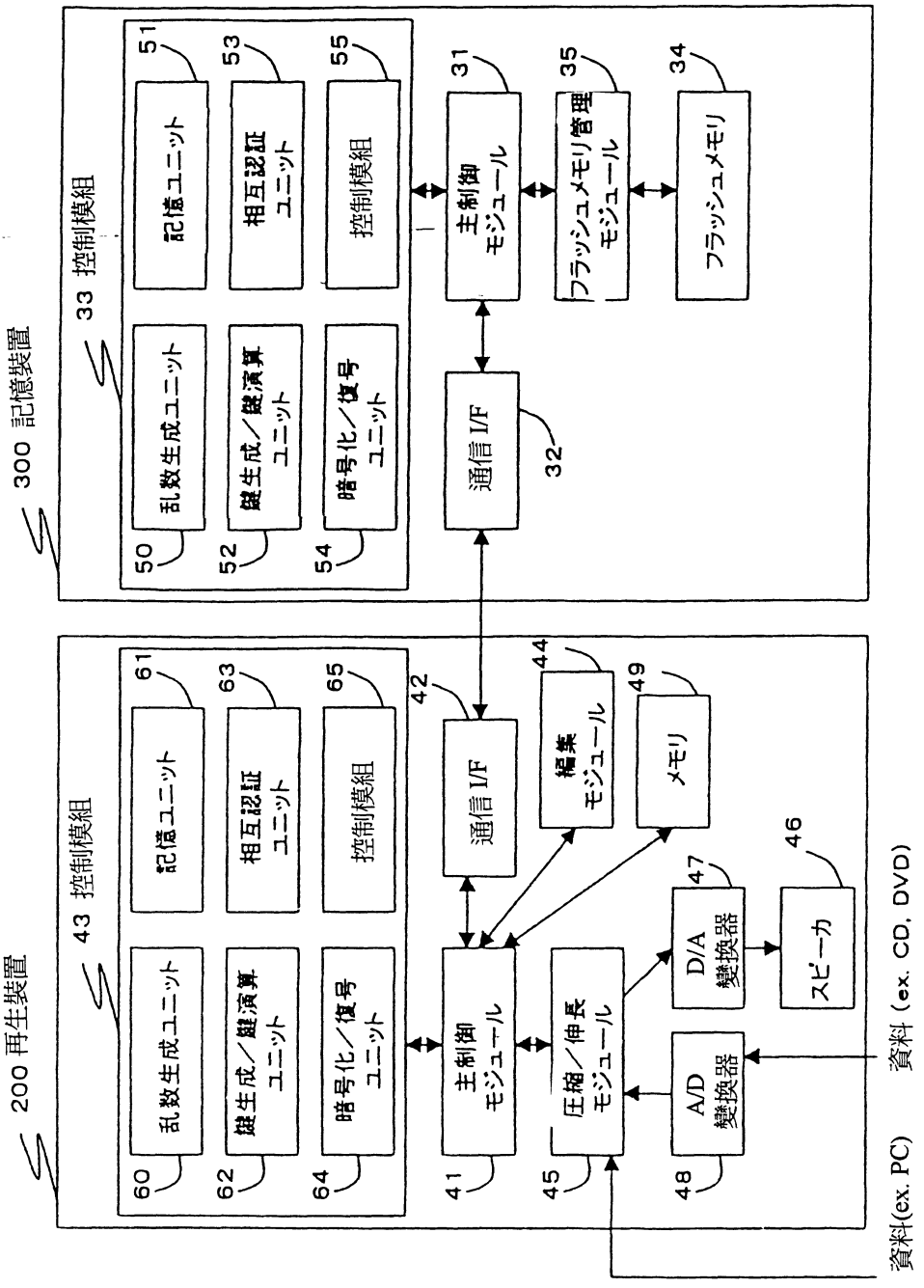
標籤	資料(編碼密碼)
{0, 0}	Enc(K(t)0, K(t)root)
{0, 1}	Enc(K(t)1, K(t)root)
{0, 1}	Enc(K(t)00, K(t)0)
{1, 0}	Enc(K(t)01, K(t)0)
{0, 1}	Enc(K(t)10, K(t)1)
{0, 1}	Enc(K(t)000, K(t)00)
{0, 1}	Enc(K(t)011, K(t)01)
{1, 0}	Enc(K(t)100, K(t)10)
{1, 1}	Enc(Ka, K(t)000)
{1, 1}	Enc(Kg, K(t)011)
{1, 1}	Enc(Kj, K(t)100)
Enc(K(t)root, K(t)con)	

第 14 圖

利用經簡化的有效化密碼區塊(EKB:Enabling Key Block)，將世代 t 的內容密碼送到裝置 Ka,Kg,Kj



第 15 圖

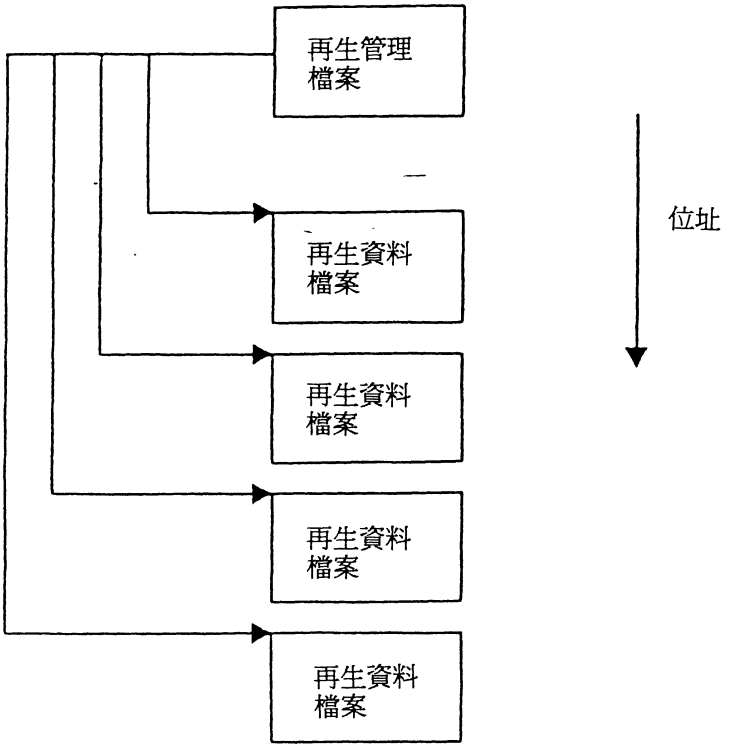

200 再生裝置
43 控制模組
60 乱数生成ユニット
62 鍵生成／鍵演算ユニット
64 暗号化／復号ユニット
61 記憶ユニット
63 相互認証ユニット
65 控制模組
41 主制御モジュール
42 通信 I/F
45 圧縮／伸長モジュール
44 編集モジュール
49 メモリ
48 A/D 變換器
47 D/A 變換器
46 スピーカ
資料(ex. PC)
資料 (ex. CD, DVD)
300 記憶裝置
33 控制模組
50 乱数生成ユニット
52 鍵生成／鍵演算ユニット
54 暗号化／復号ユニット
51 記憶ユニット
53 相互認証ユニット
55 控制模組
32 通信 I/F
31 主制御モジュール
35 フラッシュメモリ管理モジュール
34 フラッシュメモリ

第 16 圖

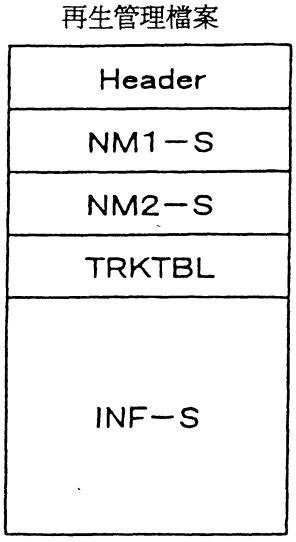
被儲存在記憶裝置之記憶單元的資料

認證密碼資料	—	IK0 IK1 IK2 IK3 : : IK30 IK31
裝置識別資料		ID0
記憶用密碼資料		Kstm

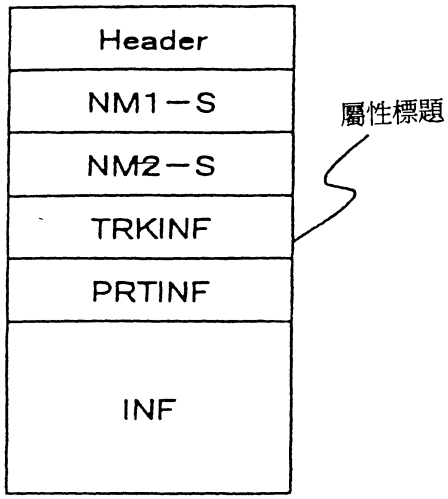
第 17 圖

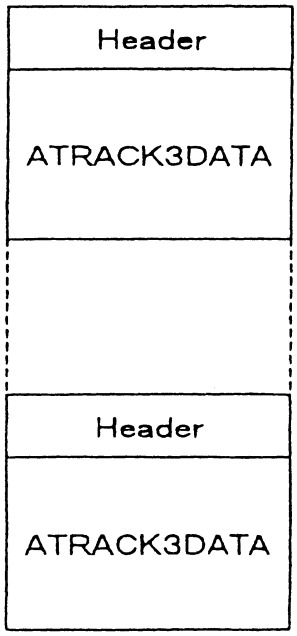


第 18 圖



第 19 圖


Header
NM1－S
NM2－S
TRKINF
PRTINF
INF
屬性標題


Header
ATRACK3DATA
Header
ATRACK3DATA

第 20 圖

再生管理檔案

A

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID−TL0				Reserved		Mcode		REVISION				Reserved			
0x0010	SN1C+L		SN2C+L		SINFSIZE		T−TRK		VerNo		Reserved					

B

0x0020	NM1−S(256)							
0x0120	NM2−S(512)							
0x0310								
0x0320	Reserved(4)			EKB version	E(Kstm, Kcon)			
0x0330	E(KEKn, Kcon)				C_MAC[0]			
0x0340	Reserved(8)				Reserved(3)	MGR	S−YMDhms	
0x0350	TRK−001	TRK−002	TRK−003	TRK−004	TRK−005	TRK−006	TRK−007	TRK−008
0x0360	TRK−009	TRK−010	TRK−011	TRK−012	TRK−013	TRK−014	TRK−015	TRK−016
0x0660	TRK−393	TRK−394	TRK−395	TRK−396	TRK−397	TRK−398	TRK−399	TRK−400
0x0670	INF−S(14720)							
0x3FFF	BLKID−TL0			Reserved	Mcode	REVISION		Reserved

