

發明專利說明書 200423668

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：92133605

※申請日期：92 年 11 月 28 日

※IPC 分類：H04L 9/00 ,
G11B 7/007

壹、發明名稱：

(中) 內容資料管理方法，記錄且／或複製裝置，以及記錄媒體

(外) Content management method, recording and/or reproducing apparatus,
and recording medium

貳、申請人：(共 1 人)

1. 姓 名：(中) 東芝股份有限公司

(英) KABUSHIKI KAISHA TOSHIBA

代表人：(中) 1. 岡村正

(英)

地 址：(中) 日本國東京都港區芝浦一丁目一番一號

(英)

國籍：(中英) 日本 JAPAN

參、發明人：(共 5 人)

1. 姓 名：(中) 小島正

(英) KOJIMA, TADASHI

地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式會社東芝 知的
財產部內

(英)

2. 姓 名：(中) 山田尚志

(英) YAMADA, HISASHI

地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式會社東芝 知的
財產部內

(英)

3. 姓 名：(中) 加藤拓

(英) KATO, TAKU

地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式會社東芝 知的
財產部內

(英)

4. 姓 名：(中) 石原淳
(英) ISHIHARA, ATSUSHI
地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式会社東芝 知的
財產部內
(英) _____

5. 姓 名：(中) 平良和彥
(英) TAIRA, KAZUHIKO
地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式会社東芝 知的
財產部內
(英) _____

肆、聲明事項：

◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 日本 _____； 2002/11/29； 2002-348925 ☒ 有主張優先權 _____

4. 姓 名：(中) 石原淳
(英) ISHIHARA, ATSUSHI
地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式會社東芝 知的
財產部內
(英) _____

5. 姓 名：(中) 平良和彥
(英) TAIRA, KAZUHIKO
地 址：(中) 日本國東京都港區芝浦一丁目一番一號 株式會社東芝 知的
財產部內
(英) _____

肆、聲明事項：

◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 日本 _____； 2002/11/29； 2002-348925 ☒ 有主張優先權 _____

(1)

玖、發明說明

【發明所屬之技術領域】

本發明關於管理內容資料的內容管理方法和使用方法
方法的記錄／複製裝置；及記錄有內容資料的記錄媒體。
詳言之，本發明關於內容管理方法、進行內容資料預定移
動並防止無限制非法拷貝的記錄／複製裝置、用於該方法
和裝置的記錄媒體。

【先前技術】

傳統上，關於記錄數位資訊（例如文件、聲音、影像、
程式）的媒體，CD或LD用於記錄聲音或影像的媒體。
此外，軟碟或硬碟用於電腦中記錄程式或資料的媒體。除
了這些記錄媒體外，也發展出大容量記錄媒體的DVD。

各種數位記錄媒體中，記錄數位資料（包含可解碼的
編碼或壓縮資料）。因此，記錄資料可輕易從一媒體拷貝
到另一媒體而不失真。因此，這些數位記錄媒體中，有可
產生大量拷貝的問題，造成著作權侵害。

目前，關於技術的內容加密／解密法（日本特開
No. 09-136709），稱為CSS（內容鎖碼系統）的著作權保
護系系導入專用於複數的DVD，以防內容的非法拷貝。

但上述傳統裝置中，進行內容移動，並防止非法拷貝
及保護著作權，同時，傳統複數裝置不能進行內容複製。
亦即，不能確保使用者的方便。

(2)

【發明內容】

發明概述

本發明的實施例提供內容管理方法、記錄／複製裝置、記錄媒體，可移動內容並防止內容散播，在傳統通用裝置確保最小複製相容性。

依據本發明，為解決上述問題，提供一種內容管理方法，包括：內容資料被第一鑰（TK）加密；第一鑰被預定多種第二鑰（MUK）加密；加密的第一鑰（Enc-TK）被第三鑰（MM）多重加密；第三鑰被預定第四鑰（MMK）加密；在記錄媒體記錄被第一鑰加密的內容資料（Enc-Contents）、被預定多種第二鑰加密的第一鑰（Enc-TK）、加密的第一鑰（Enc-TK）被第二和第三鑰（MM）多重加密所得的第一鑰（Enc2-TK），被第四鑰加密的第三鑰（Enc-MM）記錄於記錄媒體的安全區。

依據本發明，如上述，在記錄媒體記錄多重加密的第一鑰（Enc2-TK），以預定限制來移動內容，該鑰是控制內容移動之加密鑰的移動鑰（Move-Key），也是被第二和第三鑰多重加密加密鑰所得的標題鑰。另一方面，不需對應於移動鑰（Move-Key）的專用機，媒體鑰（Enc-TK）（只被第二鑰（MKB，M-ID）加密一次之具有標題鑰（TK）的媒體限制標題鑰）也記錄於不同區，以使傳統通用機內容。依此方式，媒體鑰（Enc-TK）引發通用機複製，移動鑰（Move-Key）移動內容，同時防止內容資料散播。

(3)

依據本發明，有一種內容管理方法，其中允許記錄媒體間的移動時，若內容資料從內容資料源（S）記錄於第一記錄媒體（D1），則在第一記錄媒體（D1）記錄有（流程1）：被第一鑰（TK）加密的內容資料（Enc-Contents）；被第二鑰加密的第一鑰（Enc-TK），是限於記錄媒體的內容（MB-KEY）；被第二和第三鑰多重加密的內容移動控制加密鑰（Enc2-TK）；若內容資料從第一記錄媒體（D1）移到第二記錄媒體（D2），則內容資料在解密後重新加密，刪除記錄於第一記錄媒體的內容移動控制加密鑰。

本發明的內容管理方法特徵在於，有關上述兩鑰，亦即通用機複製的媒體鑰（Enc-TK）和移動內容的移動鑰（Move-Key），當內容資料從內容資料源（S）記錄到第一碟（D1）時，記錄兩鑰，藉以進一步移動內容，同時，可用之外的通用機來拷貝。當內容資料從第一碟（D1）移動第二碟（D2）時，從第一碟（D1）刪除移動鑰（Move-Key），只留下通用機複製的媒體鑰（Enc-TK）。依此方式，不能進一步移動，再者，隨後可進行通用機複製。當內容資料移到第二碟（D2）時，只記錄移動鑰（Move-Key），因此只引發專用機複製。再者，隨後可移到第三碟等。

本發明的內容管理方法提供內容管理方法、記錄／複製裝置、記錄媒體，由上述第一碟記錄設計和隨後移動設計可複製或移動內容資料；可移動內容資料並防止內容資

(4)

料散播；再者，在傳統通用機和專門機都可複製。

發明詳述

以下參照附圖來詳述本發明的內容管理方法、記錄／複製裝置、記錄媒體。圖1是方塊圖，描繪本發明之內容管理方法的加密例子。圖2和3是方塊圖，各顯示加密之內容之一般方法的解密例子。圖4顯示記錄有加密之內容的記錄媒體例子。圖5顯示本發明之內容管理方法之移動鑰（Move-Key；Enc2-TK）和媒體鑰（MB-Key；Enc2-TK）的移動例子。

〔本發明之內容管理方法的概述〕

參照附圖來概述本發明的內容管理方法。首先，說明加密／解密設計。本發明之內容管理方法的特性在於記錄媒體中記錄有：確保內容資料移動的移動鑰（Move-Key；Enc2-TK）、確保複製裝置之複製的媒體鑰（MB-Key；Enc2-TK）、及加密的內容資料。

〔加密〕

藉AV編碼器模組M1的工作和驅動器V1的工作，可說明本發明的內容管理方法中之加密／解密的設計。圖1的AV編碼器模組M1中，影像（V）或聲音（A）信號由編碼器12以DVD格式編碼，選擇器13選擇編碼的信號及數位資

(5)

料 11。然後，選擇的信號藉由標題鑰（TK）在鎖碼電路 14 進行鎖碼（加密）處理，處理的信號在碟 D 記錄成（Enc-Contents）。

此時，亂數產生器 18 產生標題鑰（TK）。解密的鑰 TK 在解碼器電路 20 由解密鑰（MUK）解密，產生解密的標題鑰（Enc-TK）。如下得到具有加密標題鑰（TK）的加密鑰（MUK）。藉由 MKB 處理器 17，使用從記錄媒體讀出的資料來處理裝置鑰 K1（DvK116）以產生媒體鑰（MMK），再者，在 MID 處理器 19 的處理後，產生所得的鑰。

再者，加密標題鑰（Enc-TK）被安全鑰（MM）多重加密，產生多重加密標題鑰（Enc2-TK），然後，連同加密標題鑰（Enc-TK）送到選擇器 27。

亂數產生器 24 供應安全鑰（MM）。依據記錄媒體的指定 MKB，驅動器 V1 的裝置鑰（DvK2）由 MKB 處理 23 進行 MKB 處理。安全鑰（MM）被所得的加密鑰（MMK）加密，得到加密的加密鑰（Enc-MM）。

在光碟 D 的記錄區記錄所得的加密內容資料（Enc-Contents）：標題鑰（Enc-TK）（= 被加密鑰（MUK）加密的媒體鑰（MB-Key））；及被第二和第三鑰多重編碼的標題鑰（Enc2-TK）（= 移動鑰（Move-Key））。再者，先前加密的第三鑰（Enc-MM）記錄於光碟 D 的安全區。圖 4 顯示將這些信號記錄到光碟 D 的例子。

依據記錄處理控制部之 R 控制 15 的控制信號，移動鑰

(6)

(Move - Key ; Enc2 - TK) 和 媒體 鑰 (MB - Key ; Enc2 - TK) 都 經由 選擇 器 27 記錄 到 光 碟 D 。

爲 由 另一 複製 裝置 達成 記錄 於 光 碟 記錄 媒體 之 資訊 的 複製 和 交換 ， 以 多個 裝置 鑰 (DvK) 產生 相同 鑰 資訊 (MK) 。 再者 ， 媒體 特定 進行 媒體 限制 ， 以防 完全 拷 貝 到 另一 媒體 。