C

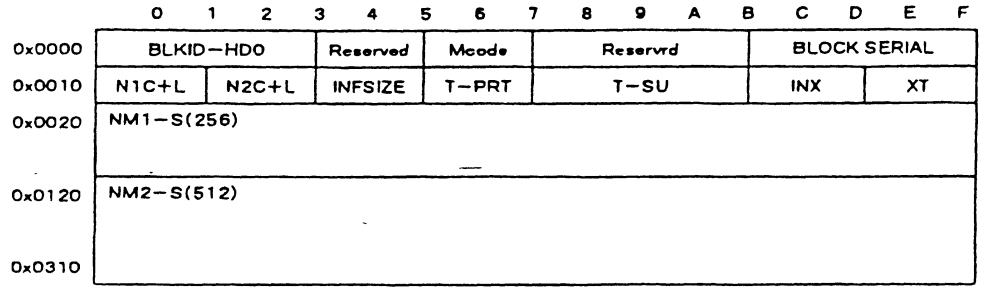
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
INF	0X00	ID	0X00	SIZE		Mcode		C+L		Reserved		DATA 可變長			

第 21 圖

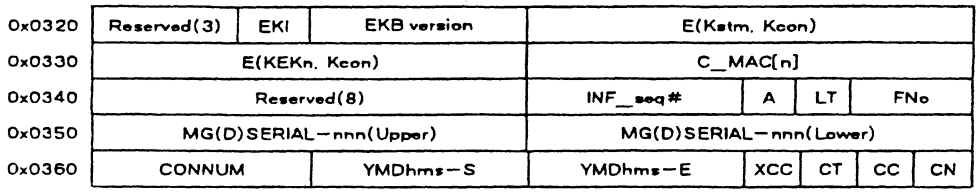
ATRACK3 資料檔案

	0 1 2 3 4 5 6 7 8 9 A B C D E F
0x0000	BLKID−HD0 | Reserved | Mcode | Reservrd | BLOCK SERIAL
0x0010	N1C+L | N2C+L | INFSIZE | T−PRT | T−SU | INX | XT
0x0020	NM1−S(256)
0x0120	NM2−S(512)
0x0310	
0x0320	Reserved(3) | EKI | EKB version | E(Kstm, Kcon)
0x0330	E(KEKn, Kcon) | C_MAC[n]
0x0340	Reserved(8) | INF_seq# | A | LT | FNo
0x0350	MG(D)SERIAL−nnn(Upper) | MG(D)SERIAL−nnn(Lower)
0x0360	CONNUM | YMDhms−S | YMDhms−E | XCC | CT | CC | CN
0x0370	PRTSIZE | PRTKEY | Reserved(8)
0x0380	CONNUM0 | PRTSIZE(0x0388) | PRTKEY
0x0390	Reserved(8) | CONNUM0
	INF(0x0400)
0x3FFF	BLKID−HD0 | Reserved | Mcode | Reservrd | BLOCK SERIAL
0x4000	BLKID−A3D | Reserved | Mcode | CONNUM0 | BLOCK SERIAL
0x4010	BLOCKSEED | INITIALIZATION VECTOR
0x4020	SU−000(Nbyte=384byte)
0x41A0	SU−001(Nbyte)
0x4320	SU−002(Nbyte)
0x04A0	SU−041(Nbyte)
0x7DA0	Reserved(Nbyte=208byte)
0x7F20	BLK SEED
0x7FF0	BLKID−A3D | Reserved | Mcode | CONNUM0 | BLOCK SERIAL

第 22 圖


0 1 2 3 4 5 6 7 8 9 A B C D E F
0x0000
BLKID—HD0
Reserved
Mcode
Reservrd
BLOCK SERIAL
0x0010
N1C+L
N2C+L
INFSIZE
T—PRT
T—SU
INX
XT
0x0020
NM1—S(256)
0x0120
NM2—S(512)
0x0310

第 23 圖


0x0320
Reserved(3)
EKI
EKB version
E(Kstm, Kcon)
0x0330
E(KEKn, Kcon)
C_MAC[n]
0x0340
Reserved(8)
INF_seq#
A
LT
FNo
0x0350
MG(D)SERIAL—nnn(Upper)
MG(D)SERIAL—nnn(Lower)
0x0360
CONNUM
YMDhms—S
YMDhms—E
XCC
CT
CC
CN

第 24 圖

位元 7:ATRACK3 的模式　　0: Dual　　1: Joint

位元 6,5,4:3 位元的 N 爲模式的值

N	模式	時間	轉送速率	SU	位元組
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	mono	181min	47kbps	119SU	136
0	mono	258min	33kbps	169SU	96

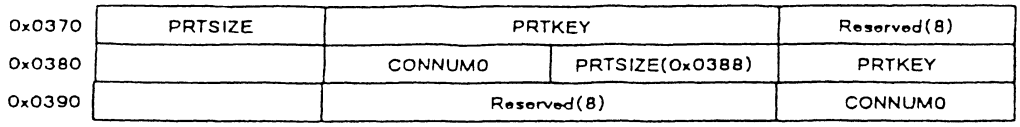
位元 3:保留
位元 2:資料區分　0:音頻　1:其他
位元 1:再生 SKIP　0:一般再生　1:SKIP
位元 0:加強　0:OFF　1:ON(50/15 μS)

第 25 圖

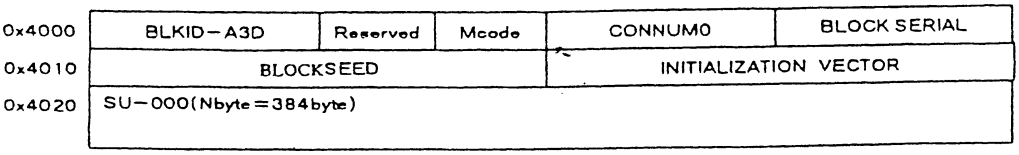
HCMS

位元 7:允許複製0:禁止複製1:可複製
位元 6:世代　0:原始　1:第 1 次(第 1 世代)以上
位元 5-4:有關高速數位複製之複製控制
00:複製世代　01:複製第 1 次　10:可以複製
將已經複製第 1 次的子代設成禁止複製
位元 3-2:MagicGate 認證位準
00:Level10(Non-MG)　01:Level1
02:Level2　11:Reserved
Level10 以外無法合併
位元 1,0:Reserved

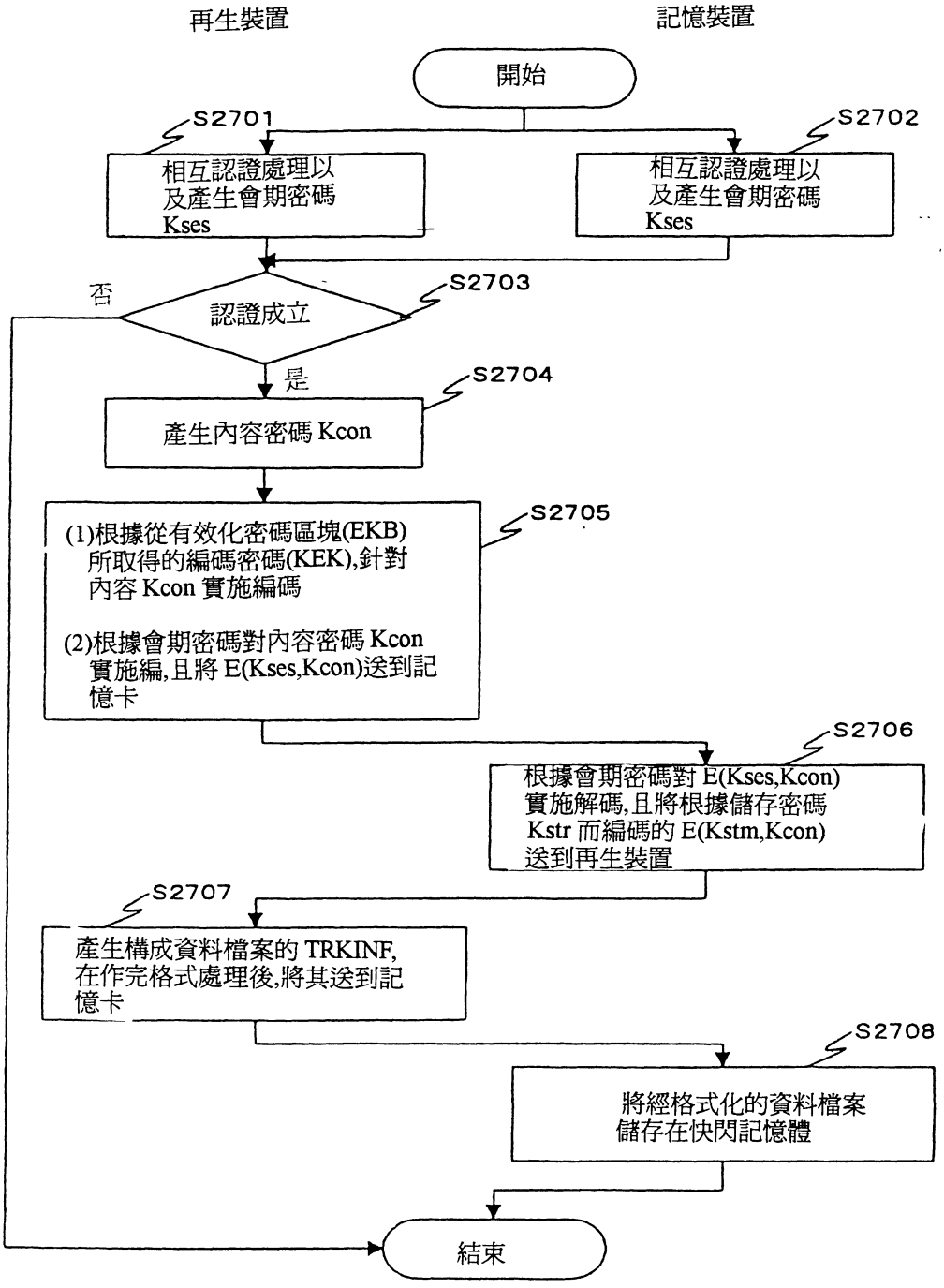
第 26 圖


0x0370
PRTSIZE
PRTKEY
Reserved(8)
0x0380
CONNUM0
PRTSIZE(0x0388)
PRTKEY
0x0390
Reserved(8)
CONNUM0

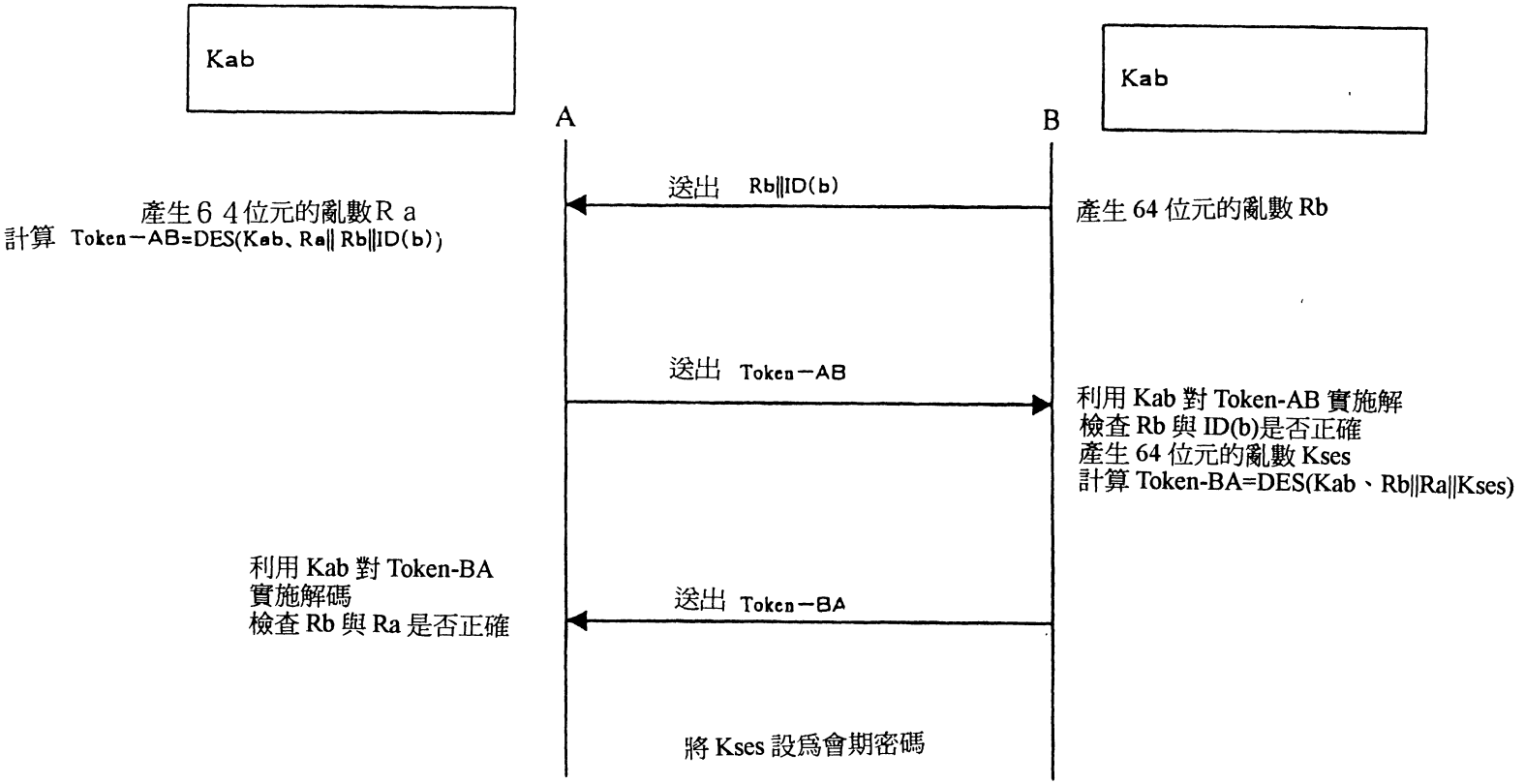
第 27 圖


0x4000
BLKID-A3D
Reserved
Mcode
CONNUM0
BLOCK SERIAL
0x4010
BLOCKSEED
INITIALIZATION VECTOR
0x4020
SU-000(Nbyte=384byte)

第 28 圖

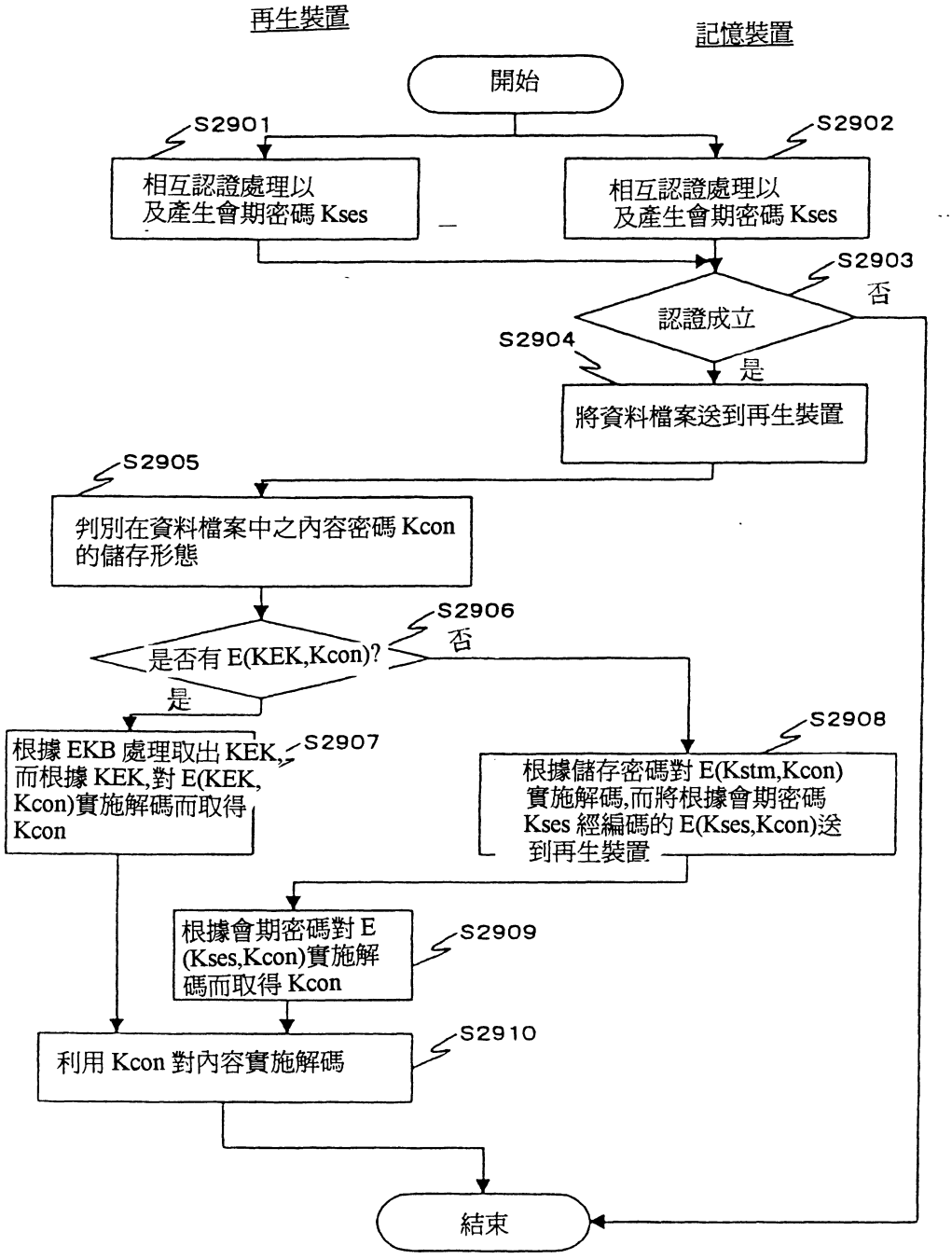

再生裝置
記憶裝置
開始
S2701
相互認證處理以及產生會期密碼 Kses
S2702
相互認證處理以及產生會期密碼 Kses
否
認證成立
S2703
是
S2704
產生內容密碼 Kcon
S2705
(1)根據從有效化密碼區塊(EKB)所取得的編碼密碼(KEK),針對內容 Kcon 實施編碼
(2)根據會期密碼對內容密碼 Kcon 實施編,且將 E(Kses,Kcon)送到記憶卡
S2706
根據會期密碼對 E(Kses,Kcon)實施解碼,且將根據儲存密碼 Kstr 而編碼的 E(Kstm,Kcon)送到再生裝置
S2707
產生構成資料檔案的 TRKINF,在作完格式處理後,將其送到記憶卡
S2708
將經格式化的資料檔案儲存在快閃記憶體
結束