如下 述 ， 拷 貝 或 移動 內容 時 ， 二 加密 鑰 ， 亦 即 移動 鑰 (Move - Key ; Enc2 - TK) 和 選擇 性 記錄 於 光 碟 D ， 藉 以 在 移動 限制 性 內容 資料 的 預定 條件 或 處理 下 由 通用 機 複製 。

(二 種 複製 設計)

關於 圖 4 之 記錄 有 加密 之 內容 資料 的 光 碟 D 和 加密 的 鑰 資訊 ， 如下 ， 傳統 通用 光 碟 複製 裝置 可 複製 至少 記錄 有 一 媒體 鑰 (MB - Key ; Enc - TK) 的 光 碟 D 。 再者 ， 只有 實施 本 發明 之 內容 管理 方法 的 光 碟 複製 裝置 複製 只 記錄 有 移動 鑰 (Move - Key ; Enc2 - TK) 的 光 碟 D 。

亦 即 ， 圖 2 顯示 只用 本 發明 的 媒體 鑰 (MB - Key ; Enc - TK) 以 傳統 機 的 複製 裝置 來 執行 解密 處理 。 此 圖 中 ， 在 至少 記錄 有 一 媒體 鑰 (MB - Key ; Enc - TK) 的 光 碟 D ， 預 先 記錄 於 媒體 的 媒體 鑰 方 塊 資訊 (MKB) 和 媒體 特定 資訊 (M - ID) 及 媒體 鑰 (MB - Key ; Enc - TK) 經由 匯 流 排 鑑定 21 送 到 AV 解 碼 器 模組 M2 。 再者 ， 加密 內容 資料 (Enc - Contents) 送 到 AV 解 碼 器 模組 M2 。

(7)

加密的內容資料 (Enc - Contents) 要在解鎖碼器 29 由標題鑰 (TK) 解鎖碼，所得資料在送到 AV 解碼器 30 後複製。從碟 D 讀出加密標題鑰 (Enc - TK)，送到解密部 28，被加密鑰 (MUK) 解密，得到標題鑰 (TK)。此外，根據媒體鑰方塊資訊 (MKB) 和媒體特定資訊 (M - ID)，MKB 處理器 17 和 MID 處理器 19 獲得加密鑰 (MUK)。

依此方式，即使在非本發明的內容資料管理方法的傳統光碟複製裝置，也可複製包含在記錄有媒體鑰 (MB - Key ; Enc - TK) 之光碟 D 的內容資料。

另一方面，如圖 3，只指定移動鑰 (Move - Key ; Enc2 - TK) 的光碟 D 中，執行本發明之內容資料管理方法的處理，藉以複製。

亦即，使用 MKB 處理 23 所得之鑰 (MMK) 由解密部 31 解密，從光碟單元指派媒體鑰方塊資訊 (MKB)、加密標題 (Enc - MM)、多重加密標題鑰 (Enc2 - TK)、加密內容 (Enc - Contents) 的驅動器 V1 得到安全鑰 (MM)。依此方式，多重加密標題鑰 (Enc2 - TK) 解密成加密標題鑰 (Enc - TK)，經由匯流排鑑定 21 送到模組 M2。

模組 M2 中，模組 M2 特定的裝置鑰 (DvK) 根據媒體鑰方塊資訊 (MKB) 進行 MKB 處理 17，根據媒體特定資訊 (M - ID)，加密標題 (Enc - TK) 在解密部 28 由進行 MID 處理 19 所得的加密鑰 (MUK) 解密，藉以得到標題鑰 (TK)。

使用標題鑰 (TK)，加密的內容資料 (Enc -

(8)

Contents) 被解鎖碼部 29 解密，因此內容資料可送到 AV 解碼器 30。

依此方式，只指定移動鑰 (Move-Key; Enc2-TK) 的碟 D 中，只有執行本發明之內容資料管理方法之處理的光碟記錄／複製裝置可複製或移動。

[本發明之內容管理方法的移動內容]

由實例來說明本發明之內容資料管理方法之移動內容資料的設計。圖 5 中，在本發明之內容資料管理方法，使用二種鑰，亦即移動鑰 (Move-Key; Enc2-TK) 和媒體鑰 (MB-Key; Enc-TK)，這些鑰記錄於記錄媒體，因此可限制複製、拷貝、移動。亦即，依據本發明之內容資料管理方法，存在諸如光碟的三種記錄媒體、"媒體鑰 (MB-Key) 和移動鑰 (Move-Key)"、"只有媒體鑰 (MB-Key)"、"只有移動鑰 (Move-Key)"。此處不說明內容資料，只說明二種鑰，亦即媒體鑰和移動鑰。

圖 5 中，關於拷貝受限的源內容，媒體鑰 (MB-Key) 和移動鑰 (Move-Key) 指定給第一碟 D1 (記錄媒體)。依此方式，本發明的複製裝置和一般複製裝置可複製。

接著，若碟 D1 的內容資料由本發明的複製裝置移到新碟 D2，則從碟 D1 刪除移動鑰 (Move-Key)，得到只有媒體鑰 (MB-Key) 的碟 D1'。只有移動鑰 (Move-Key) 記錄於新碟 D2。依此方式，只有一般複製裝置可複製碟 D1'。此外，一般複製裝置不能複製碟 D2。只有本

(9)

發明的記錄／複製裝置可複製或處理此碟。

再者，若做為移動鑰（Move－Key）之2的內容資料，則本發明的複製裝置刪除光碟D2的移動鑰（Move－Key），不能再度複製。只有移動鑰（Move－Key）記錄於光碟D3，只有本發明的記錄／複製裝置可複製或處理此碟。

再者，本發明的記錄／複製裝置從光碟D的移動內容資料時，目標不限於光碟。諸如SD（安全數位）的一般數位記錄媒體也可。移動鑰（Move－Key）可從光碟D3移到SD（安全數位）卡D4。如同從光碟D2移到光碟D3的情形，從光碟D3刪除移動鑰（Move－Key），不能複製。只有移動鑰（Move－Key）記錄於SD（安全數位）卡D4，只有本發明的記錄／複製裝置可複製或處理此碟。

〔本發明之內容管理方法的應用例〕

參照附圖來詳述本發明的內容管理方法用於特定光碟記錄／複製裝置的實施例。圖6是方塊圖，描繪應用本發明實施例之內容管理方法之記錄／複製裝置的結構例子。圖7是方塊圖，顯示用於記錄／複製裝置的加密設計詳細例子。圖8是方塊圖，顯示解密設計詳細例子。

〔記錄／複製裝置〕

圖6顯示應用本發明實施例之內容管理方法的光碟記錄／複製裝置A。光碟記錄／複製裝置具有控制部，包

(10)

括：管理整個作業的系統控制部162、做為工作區的RAM161、ROM160、伺服控制部152。再者，此裝置有將雷射束照到光碟D的光讀取頭154，和接收複製之偵測信號或供應記錄信號的信號處理部156，藉以執行ECC處理等。裝置A有圖1的匯流排鑑定21。再者，裝置同樣有經由纜線提供的匯流排鑑定21，和執行編碼或解碼的資料處理部158。外，做為諸如SD卡之記錄媒體之介面的媒體寫寫器166接到信號處理部156。介面165接到資料處理部158。再者，裝置A有：接到上述伺服控制部152的伺控制系統處理器電路155、相連的致動驅動器153、碟馬達151。

有此組態的光碟單元A中，系統控制部162使用RAM161做為工作區，依據包含本發明的程式執行預定作業，程式記錄於ROM160。從光讀取頭154輸出的雷射束照到光碟D。光碟D的反射光由頭放大器轉變成電信號。此電信號輸入信號處理部156。RF放大器包含在信號處理部156。

在記錄作業，參照圖1所述的加密處理用於內容資料，對光碟D執行記錄處理。詳言之，使用經由寫入聲道電路（未示出）所產生的寫入時脈，資料處理部158指配偵錯碼（EDC）或ID給經由介面165所送的內容資料，使用上述編碼來應用資料鎖碼處理。再者，使用與媒體相容的雷射束，此資料處理部指配改錯碼（ECC），指配同步信號，調變同步信號除外的信號，將信號記錄於光碟D。

在複製作業，參照圖2和3所述的解碼處理用於內容資

(11)

料，對存入光碟D的內容資料執行複製處理。詳言之，從光讀取頭154之頭放大器讀出的RF信號經由最佳等化器送到信號處理部156的PLL電路（未示出）。PLL電路所產生的讀取時脈讀出聲道資料。使用上述解密的解密處理用於讀取資料。再者，解密的資料被資料處理部158同步化，讀出符號資料。然後，執行使用改錯或上述解密處理的解鎖碼處理，解鎖碼的資料經由介面165轉到外部。

依此方式，上述光碟記錄／複製裝置A應用記錄處理和複製處理。

此外，信號處理部156和資料處理部158各有匯流排鑑定部21，防止第三人切斷纜線來抽取信號及試圖非法盜拷。依此方式，此產生器產生相同加密鑰，加密傳輸資訊，傳到遠端。收到傳輸信號的遠端裝置由當地產生的相同加密鑰將加密的傳輸資訊解密。依據預定時間，改變及產生此加密鑰，因此第三人難以複製。只要此時不能複製加密鑰，即使纜線切斷來抽取信號，也不能非法拷貝內容資料。

[調變／解調處理之加密鑰的安全]

此處說明應用信號處理部156所執行之調變器／解調器電路作業之加密鑰資訊的安全處理。在圖7之記錄處理之內容管理方法的主要部分，AV編碼器模組M1與圖1相同。在圖8之記錄處理之內容管理方法的主要部分，AV解碼器模組M2與圖3相同。此處省略重複說明。

(12)

在圖7的驅動器V3，除了圖1的驅動器V1組態，也顯示ECC電路。亦即，當ECC電路43指定改錯信號時，調變器電路44調變內容鎖碼14的信號。再者，ECC電路47也將加密的安全鑰（Enc-MM）改錯編碼，第二調變器電路48調變加密鑰。然後，調變的鑰被選擇器44以部分的主資料取代，由寫入聲道電路46記錄於光碟D的儲存區。