第 29 圖



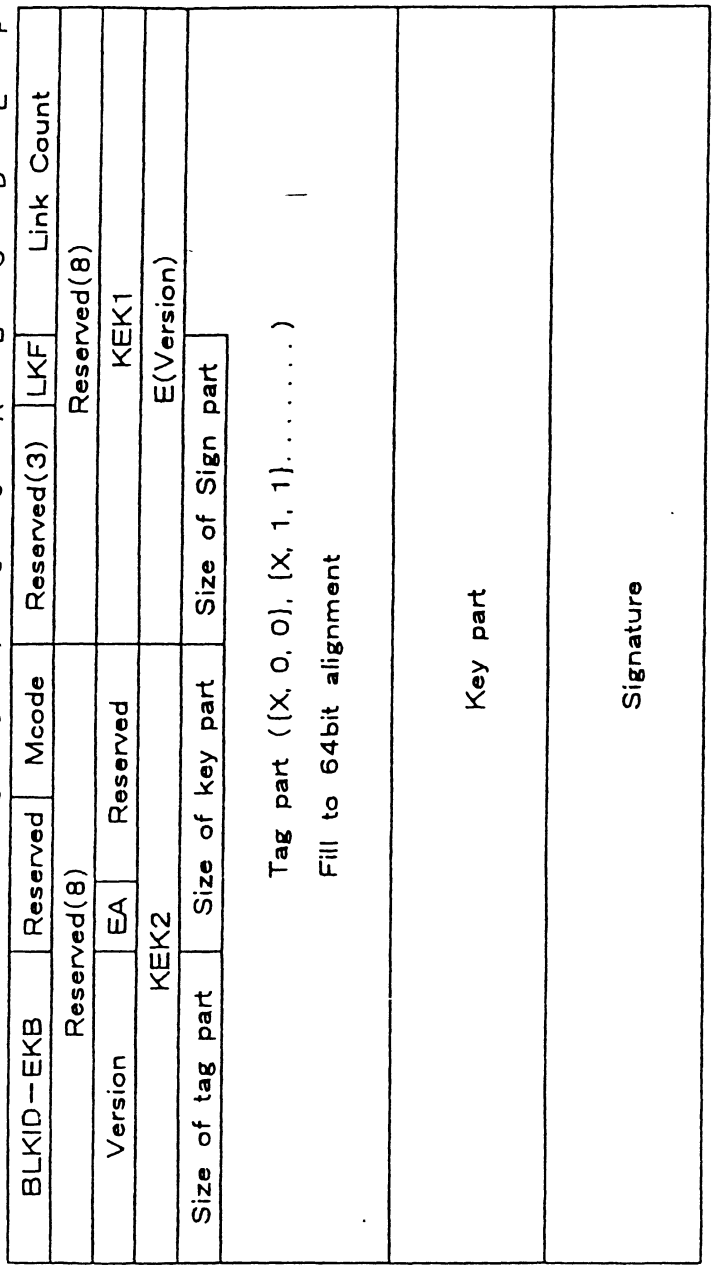
利用 ISO/IEC9798-2 對稱密碼編碼技術之相互認證以及密碼共有方式

第 30 圖

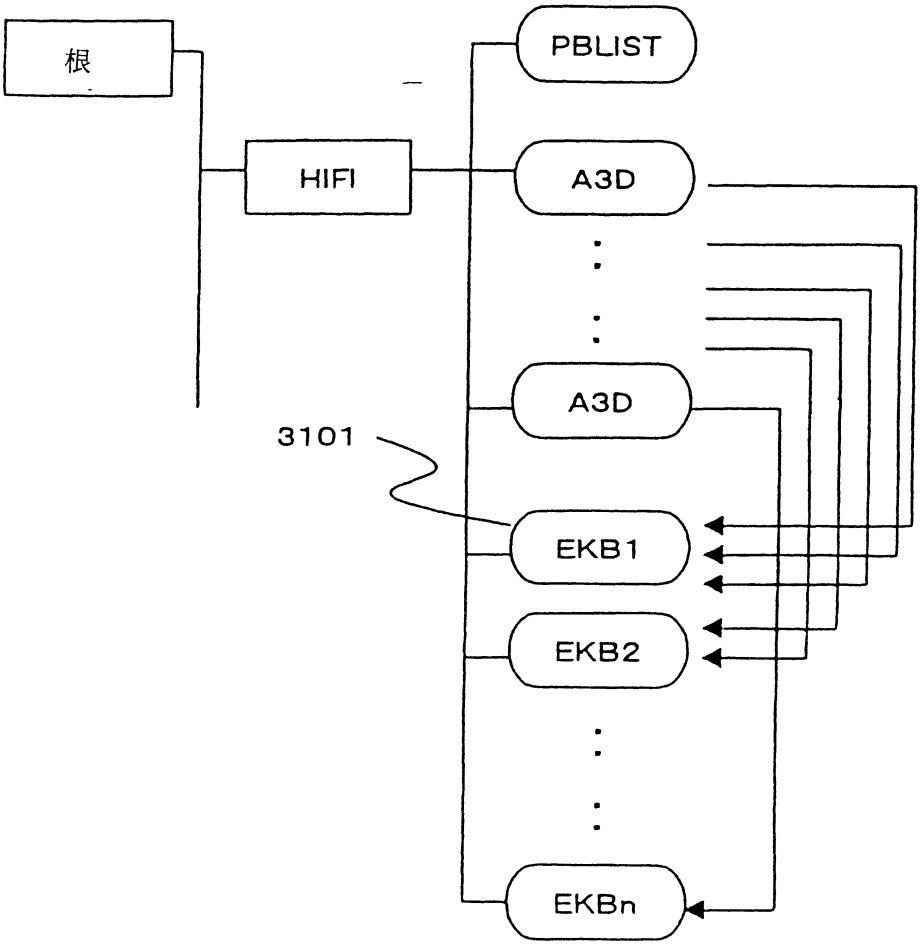

再生裝置
記憶裝置
開始
S2901
相互認證處理以及產生會期密碼 Kses
S2902
相互認證處理以及產生會期密碼 Kses
S2903
認證成立
否
是
S2904
將資料檔案送到再生裝置
S2905
判別在資料檔案中之內容密碼 Kcon的儲存形態
S2906
是否有 E(KEK,Kcon)?
否
是
S2907
根據 EKB 處理取出 KEK,而根據 KEK,對 E(KEK,Kcon)實施解碼而取得 Kcon
S2908
根據儲存密碼對 E(Kstm,Kcon)實施解碼,而將根據會期密碼 Kses 經編碼的 E(Kses,Kcon)送到再生裝置
S2909
根據會期密碼對 E(Kses,Kcon)實施解碼而取得 Kcon
S2910
利用 Kcon 對內容實施解碼
結束