一方面，在圖8的驅動器V4，從光碟D讀出指定改錯碼的資料，第二解調器電路45解調讀出的資料。然後，ECC電路46可抽取加密的安全鑰（Enc-MM）。另一方面，圖7中，使用異於調變器44的第二調變器48來調變及記錄加密的安全鑰（Enc-MM）。因此，在讀出部於解調器42不能解調加密的安全鑰（Enc-MM），鑰被處理成錯誤資料。依此方式，第三人不能為盜拷而抽取加密的安全鑰（Enc-MM）。如此應用調變／解調處理，可產生不被一般主資料調變處理測到的安全資訊。此外，在安全區記錄及複製加密的鑰資訊（Enc-MM）。依此方式，即使利用諸如光碟的記錄媒體，也可構成高水準的保護系統。

【實施方式】

〔移動流程圖1〕

由流程圖來詳述在記錄媒體間移動內容資料的處理。圖9是流程圖，顯示在記錄媒體D1記錄本發明之內容管理方法所加密之內容和鑰資訊的作業。圖10是流程圖，顯示內容從記錄媒體D1移到另一記錄媒體D2。圖11是流程圖

(13)

，顯示內容從記錄媒體 D2 移到另一記錄媒體 D3。圖 12 是流程圖，顯示以聲道下降來移動。

光碟記錄／複製裝置的信號處理部 156 和資料處理部 158 的組態達成本發明之內容管理方法，如上述。即使將內容管理方法用於偵測資訊，也可執行這些處理。下文中，藉流程圖來詳述本發明之內容管理方法。

圖 9 的流程圖中，說明內容資料從拷貝受限的內容資料 S 拷貝到諸如光碟 D 的記錄媒體 D1。

首先，從記錄媒體 D1 讀出產生鑰資訊的媒體鑰方塊資訊 (MKB) 和媒體特定資訊 (M-ID)，這些資訊轉移到 AV 編碼器部 M1 (S11)。然後，在 AV 編碼器部 M1，使用裝置特定解密鑰 (DvK1) 16，從媒體鑰方塊資訊 (MKB) 抽取鑰資訊 (MK)。然後，從鑰資訊 (MK) 和媒體特定資訊 (M-ID) 產生加密標題鑰的加密鑰 (MUK) (S12)。

接著，亂數產生處理產生標題鑰 (TK)。然後，著作權保護的內容資料被標題鑰 (TK) 鎖碼加密 (S13)。然，鑰 (MUK) 加密標題鑰 (TK)，產生加密標題鑰 (Enc-TK) (S13)。然後，加密的內容 (Enc-Contents) 和加密標題鑰 (Enc-TK) 經由匯流排鑑定部轉移到驅動器 V1 (S14)。

判定是否可移動記錄內容 (S14)。當判結果肯定時，亂數產生處理產生安全鑰 (MM)。然後，加密標題鑰 (Enc-TK) 被安全鑰 (MM) 多重加密。然後，加密內

(14)

容 (Enc - Contents) 的媒體鑰 (MB - Key) 和一組加密標題鑰 (Enc - TK) 及多重加密標題鑰 (Enc2 - TK) 的移動鑰 (Move - Key) 記錄於記錄媒體 D1 (S16) 。

再者，藉由驅動器 V1 的裝置鑰 (DvK2)，根據媒體鑰方塊資訊 (MKB) 來偵測加密鑰 (MMK)。安全鑰 (MM) 被加密鑰 (MMK) 加密，產生加密的加密鑰 (Enc - MM) (S17)。然後，加密的加密鑰 (Enc - MM) 的信號記錄於安全區 (S18)。

若在步驟 S15 判定結果否定，則加密內容 (Enc - Contents) 的媒體鑰 (MB - Key) 和一組加密標題鑰 (Enc - TK) 記錄於記錄媒體 D1 (S19)。

藉由這些處理，內容資料被加密，移動鑰 (Move - Key ; Enc2 - TK) 和媒體鑰 (MB - Key ; Enc - TK) 二者或只有媒體鑰記錄於光碟 D1。

[移動流動圖 2]

圖 10 的流程圖中，說明內容從記錄媒體 D1 移到另一記錄媒體 D2。

首先，從移動目的記錄媒體 D2 讀出媒體鑰方塊資訊 (MKB) 和媒體特定資訊 (M - ID)，產生加密鑰 (MUK2)。接著，設定記錄媒體 D1，偵測內容管理資訊 (S22)。判定對應的內容媒體鑰 (MB - Key) 和移動鑰 (Move - Key) 是否存在 (S23)。

在步驟 S23 判定只有移動鑰 (Move - Key) 存在時，

(15)

使用媒體鑰方塊資訊 (MKB) 和裝置鑰 (DvK2) 來偵測加密鑰 (MMK) 。然後，加密的加密鑰 (Enc - MM) 解密，偵測安全鑰 (MM) 。然後，安全鑰 (MM) 解密多重加密標題鑰 (Enc2 - TK) ，產生加密標題鑰 (Enc - TK) (S31) 。

在步驟23媒體鑰 (MB - Key) 和移動鑰 (Move - Key) 都存在時，記錄媒體 D1 的媒體鑰方塊資訊 (MKB) 和媒體特定資訊 (M - ID) 經由匯流排鑑定轉移，裝置特定加密鑰 (DvK1) 偵測加密鑰 (MUK) (S24) 。再者，加密標題鑰 (Enc - TK) 被加密鑰 (MUK) 解密，產生標題鑰 (TK) 。此外，從記錄媒體 D1 讀出加密的內容，讀出的內容被標題鑰 (TK) 解密。然後，解密的内容被新亂數產生器所產生的標題鑰 (TK2) 重新鎖碼 (加密) ，暫時記錄加密的內容 (S25) 。然後，刪除多重加密標題鑰 (Enc2 - TK) ，即記錄媒體 D1 之對應內容的移動鑰 (Move - Key) (S26) 。

然後，目前記錄媒體變成記錄媒體 D2；標題鑰 (TK2) 被加密鑰 (MUK2) 加密；產生加密標題鑰 (Enc - TK2) (S27) 。然後，在記錄驅動器產生新安全鑰 (MM2) ；加密標題鑰 (Enc - TK2) 被多重加密；產生多重加密標題鑰 (Enc2 - TK2) (S27) 。

然後，在記錄媒體 D2 使用媒體方塊資訊 (MKB) 和裝置鑰 (DvK2) ，產生加密鑰 (MMK) ；安全鑰 (MM2) 被加密；產生加密的加密鑰 (Enc - MM2) (S28) 。接

(16)

著，標題鑰（TK2）所加密的加密內容（Enc-Contents）和多重加密標題鑰（Enc2-TK2）記錄於記錄媒體D2。再者，加密的加密鑰（Enc-MM2）記錄於安全區（S29）。

此外，在步驟S23沒有移動鑰（Move-Key）時，移動失效（S30）。

依此方式，從移動源記錄媒體D1刪除移動鑰（Move-Key），只得到媒體鑰（MB-Key）。然後，不移動內容資料。結果，傳統通用機的複製裝置可複製，但不能移動內容資料。另一方面，只有移動鑰（Move-Key）在移動目的記錄媒體D2。只有可實施本發明之內容管理方法的專門機可複製及進一步移動。

〔移動流程圖3〕

圖11的流程圖中，說明內容從記錄媒體D2移到另一記錄媒體D3。

首先，從移動目的記錄媒體D3讀出媒體鑰方塊資訊（MKB）和媒體特定資訊（M-ID），產生加密鑰（MUK2）（S21）。

接著，設定記錄媒體D2，偵測內容管理資訊（S22）。然後，判定對應的內容媒體鑰（MB-Key）和移動鑰（Move-Key）是否存在（S23）。

移動鑰（Move-Key）不存在時，不移動內容資料（S30）。

判定只有移動鑰（Move-Key）存在時，使用媒體鑰

(17)

方塊資訊 (MKB) 和裝置鑰 (DvK2) 來抽取加密鑰 (MMK) 。然後，加密的加密鑰 (Enc - MM) 解密，偵測安全鑰 (MM) 。然後，安全鑰 (MM) 解密多重加密標題鑰 (Enc2 - TK2) ，產生加密標題鑰 (Enc2 - TK2) (S31) 。

在步驟 S23 判斷媒體鑰 (MB - Key) 和移動鑰 (Move - Key) 存在時，記錄媒體 D2 的媒體鑰方塊資訊和媒體特定資訊 (M - ID) 經由匯流排鑑定轉移。然後，裝置特定解密鑰 (DvK1) 偵測標題鑰的加密鑰 (MUK2) (S42) 。接著，加密標題鑰 (Enc - TK2) 被解密鑰 (MUK2) 解密，偵測標題鑰 (TK2) 。然後，從記錄媒體 D2 讀出加密的內容 (Enc - Contents) ，讀出的內容暫時儲存 (S43) 。然，刪除多重加密標題鑰 (Enc2 - TK2) ，即記錄媒體 D2 之對應內容的移動鑰 (Move - Key) (S26) 。

接著，目前記錄媒體變成記錄媒體 D3；標題鑰 (TK2) 被加密鑰 (MUK2) 加密；產生加密標題鑰 (Enc - TK3) (S27) 。接著，在記錄驅動器產生新安全鑰 (MM3) ；加密標題鑰 (Enc - TK3) 被多重加密；產生多重加密標題鑰 (Enc2 - TK3) 。然後，在記錄媒體 D3 使用媒體鑰方塊資訊 (MKB) 和裝置鑰 (DvK2) ，產生加密鑰 (MMK) ；安全鑰 (MM3) 被加密；產生加密的加密鑰 (Enc - MM3) (S28) 。然後，標題鑰 (TK2) 所加密的加密內容 (Enc - Contents) 和多重加密標題鑰 (Enc2 - TK3) 記錄於記錄媒體 D3，加密的加密鑰 (Enc2 - MM3) 記

(18)

錄於安全區 (S29)。圖 11 之流程圖 3 的加密標題鑰 (Enc2 - TK3) 有許多步驟與圖 10 的流程圖 2 相同，但差異在步驟 S42 和 S43，標題鑰 (TK2) 被加密鑰 (MUK2) 加密，產生加密標題鑰 (Enc - TK3)。