第 31 圖

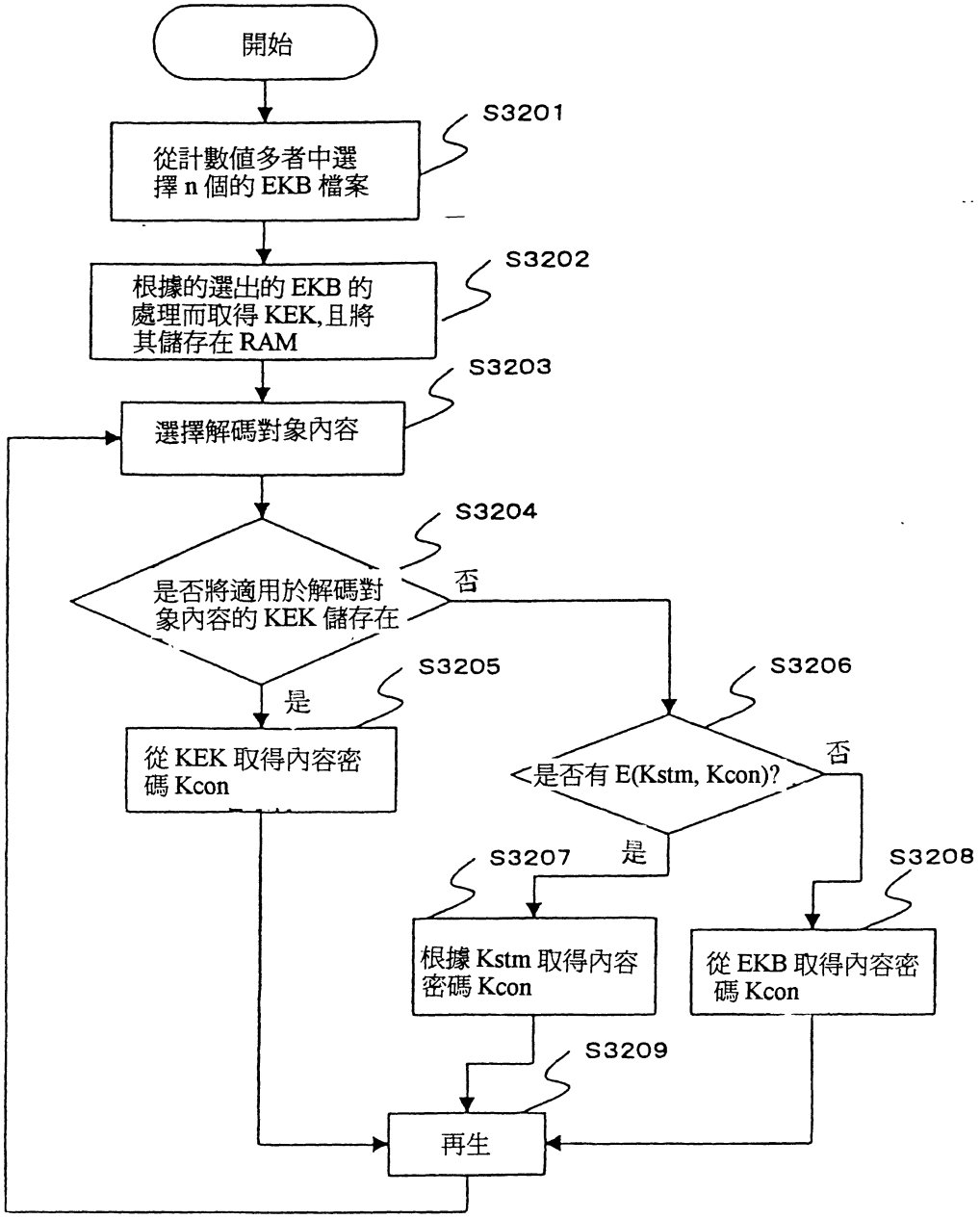
配送密碼允許資訊檔案



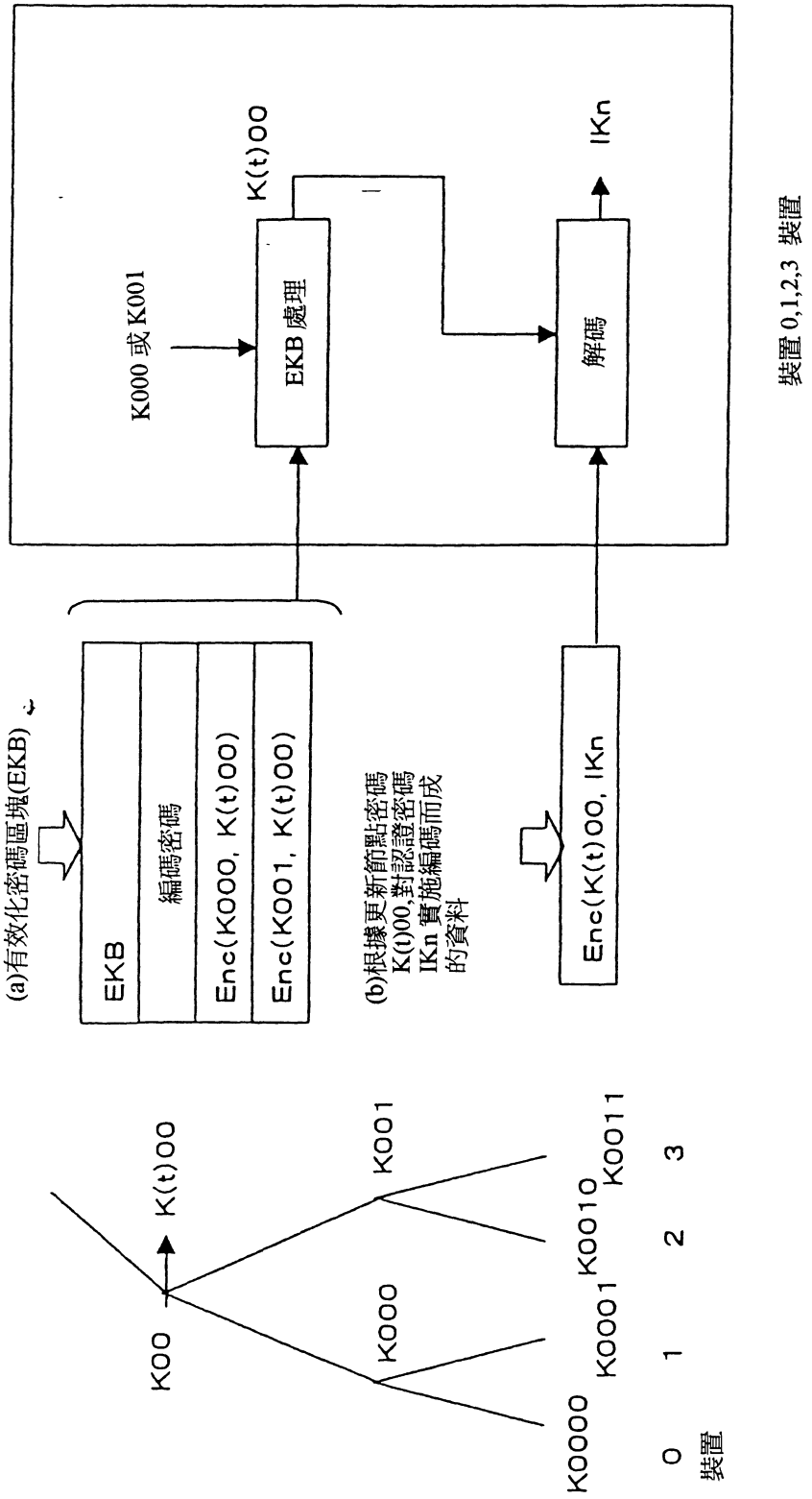
第 32 圖



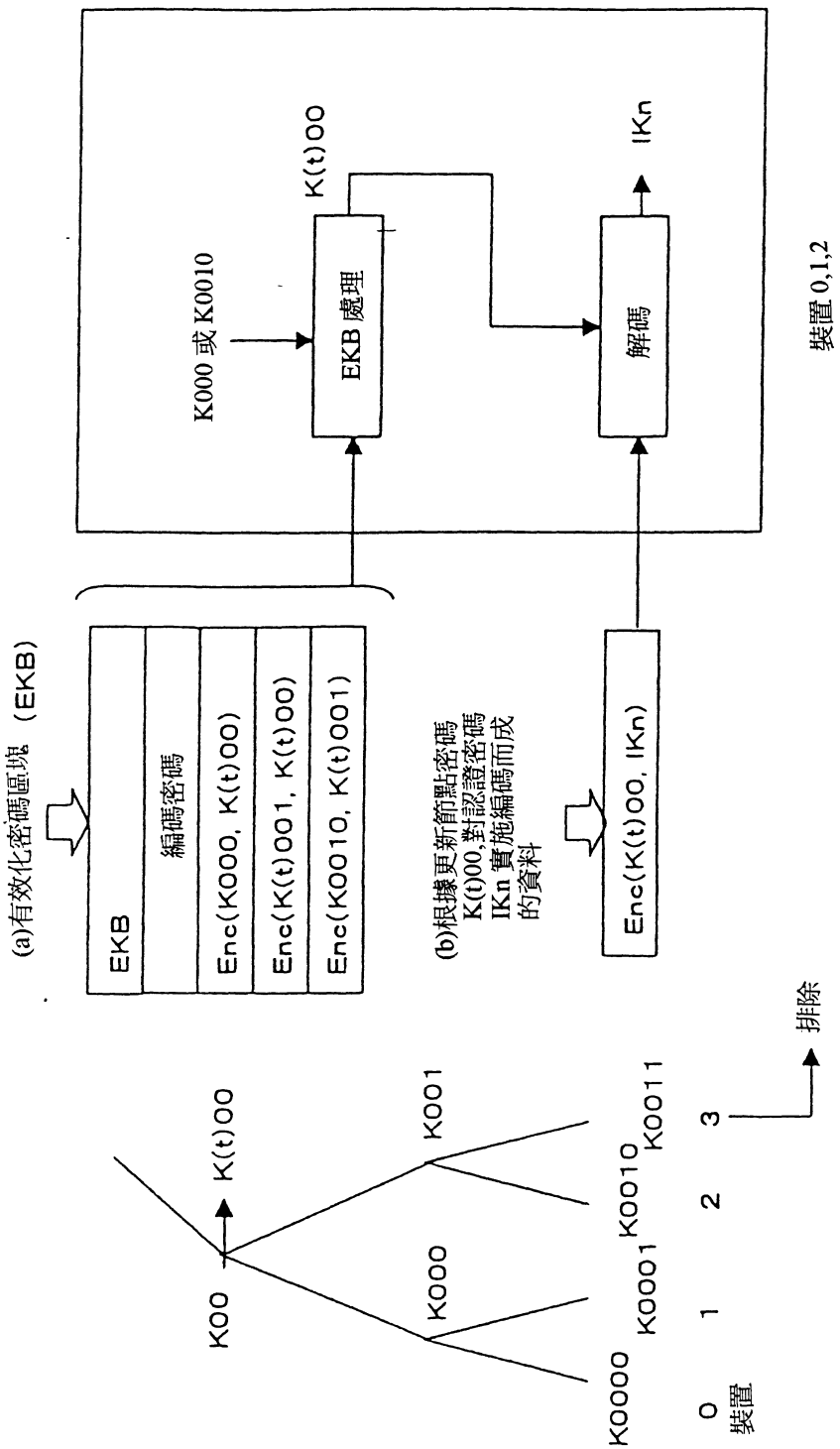
第 33 圖


開始
S3201
從計數值多者中選擇 n 個的 EKB 檔案
S3202
根據的選出的 EKB 的處理而取得 KEK, 且將其儲存在 RAM
S3203
選擇解碼對象內容
S3204
是否將適用於解碼對象內容的 KEK 儲存在
否
是
S3205
從 KEK 取得內容密碼 Kcon
S3206
<是否有 E(Kstm, Kcon)?
否
是
S3207
根據 Kstm 取得內容密碼 Kcon
S3208
從 EKB 取得內容密碼 Kcon
S3209
再生

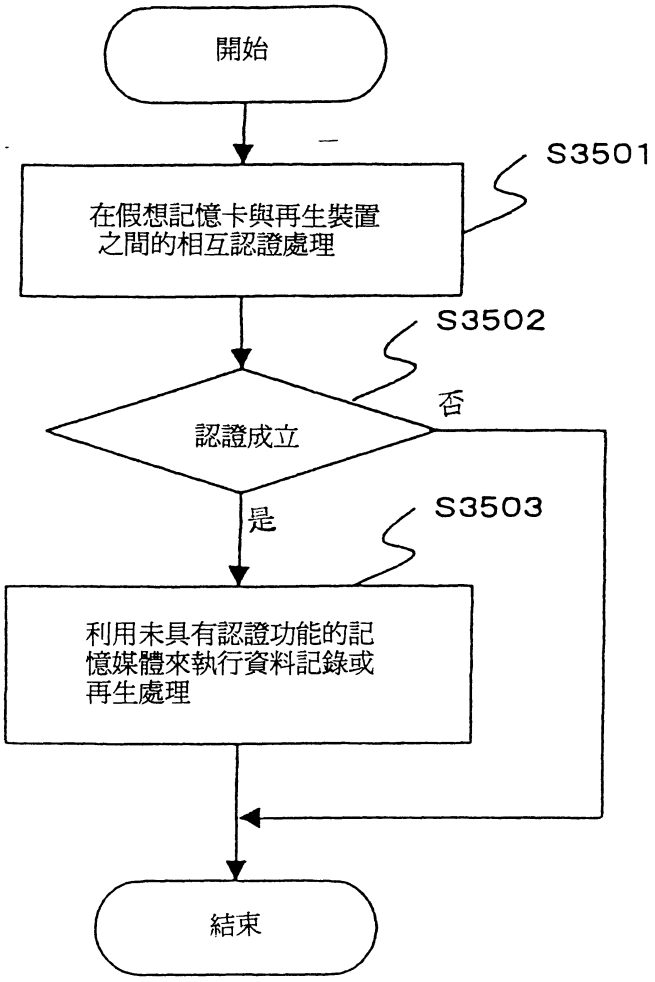
第 34 圖


(a)有效化密碼區塊(EKB)
EKB
編碼密碼
Enc(K000, K(t)00)
Enc(K001, K(t)00)
K000 或 K001
EKB 處理
K(t)00
(b)根據更新節點密碼
K(t)00,對認證密碼
IKn 實施編碼而成
的資料
Enc(K(t)00, IKn
解碼
IKn
裝置 0,1,2,3 裝置
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
裝置

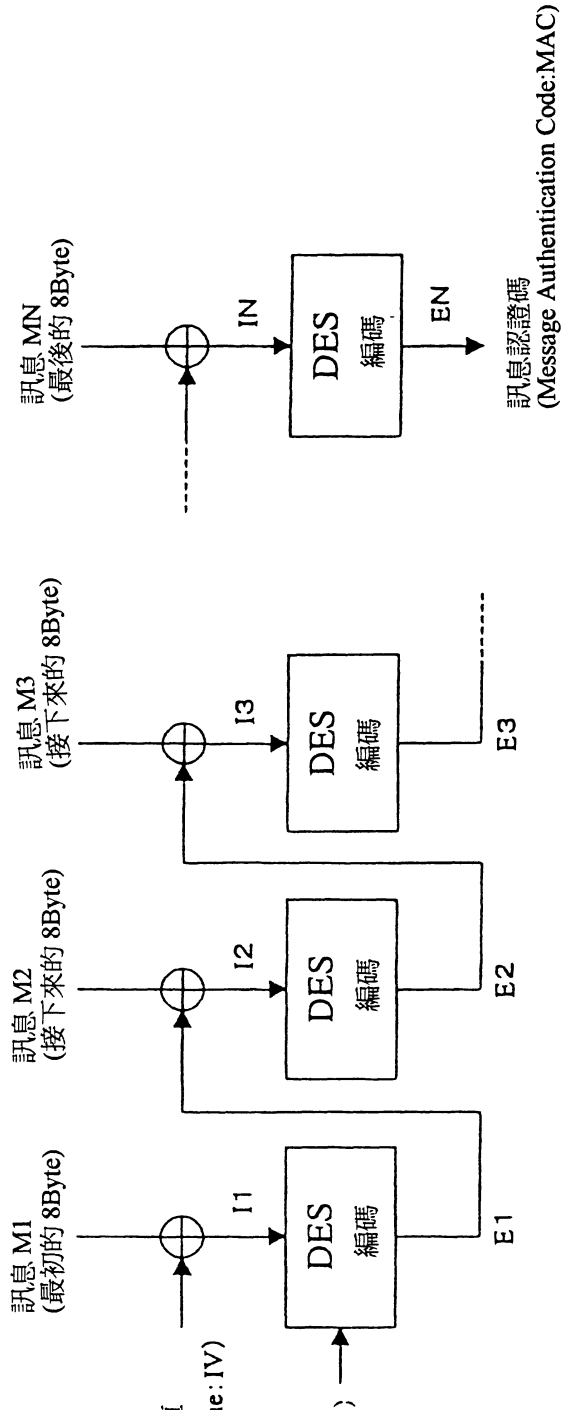
第 35 圖


(a)有效化密碼區塊（EKB）
EKB
編碼密碼
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
(b)根據更新節點密碼
K(t)00,對認證密碼
IKn 實施編碼而成
的資料
Enc(K(t)00, IKn)
K000 或 K0010
EKB 處理
K(t)00
解碼
IKn
裝置 0,1,2
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
裝置
1
2
3
排除

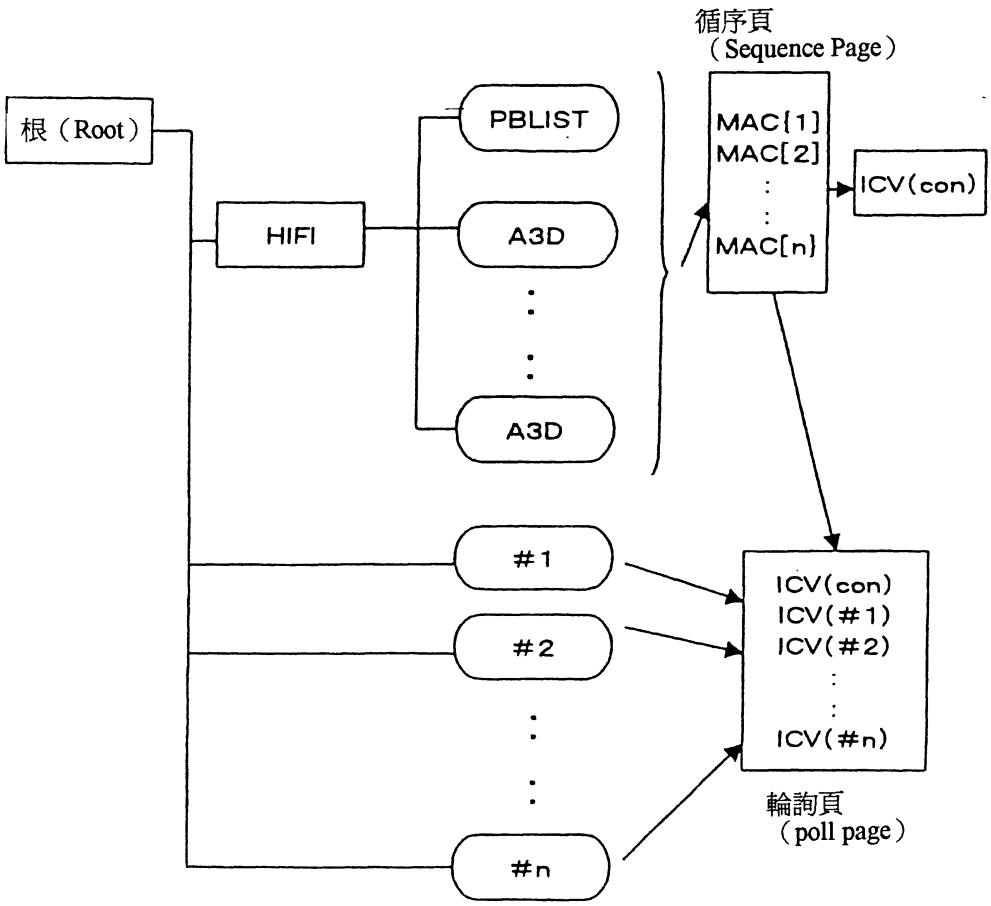
第 36 圖


開始
S3501
在假想記憶卡與再生裝置之間的相互認證處理
S3502
認證成立
否
是
S3503
利用未具有認證功能的記憶媒體來執行資料記錄或再生處理
結束

第 37 圖

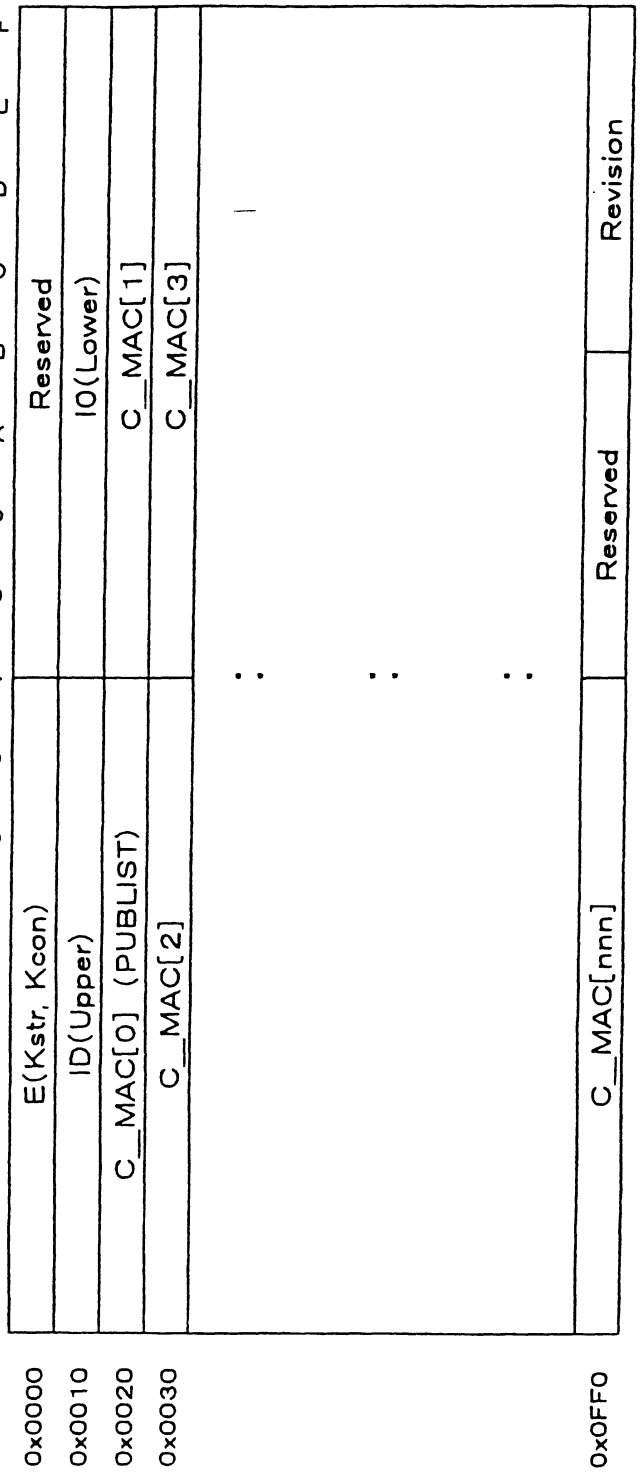

訊息 M1
(最初的 8Byte)
訊息 M2
(接下來的 8Byte)
訊息 M3
(接下來的 8Byte)
訊息 MN
(最後的 8Byte)
初始值
(Initial Value: IV)
密碼(K1)
I1
I2
I3
IN
DES
編碼
E1
E2
E3
EN
訊息認證碼
(Message Authentication Code:MAC)
⊕ 排他性邏輯和處理（8位元組單位）

第 38 圖


循序頁
（Sequence Page）
根（Root）
PBLIST
HIFI
A3D
A3D
MAC[1]
MAC[2]
MAC[n]
ICV(con)
#1
#2
#n
ICV(con)
ICV(#1)
ICV(#2)
ICV(#n)
輪詢頁
（poll page）

第 39 圖

循序頁格式
(Sequence Page Format)