依此方式，在移動源記錄媒體 D2，刪除移動鑰 (Move - Key)，因此不能移動或複製內容資料。另一方面，在移動目的記錄媒體 D3，只得到移動鑰 (Move - Key)，只有可實施本發明之內容管理方法的專門機可複製及進一步移動。

此外，本發明之內容管理方法的記錄媒體不限於光碟，可包含諸如 SD (安全數位) 卡 D4 的一般數位記錄媒體，如圖 5。

[移動流程圖 4]

再者，圖 12 的流程圖之移動內容資料的處理中，聲道減為 2 聲道來處理多聲道音源資料 (5.1 聲道)。這些處理基本上與圖 11 的流程圖相同。步驟 44 取代圖 11 之流程圖的步驟 S42 和 S43。

亦即，在圖 12 之流程圖的步驟 S44，加密標題鑰 (Enc - TK) 被加密鑰 (MUK2) 解密，產生標題鑰 (TK2)。然，從記錄媒體 D2 讀出加密的內容 (Enc - Contents)，讀出的內容被標題鑰 (TK2) 解密。再者，多聲道音源資料減為 2 聲道；資料再度被亂數產生器所產生的標題鑰 (TK3) 鎖碼 (加密)，暫時記錄加密的資料 (S44)。

(19)

在此處理，當音源資料（5.1聲道）減為2聲道時，內容資料可從記錄媒體D2移到新記錄媒體D3。其功效與圖11之流程圖的移動處理相同。

〔增加各音樂項目檔之鑰資訊和鑰的方法〕

再者，本發明之內容管理方法的內容資料可為多種聲音檔的形式，做為多個音樂項目上的音樂資訊。多種資訊能以影像檔儲存。此處以聲音檔來說明。在此形式，圖1之亂數產生器18所送的不同標題鑰（TK）以各檔為基礎為提供，各鑰被加密，藉以移到另一記錄媒體。依此方式，可顯著增進使用者之內容利用的自由度。

但若配合多個標題鑰（TK）產生移動鑰（Move-Key；Enc2-TK），則需由該數目的多個音樂檔在驅動部V1供安全鑰（MM）。但若由音樂檔的數目提供安全鑰（MM），然後，所有鑰存入光碟D的安全區，則因安全區需要大儲存容量而不佳。詳言之，在使用上述調變／解調處理的安全資訊記錄系統，當部分主資料損毀時，記錄安全資訊。在主資料複製處理不希望此情，因此，最好降低安全資訊。

因此，根據安全鑰（MM）依照預定程序增加多個鑰；增加的鑰用於加密；只有增加源的安全鑰（MM）存入安全區，藉以管理多個檔，同時降低安全區儲存容量。

圖13顯示在本發明之內容管理方法產生安全鑰（MM）的設計。此圖中，在圖1的亂數產生器24，根據產自亂

(20)

散 G61 的鑰源資料 (MM) 產生安全鑰 (MM1)，然後，特定函數 K 乘以內容資料識別碼或次序所決定的數字，因此產生新安全鑰 (MM2 至 MMn)。使用多個安全鑰 (MM2 至 MMn)，多個加密標題鑰 (Enc-TK1 至 Enc-TKn) 63-1 至 n 被加密 64。

但只有鑰源資料 (MM) 之加密的加密鑰 (Enc-MM) 可存入安全區，因此，所需的安全區儲存容量不增加。因此，可管理多個檔的內容，同時維持高安全性。

[管理資訊]

本發明之內容管理方法中，移動鑰 (Move-Key) 和媒體鑰 (MB-Key) 管理內容資料的複製或移動。因此，這些加密鑰檔是特別重要的資料。亦即，若加密的加密鑰不能解密，則加密的內容也不能解密或複製。因此，如圖 14，在記錄媒體 (例如光碟) 的資料區，移動鑰 (Move-Key) 檔和媒體鑰 (MB-Key) 檔設在不同檔區。然後，一表分配給一 ECC 方塊，各表寫入 4 個 ECC 方塊，藉以增進資料可靠度。

這些檔的表顯示於圖 15。亦即，在記錄媒體，存在三種鑰，「媒體鑰 (MB-Key) 和移動鑰 (Move-Key)」，「只有媒體鑰 (MB-Key)」，「只有移動鑰 (Move-Key)」，此外，若存在大量內容檔，則須容易讀出相對於各內容加密鑰之媒體鑰 (MB-Key) 與移動鑰 (Move-Key) 間的關。因此，圖 15 的移動鑰 (Move-Key

(21)

）表 and 媒體鑰（MB-Key）表中，提供一對資訊，亦即代表加密鑰是否存在的資訊和利用圖15之安全鑰（MM）之方法的資訊。列出這些表，可輕易判定各內容資料是否可移動。

藉由上述多個實施例，熟習本技藝人士可完成本發明。再者，熟習本技藝人士可任施匠思而為諸般修飾。因此，本發明並非可由實施例而被限制其實施型態。

例如，關於要儲存的安全區，當使用上述調變／解調處理時，記錄／複製安全資訊的區域可配合主資料除外的記錄／複製區。利用此法，主資料不含錯誤成分，因此，不失去內容資料可靠度。

如所述，依據本發明，確保內容資料移動的移動鑰（Move-Key；Enc2-TK）和確保傳統通用機（例如光碟）之複製裝置之複製的媒體鑰（MB-Key；Enc-TK）連同加密的內容資料記錄於記錄媒體。可對存入安全區的安全鑰解碼之本發明的記錄／複製裝置中，可藉移動鑰（Move-Key）來複製或移動。傳統通用機的複製裝置中，確保媒體鑰（MB-Key）的複製。依此方式，能有專用機的移動處理，同時防止內容資料散播。此外，傳統機可複製內容資料。

【圖式簡單說明】

圖1是方塊圖，描繪本發明實施例之內容管理方法的加密例子；

(22)

圖 2 是方塊圖，描繪本發明實施例之內容管理方法所加密之內容之一般方法的解密例子；

圖 3 是方塊圖，描繪本發明實施例之內容管理方法所加密之內容之本發明方法的解密例子；

圖 4 顯示記錄有本發明實施例之內容管理方法所加密之內容的記錄媒體例子；

圖 5 顯示本發明實施例之內容管理方法之移動鑰（Move- Key；Enc2-TK）和媒體鑰（MB-Key；Enc-TK）的移動例子；

圖 6 是方塊圖，描繪應用本發明實施例之內容管理方法之記錄／複製裝置的結構例子；

圖 7 是方塊圖，顯示當本發明實施例之內容管理方法用於記錄／複製裝置時的加密設計詳細例子；

圖 8 是方塊圖，顯示當本發明實施例之內容管理方法用於記錄／複製裝置時的解密設計詳細例子；

圖 9 是流程圖，顯示在記錄媒體 D1 記錄本發明實施例之內容管理方法所加密之內容和鑰資訊的作業；

圖 10 是流程圖，顯示本發明實施例之內容管理方法所加密的內容從記錄媒體 D1 移到另一記錄媒體 D2；

圖 11 是流程圖，顯示本發明實施例之內容管理方法所加密的內容從記錄媒體 D2 移到另一記錄媒體 D3；

圖 12 是流程圖，顯示聲道減少時本發明實施例之內容管理方法所加密的內容從記錄媒體 D2 移到另一記錄媒體 D3；

(23)

圖 13 顯示在本發明實施例之內容管理方法產生安全鑰 (MM) 的設計；

圖 14 顯示在本發明實施例之內容管理方法之記錄媒體之移動鑰 (Move-Key; Enc2-TK) 和媒體鑰 (MB-Key; Enc-TK) 的儲存區例子；

圖 15 顯示在本發明實施例之內容管理方法之記錄媒體之移動鑰 (Move-Key; Enc2-TK) 和媒體鑰 (MB-Key; Enc-TK) 之表的例子。

主要元件對照表

- 10 網際網路
- 11 中央處理單元
- 12 唯讀記憶體
- 13 隨機存取記憶體
- 14 通訊介面
- 15 硬碟
- 16 匯流排
- 21 中央處理單元
- 22 唯讀記憶體
- 23 隨機存取記憶體
- 24 通訊介面
- 25 硬碟
- 26 匯流排
- 251 轉接程式

(24)

252 碼 轉 換 表

253 不 可 存 取 URL 列 表

伍、中文發明摘要

發明名稱：內容資料管理方法，記錄且／或複製裝置，以及記錄媒體

一種內容管理方法，內容資料被第一鑰（TK）加密，第一鑰被多種第二鑰（MUK）加密，加密的第一鑰（Enc-TK）被第三鑰（MM）多重加密，第三鑰被第四鑰（MMK）加密。在記錄媒體記錄這些加密的內容資料（Enc-Contents）、第一鑰被第二鑰加密的媒體鑰、第一鑰（Enc2-MM）被第二和第三鑰多重編碼的移動鑰，被第四鑰加密的第三鑰（Enc-MM）記錄於安全區。移動鑰和媒體鑰管理此管理方法。

陸、英文發明摘要

發明名稱：Content management method, recording and/or reproducing apparatus, and recording medium

In a content management method, content data is encrypted by a first key (TK), the first key is encrypted by plural types of second keys (MUK), the encrypted first key (Enc-TK) is multiply encrypted by a third key (MM), and the third key is encrypted by a fourth key (MMK). These encrypted content data (Enc-Contents), a medium key which is the first key (Enc-TK) encrypted by the second key and a move key which is a first key (Enc2-MM) multiply encoded by the second and third keys are recorded in a recording medium, the third key (Enc-MM) encrypted by the fourth key is recorded in a security region. This management method is managed by the move key and the medium key.

(1)

拾、申請專利範圍

1. 一種內容管理方法，包括：

內容資料被第一鑰（TK）加密；

第一鑰被預定多重第二鑰（MUK）加密

經加密的第一鑰（Enc-TK）被第三鑰（MM）多重加密；

第三鑰被預定第四鑰（MMK）加密；

在記錄媒體記錄內容資料被第一鑰加密（Enc-Contents）、第一鑰（Enc-TK）被預定多種第二鑰加密、第一鑰（Enc2-TK）加密的第一鑰（Enc-TK）被第二和第三鑰（MM）多重加密而得，將由第四鑰加密的第三鑰（Enc-MM）記錄於記錄媒體的安全區。

2. 如申請專利範圍第1項的內容管理方法，其中第一鑰有多個，內容資料有多個，各自分開加密，加密的第一鑰（Enc-TK）產生多個。

3. 如申請專利範圍第1項的內容管理方法，其中第一鑰數目取決於內容資料數目，第三鑰數目取決於第一鑰數目，多個加密的第一鑰（Enc-TK）被多個第三鑰（MM）分別多重加密。

4. 如申請專利範圍第1項的內容管理方法，其中記錄有加密的內容資料（Enc-Contents）、被第二鑰加密的第一鑰（Enc-TK）、被第二和第三鑰多重加密的第一鑰（Enc2-TK）的記錄媒體，與記錄被第四鑰加密的第三鑰（Enc-MM）之安全區的記錄媒體相同。

(2)

5. 如申請專利範圍第1項的內容管理方法，其中一個第二鑰（MUK）是記錄媒體的特定資訊。

6. 如申請專利範圍第1項的內容管理方法，其中在具有編碼器模組和經由鑑定處理與其通訊之驅動器的記錄裝置實施內容管理方法，第三鑰（MM）是只在驅動器產生的鑰。

7. 如申請專利範圍第1項的內容管理方法，其中被第二鑰加密的第一鑰（Enc-TK）與被第二和第三鑰多重編碼的第一鑰（Enc2-TK）記錄於記錄媒體的不同記錄區。

8. 如申請專利範圍第1項的內容管理方法，其中若內容資料從第一記錄媒體（D1）移到第二記錄媒體（D2），則內容資料在解密後重新加密，加密的內容資料和只有控制內容移動的加密鑰記錄於第二記錄媒體，刪除記錄於第一記錄媒體之控制內容移動的加密鑰。

9. 如申請專利範圍第8項的內容管理方法，其中若內容資料從只記錄有控制內容移動之加密鑰的第二記錄媒體（D2）移到第三記錄媒體（D3），則內容資料在解密後重新加密，加密的內容資料和控制內容移動的加密鑰記錄於第三記錄媒體，刪除控制內容移動的加密鑰，藉以進行在記錄媒體間移動內容的處理。

10. 如申請專利範圍第1項的內容管理方法，另包括：

由特定亂數產生器（24）產生鑰源資料；

(3)

根據指定多個內容資料的資訊乘以特定函數，產生多個第三鑰（ $MM1$ 至 MMn ）（圖13）；

以記錄媒體中之多個加密的內容資料和多重加密的第一鑰，記錄多個第三鑰做為多個加密第一鑰的多重加密鑰；

由預定加密鑰加密亂數產生器所產生的鑰源資料，然後將加密資料記錄於記錄媒體的安全區。

11. 如申請專利範圍第1項的內容管理方法，另包括：

若被第二鑰加密的第一鑰與被第二和第三鑰多重編碼的第一鑰在獨立記錄區各記錄成獨立檔資料，則在儲存區的鑰檔開頭或在預定位置，提供具有代表鑰檔資料是否為被第二鑰加密的第一鑰或被第二和第三鑰多重編碼的第一鑰之識別資訊之加密的加密鑰檔（圖15），和代表各副本鑰檔是否存在的識別資訊。

12. 如申請專利範圍第11項的內容管理方法，其中加密的加密鑰檔寫入多次。

13. 如申請專利範圍第1項的內容管理方法，另包括：

在第一記錄媒體（ $D1$ ）和安全區記錄有加密之內容資料之第二記錄媒體的複製處理，第一鑰（ $Enc2-TK$ ）被第二和第三鑰多重編碼，第三鑰被第四鑰加密，

在第一記錄媒體，讀出被第二鑰加密的第一鑰（ $Enc-TK$ ），將以預定多種第二鑰（ MKB ， $M-ID$ ）加密的第

(4)

一鑰解密 (TK)，讀出加密的內容資料 (Enc-Contents)，內容資料被解密的第一鑰解密，藉以進行複製，

在第二記錄媒體，從安全區讀出第三鑰 (Enc-MM)，將由預定多種第四鑰 (MMK) 加密的第三鑰解密，讀出由第二鑰以及第三鑰多重編碼之第一鑰 (Enc-TK) 以偵測由第三鑰 (MM) 解密和由第二鑰加密的第一鑰 (Enc-TK)，將以預定多種第二鑰 (MUK) 加密的第一鑰解密，解密的第一鑰 (TK) 將加密的內容資料 (Enc-Contents) 解密，藉以進行複製。

14. 一種記錄媒體，包括：

加密部 (158)，由第一鑰 (TK) 加密指定的內容資料，由預定多種第二鑰 (MUK) 加密第一鑰，由第三鑰 (MM) 多重加密的第一鑰 (Enc-TK)，由預定第四鑰 (MMK) 加密第三鑰；

記錄部 (154, 156)，在第一記錄媒體記錄在加密部加密的內容資料 (Enc-Contents)、被第二鑰加密的第一鑰 (Enc-TK)、被第二和第三鑰多重編碼的第一鑰 (Enc2-TK)，在安全區記錄被第四鑰加密的第三鑰 (Enc-MM)。

15. 如申請專利範圍第14項的記錄裝置，另包括：

處理部 (154, 156)，若內容資料從第一記錄媒體 (D1) 移到第二記錄媒體 (D2)，則內容資料在解密後加密，只有加密的內容資料和控制內容移動的加密鑰記錄於第二記錄媒體，刪除記錄於第一記錄媒體之控制內容移動

(5)

的加密鑰；

若內容資料從只記錄有控制內容移動之加密鑰的第二記錄媒體（D2）移到第三記錄媒體（D3），則內容資料在解密後重新加密，加密的內容資料和控制內容移動的加密鑰記錄於第三記錄媒體，刪除控制做為源媒體之第二記錄媒體之內容移動的加密鑰，藉以進行在記錄媒體間移動內容資料的處理。

16. 如申請專利範圍第14項的記錄裝置，另包括：

處理部（154，156），由多個第一鑰分別加密多個內容資料，由預定多種第二鑰加密多個第一鑰，

若處理部由多個第三加密鑰加密加密的第一鑰，則由特定亂數產生器（24）產生鑰源資料，根據指定多個內容資料的資訊乘以特定函數，產生多個第三鑰（MM1至MMn）（圖13），

以多個加密的內容資料和多重加密的第一鑰，處理部將多個第三鑰記錄於記錄媒體做為多個加密的第一鑰；

處理部由預定加密鑰加密亂數產生器所產生的鑰源資料，將加密資料記錄於記錄媒體的安全區。

17. 如申請專利範圍第14項的記錄裝置，另包括：

處理部（154，156），若被第二鑰加密的第一鑰與被第二和第三鑰多重編碼的第一鑰在第一記錄媒體的獨立記錄區分別記錄成獨立檔資料，

則在鑰檔開頭或在預定位置，記錄具有代表鑰檔資料是否為被第二鑰加密的第一鑰或被第二和第三鑰多重編碼

(6)

的第一鑰之識別資訊之加密的加密鑰檔（圖15），和代表各副本鑰檔是否存在的識別資訊。

18. 一種記錄媒體，在第一記錄媒體（D1）的儲存區儲存有：

被第一鑰（TK）加密的內容資料（Enc-Contents）

；

由預定多種第二鑰（MUK）加密第一鑰所得的第一鑰（Enc-TK）；

由第三鑰（MM）多重加密的第一鑰（Enc-TK）所得的第一鑰（Enc2-TK）；

由預定第四鑰（MMK）加密第三鑰所得的第三鑰（Enc-TK）。

19. 如申請專利範圍第18項的記錄媒體，另包括：異於第一記錄媒體的第二和第三記錄媒體（D2，D3），記錄有被第一鑰加密的內容資料（Enc-Contents）和多重加密第一鑰所得之控制內容移動的加密鑰（Enc2-TK）。

20. 如申請專利範圍第18項的記錄媒體，其中第一記錄媒體由特定亂數產生器（24）產生鑰源資料（MM1）；將內容資料的識別碼或序號所決定的數字乘以特定函數，藉以產生多個第三鑰（MM1至MMn）（圖13）；其中這些鑰做為多個加密的第一鑰的多重加密鑰，記錄多個加密的內容資料和多重加密的第一鑰，再者，由預定加密鑰加密亂數產生器所產生的鑰源資料，並記錄於安全區。