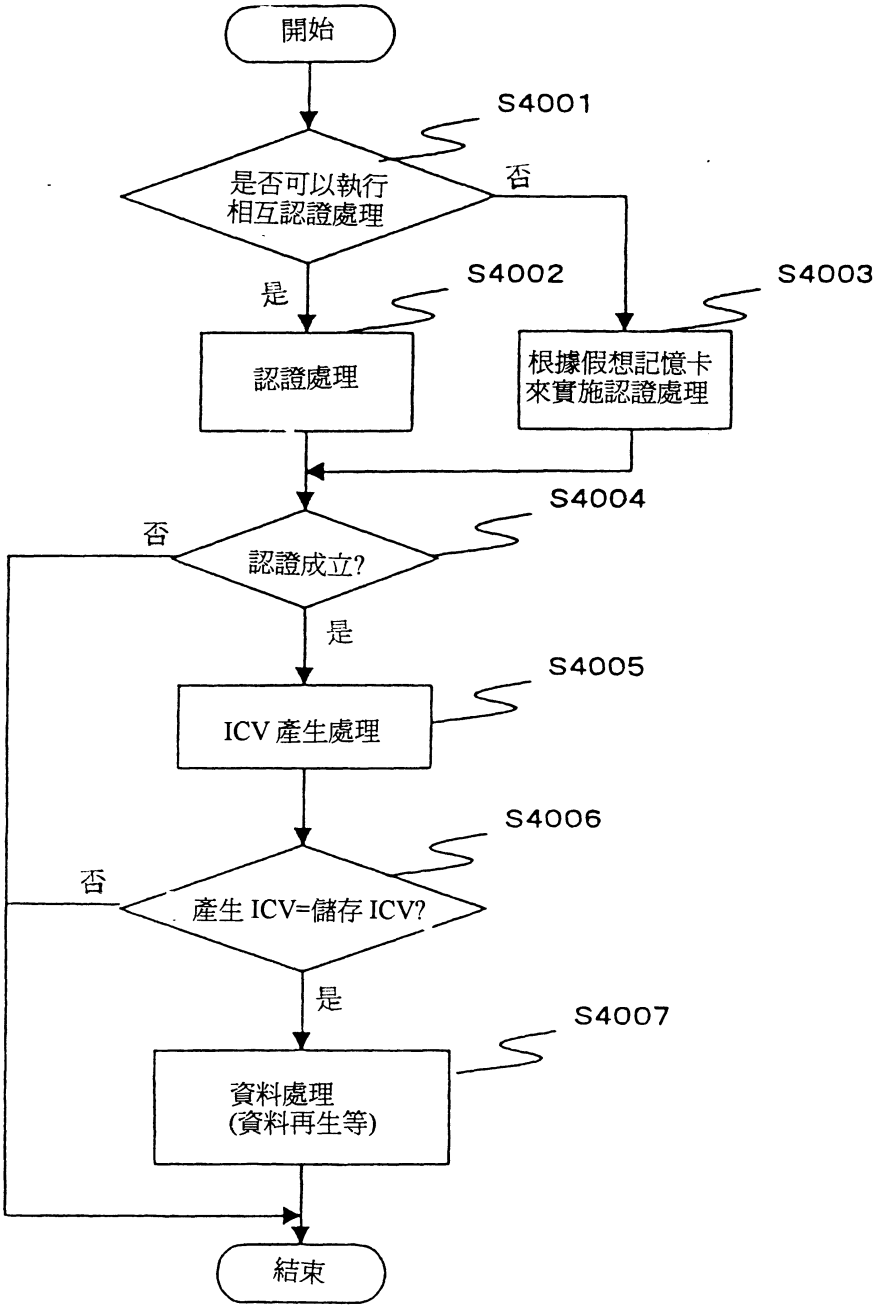


第 40 圖

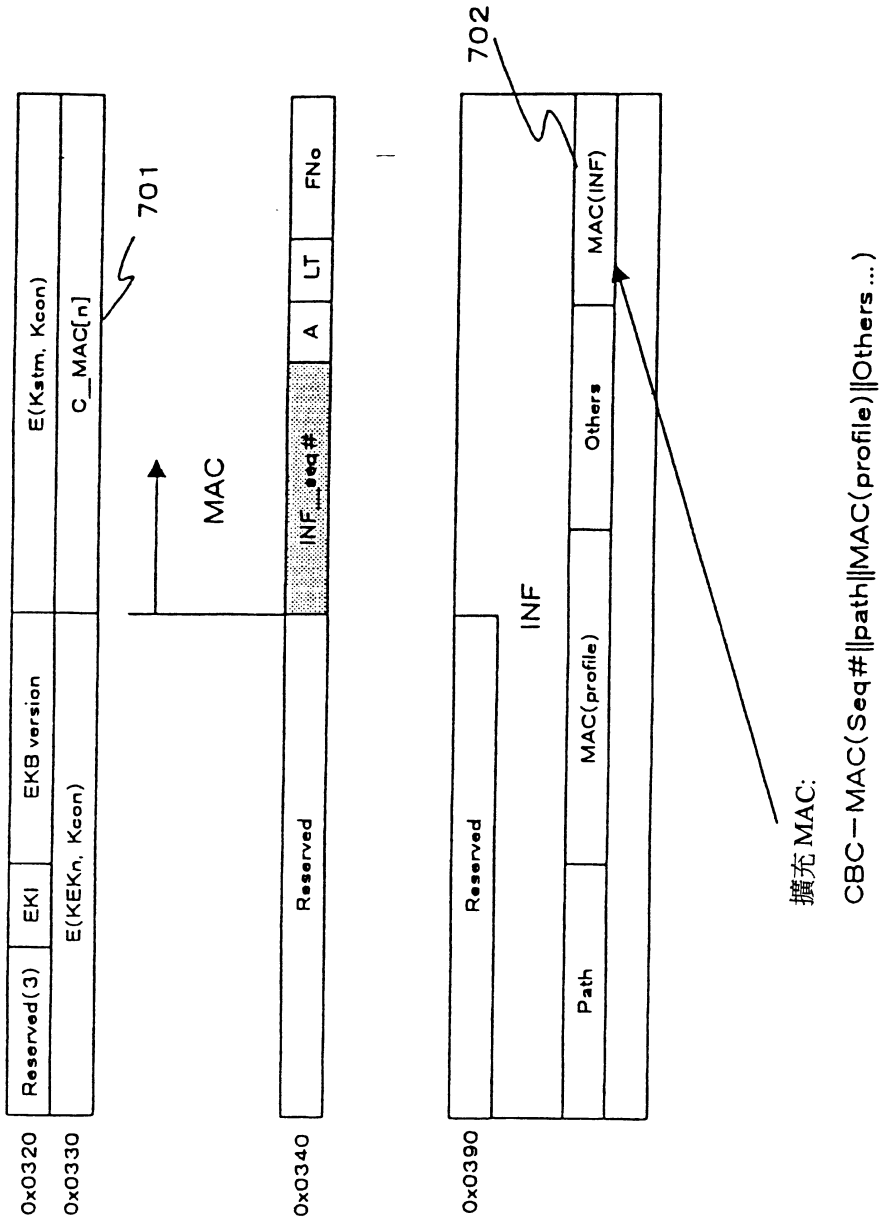
輪詢頁格式(Poll Page Format)

	0 1 2 3 4 5 6 7	8 9 A B C D E F
0x0000	#0_revision / #0_EKB version	#0_E(KEK, Kicv)
0x0010	#0_E(KEK, Kicv)	ICV0
0x0020	#1_revision / #1_EKB version	#1_E(KEK, Kicv)
0x0030	#1_E(KEK, Kicv)	ICV1
	⋮	
0x01E0	#15_revision / #15_EKB version	#15_E(KEK, Kicv)
0x01F0	#15_E(KEK, Kicv)	ICV15

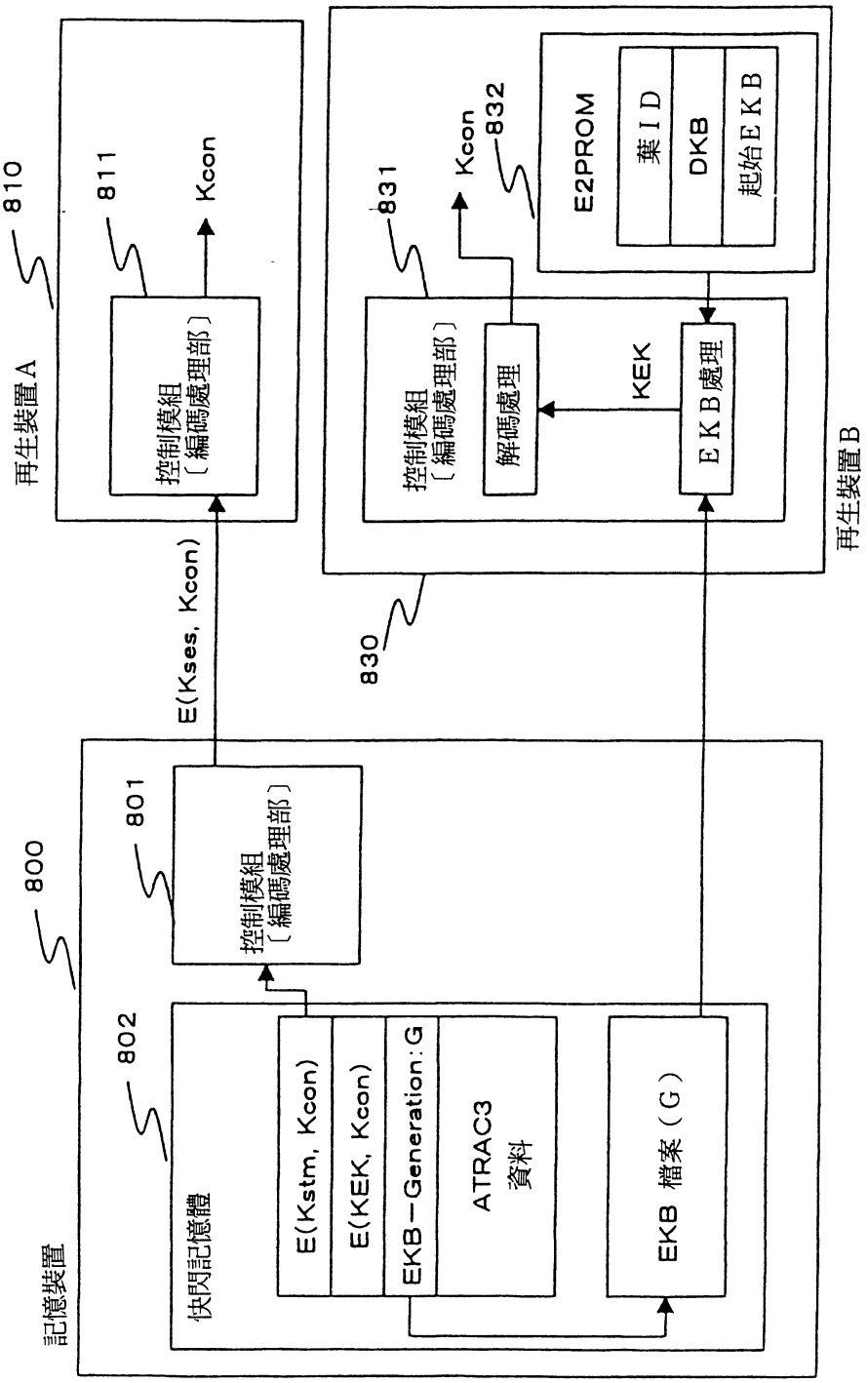
第 41 圖


開始
S4001
是否可以執行
相互認證處理
否
是
S4002
認證處理
S4003
根據假想記憶卡
來實施認證處理
S4004
否
認證成立?
是
S4005
ICV 產生處理
S4006
否
產生 ICV=儲存 ICV?
是
S4007
資料處理
(資料再生等)
結束