圖1

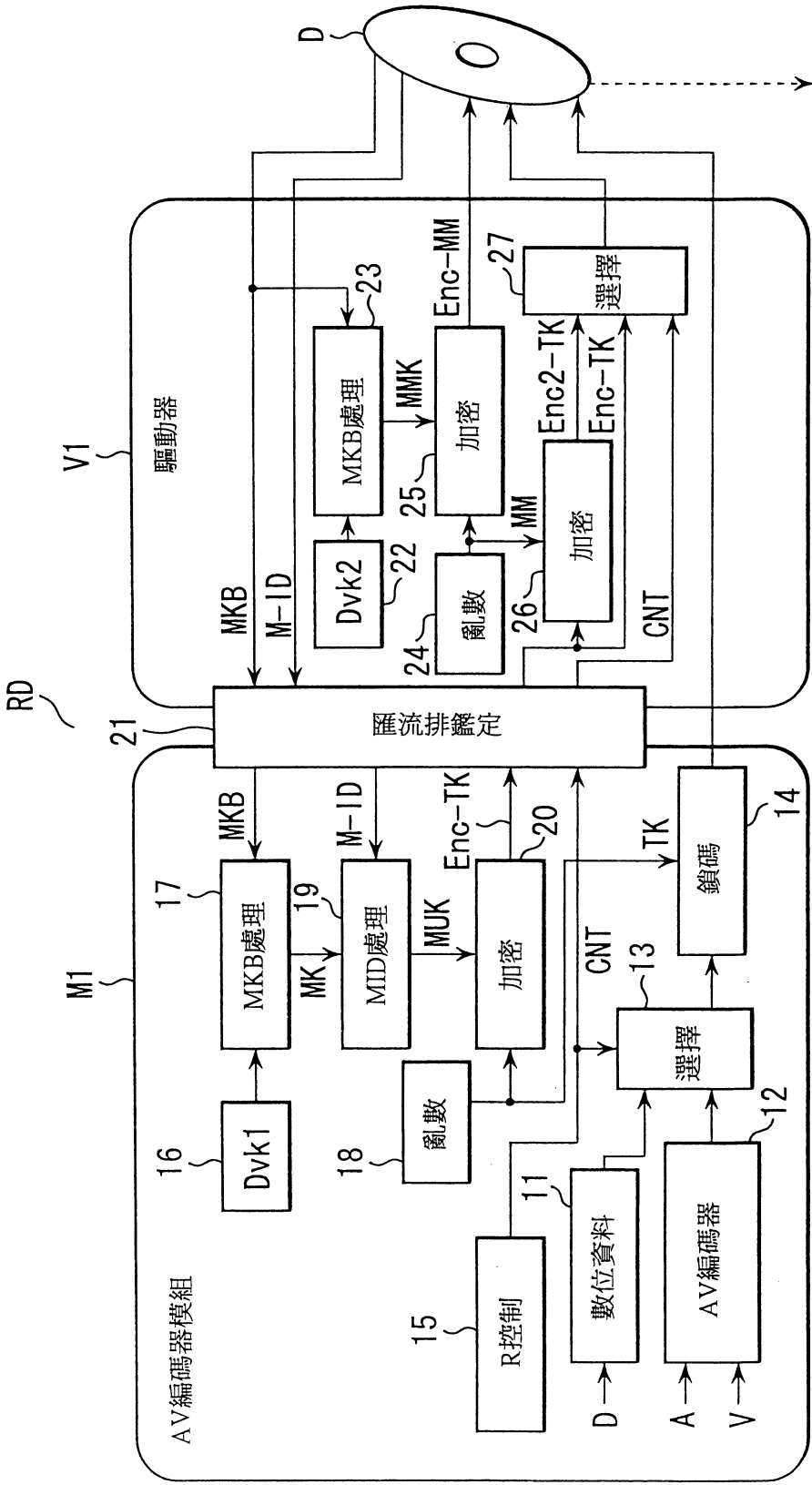


圖2

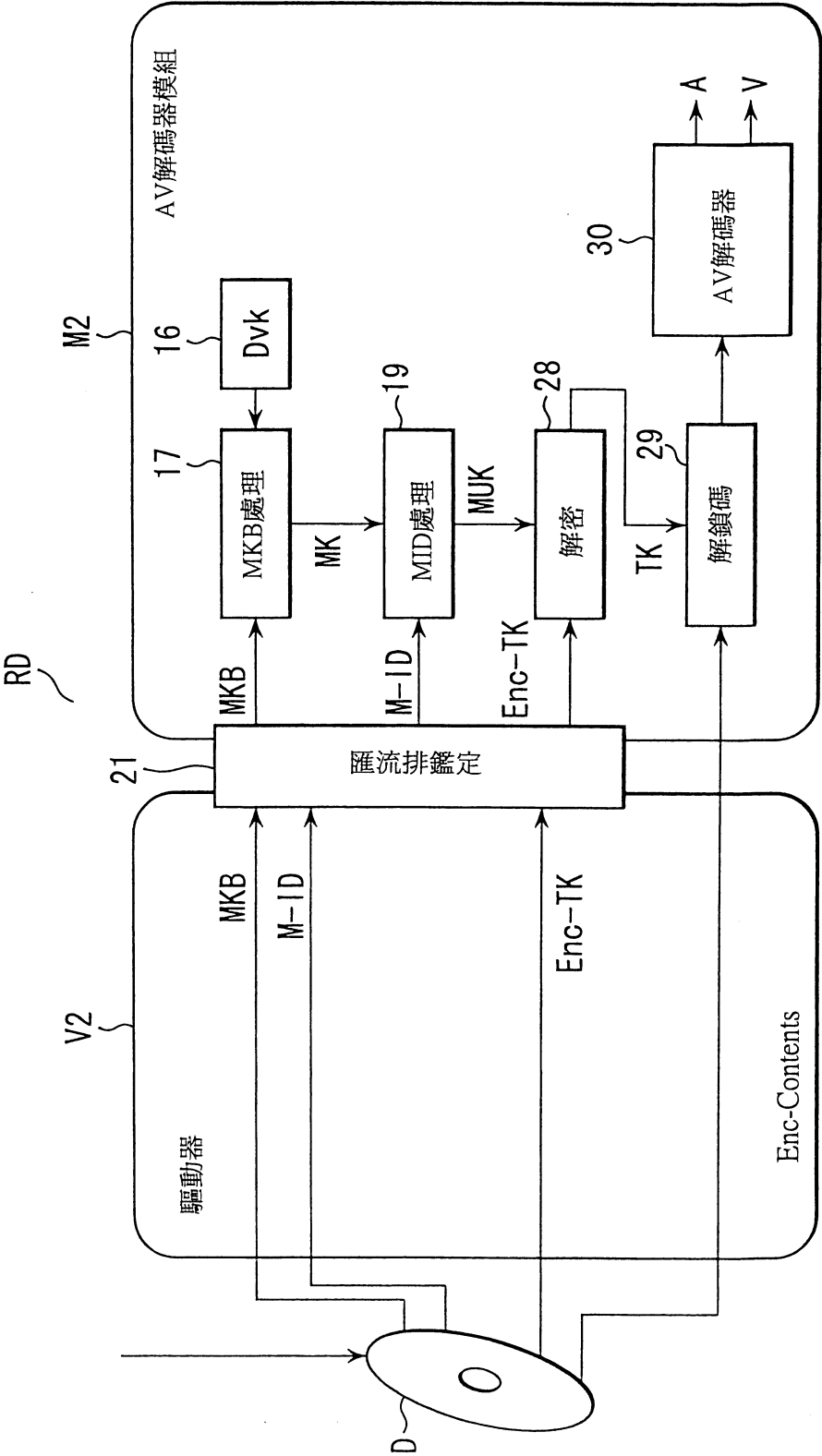


圖3

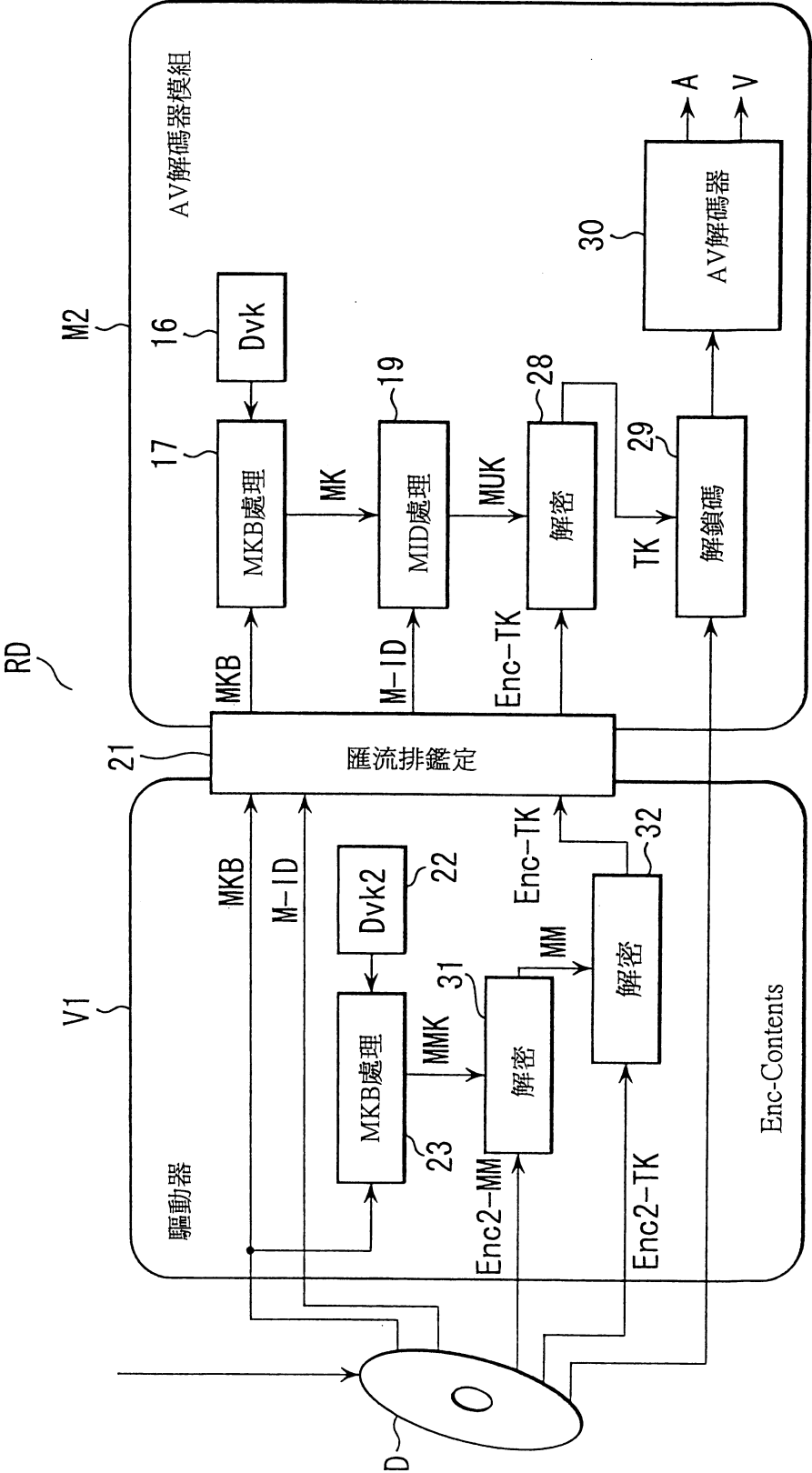


圖4

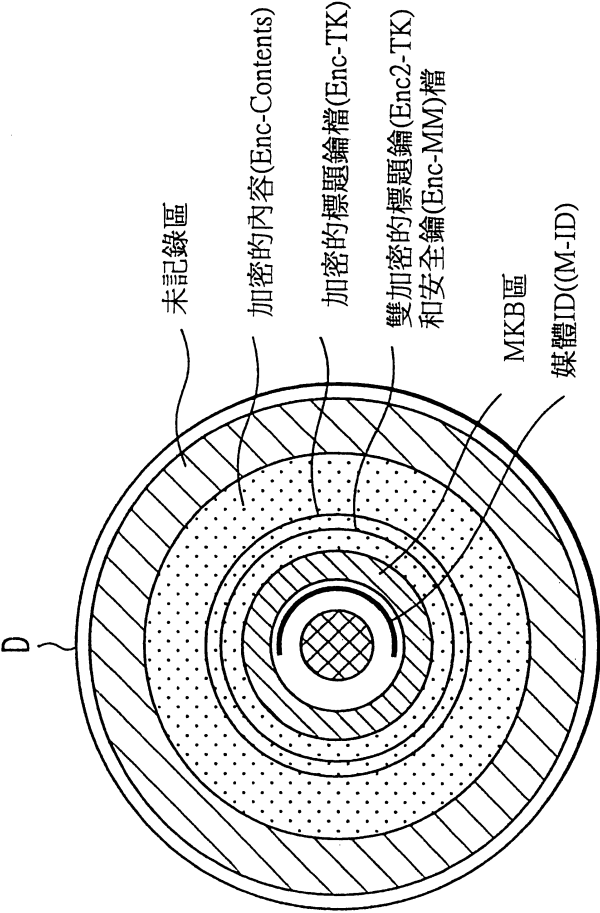


圖5

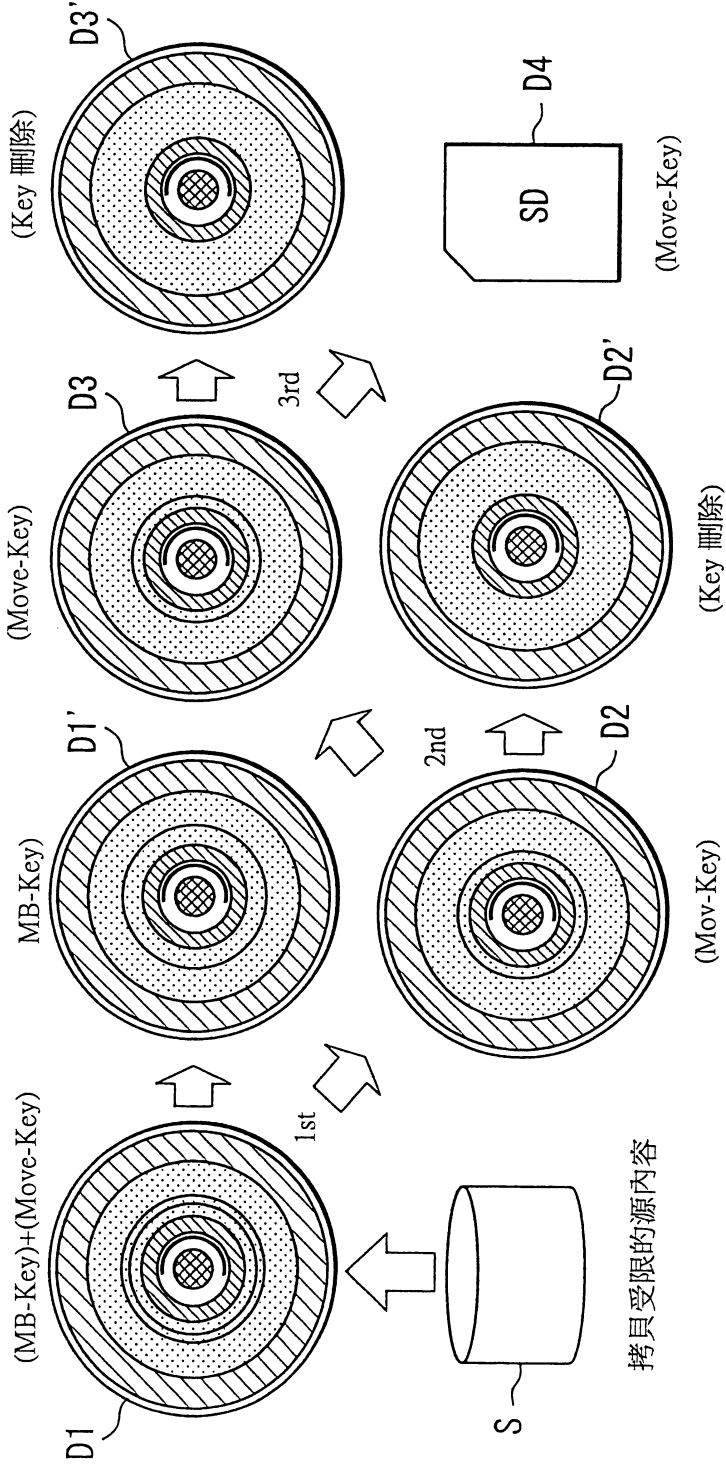


圖8

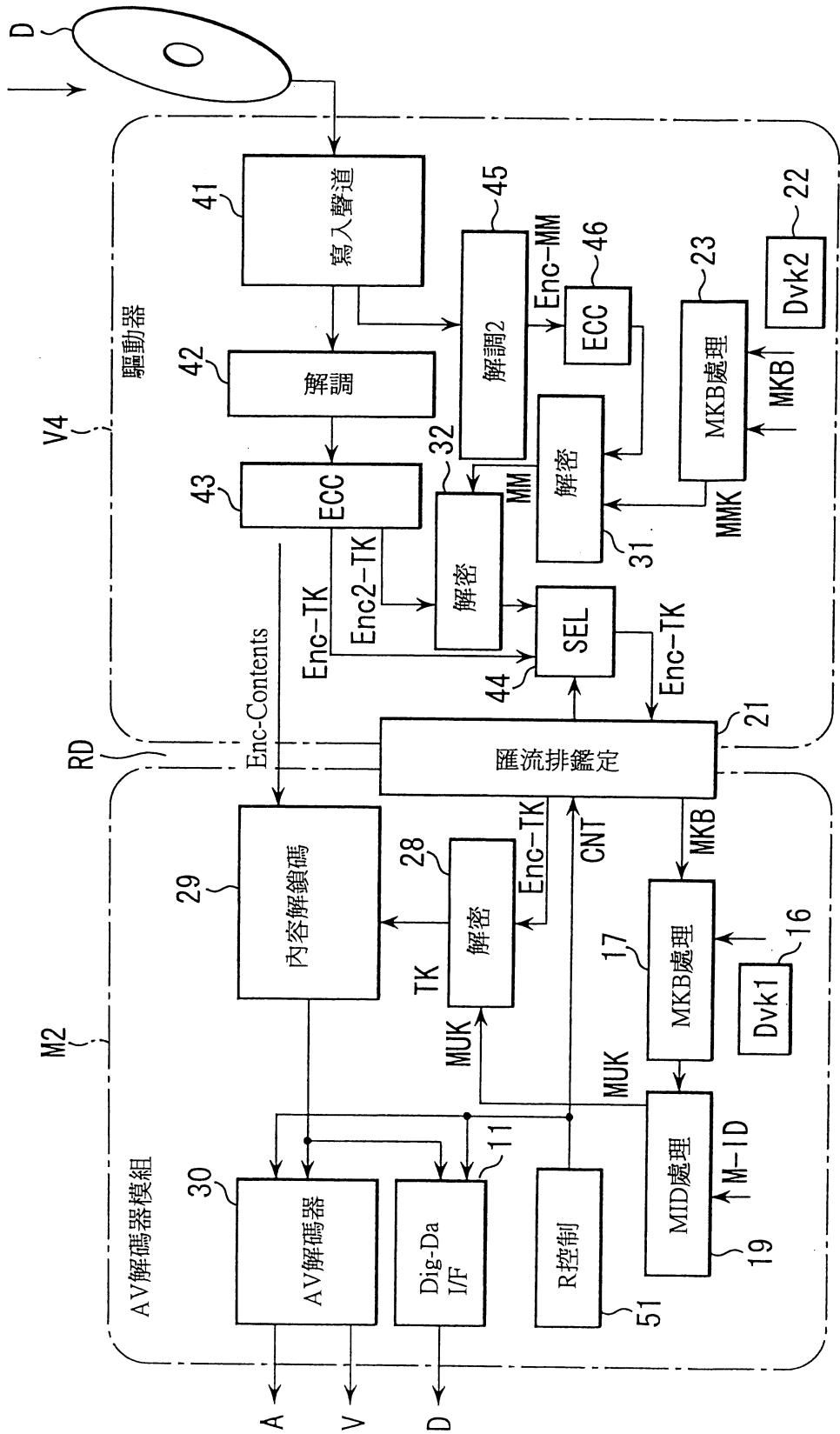


圖 9