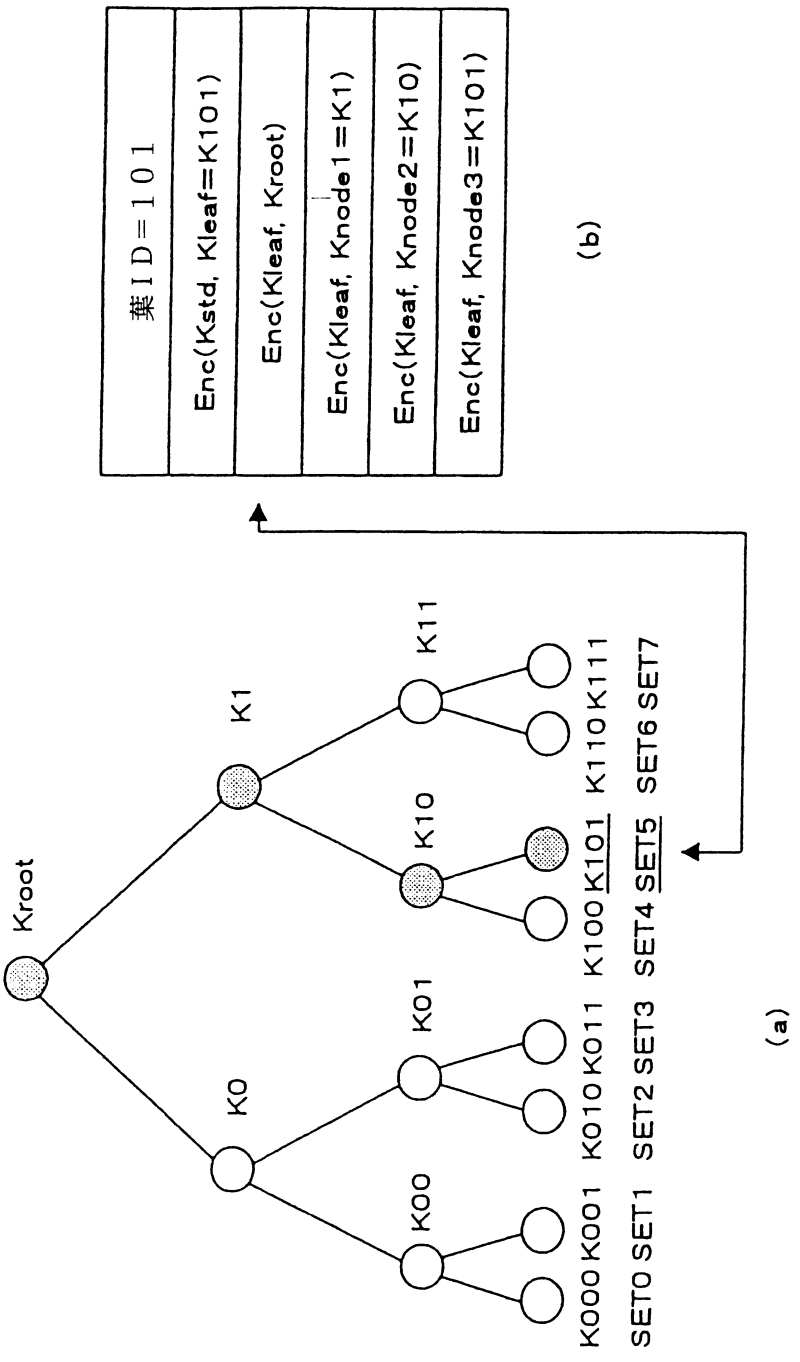
第 42 圖


0x0320
0x0330
Reserved(3)
EKI
EKB version
E(Kstm, Kcon)
E(KEKn, Kcon)
C_MAC[n]
701
MAC
0x0340
Reserved
INF_seq#
A
LT
FNo
0x0390
Reserved
INF
Path
MAC(profile)
Others
MAC(INF)
702
擴充 MAC:
CBC−MAC(Seq#||path||MAC(profile)||Others...)

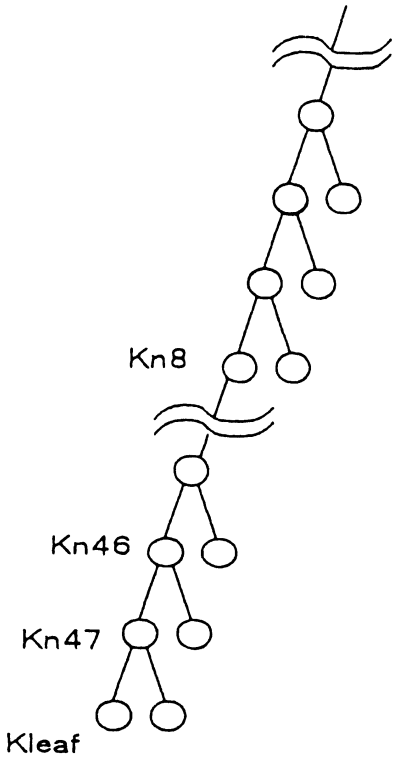
第 43 圖


記憶裝置
800
801
控制模組
〔編碼處理部〕
802
快閃記憶體
E(Kstm, Kcon)
E(KEK, Kcon)
EKB-Generation:G
ATRAC3
資料
EKB 檔案（G）
E(Kses, Kcon)
再生裝置A
810
811
控制模組
〔編碼處理部〕
Kcon
830
再生裝置B
831
控制模組
〔編碼處理部〕
解碼處理
KEK
E K B處理
Kcon
832
E2PROM
葉 I D
DKB
起始E K B

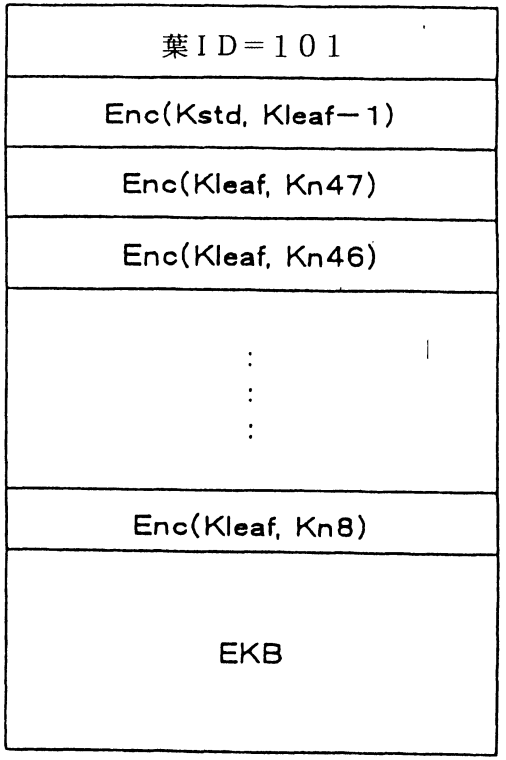
第 44 圖


Kroot
K0
K1
K00
K01
K10
K11
K000 K001 K010 K011 K100 K101 K110 K111
SET0 SET1 SET2 SET3 SET4 SET5 SET6 SET7
(a)
葉 I D = 1 0 1
Enc(Kstd, Kleaf=K101)
Enc(Kleaf, Kroot)
Enc(Kleaf, Knode1=K1)
Enc(Kleaf, Knode2=K10)
Enc(Kleaf, Knode3=K101)
(b)

第 45 圖

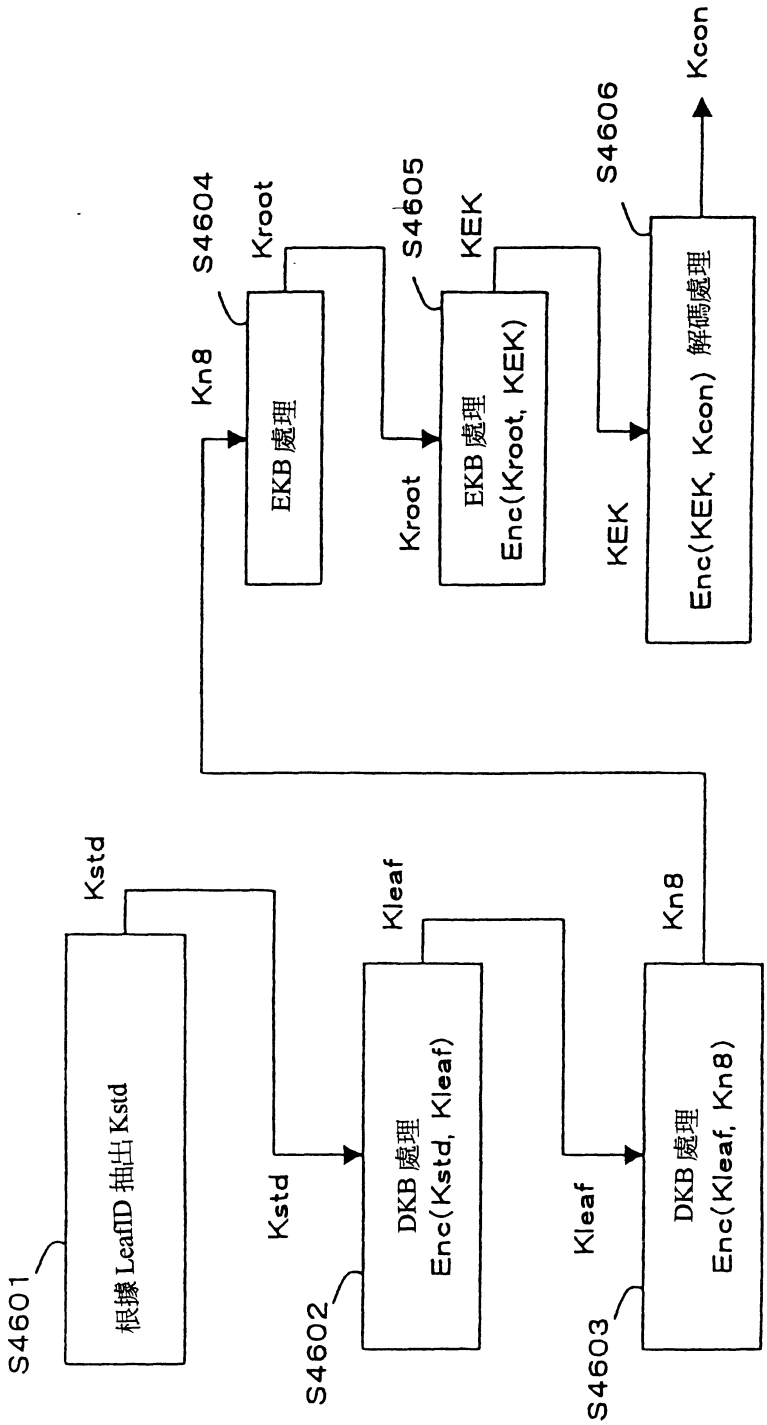

Kn8
Kn46
Kn47
Kleaf

(a)


葉ＩＤ＝１０１
Enc(Kstd, Kleaf−1)
Enc(Kleaf, Kn47)
Enc(Kleaf, Kn46)
Enc(Kleaf, Kn8)
EKB

(b)

第 46 圖


S4601
根據 LeafID 抽出 Kstd
Kstd
S4602
DKB 處理
Enc(Kstd, Kleaf)
Kleaf
S4603
DKB 處理
Enc(Kleaf, Kn8)
Kn8
S4604
EKB 處理
Kn8
Kroot
S4605
EKB 處理
Enc(Kroot, KEK)
Kroot
KEK
S4606
Enc(KEK, Kcon) 解碼處理
KEK
Kcon