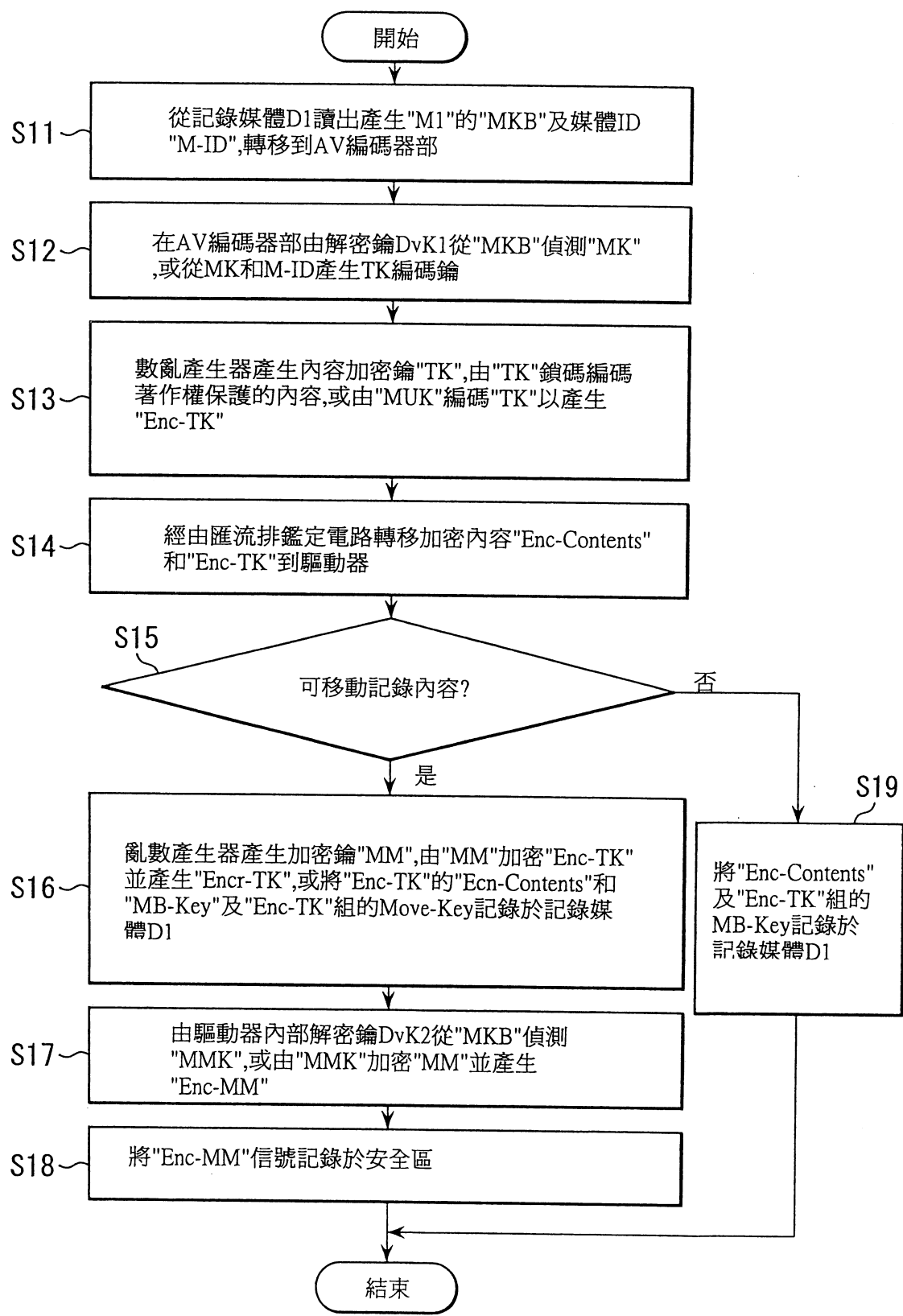


圖 10

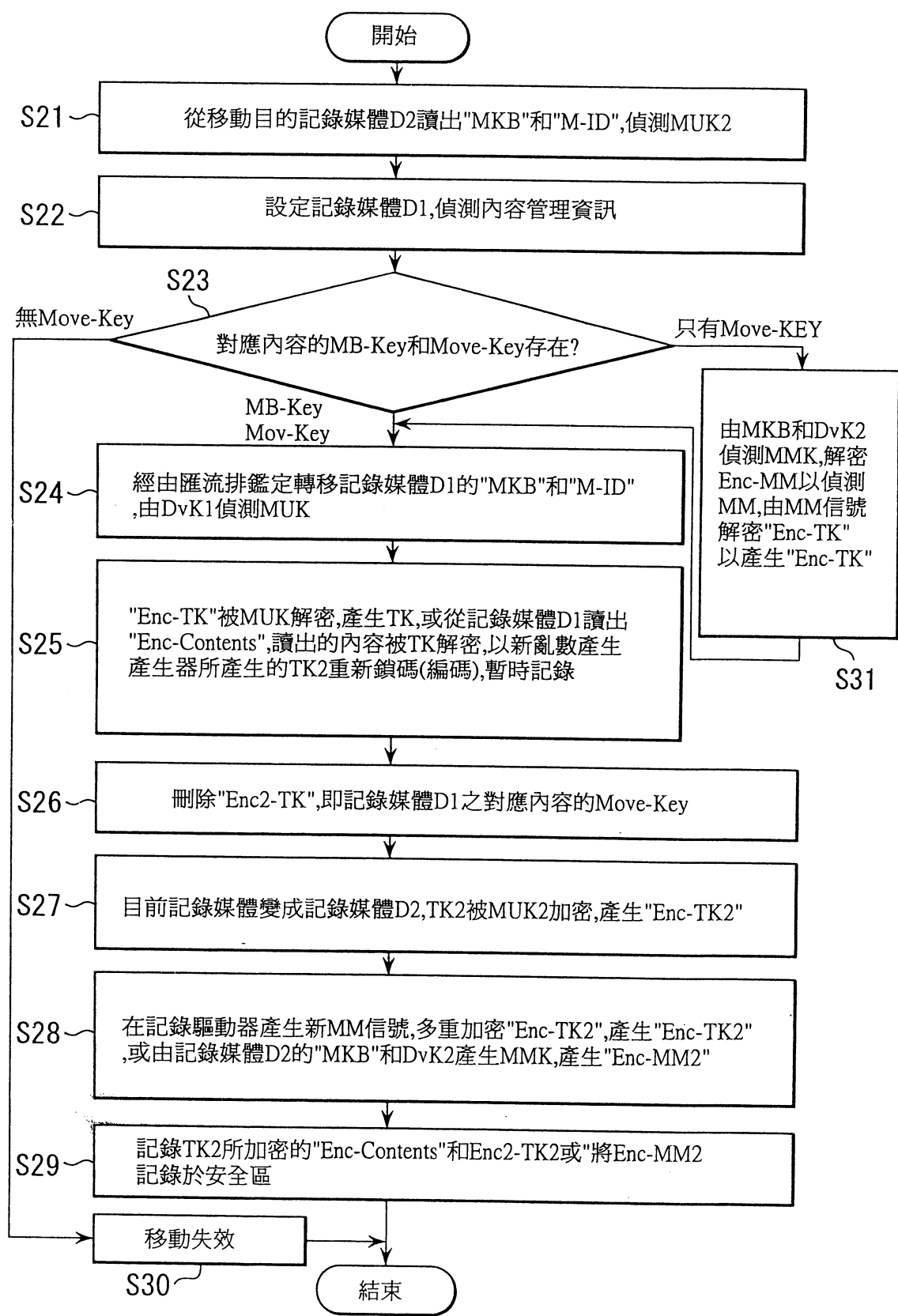


圖 11

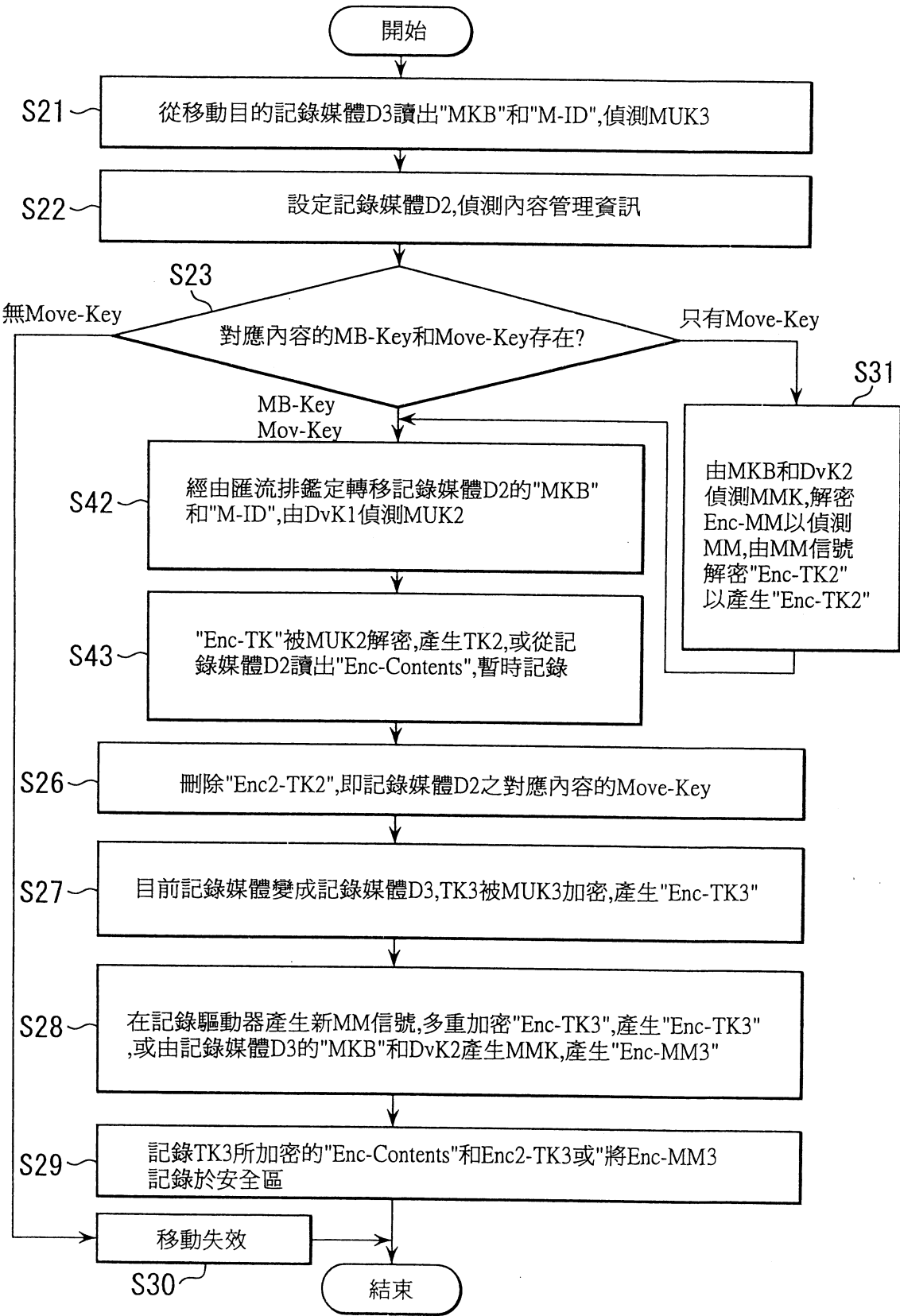


圖 12

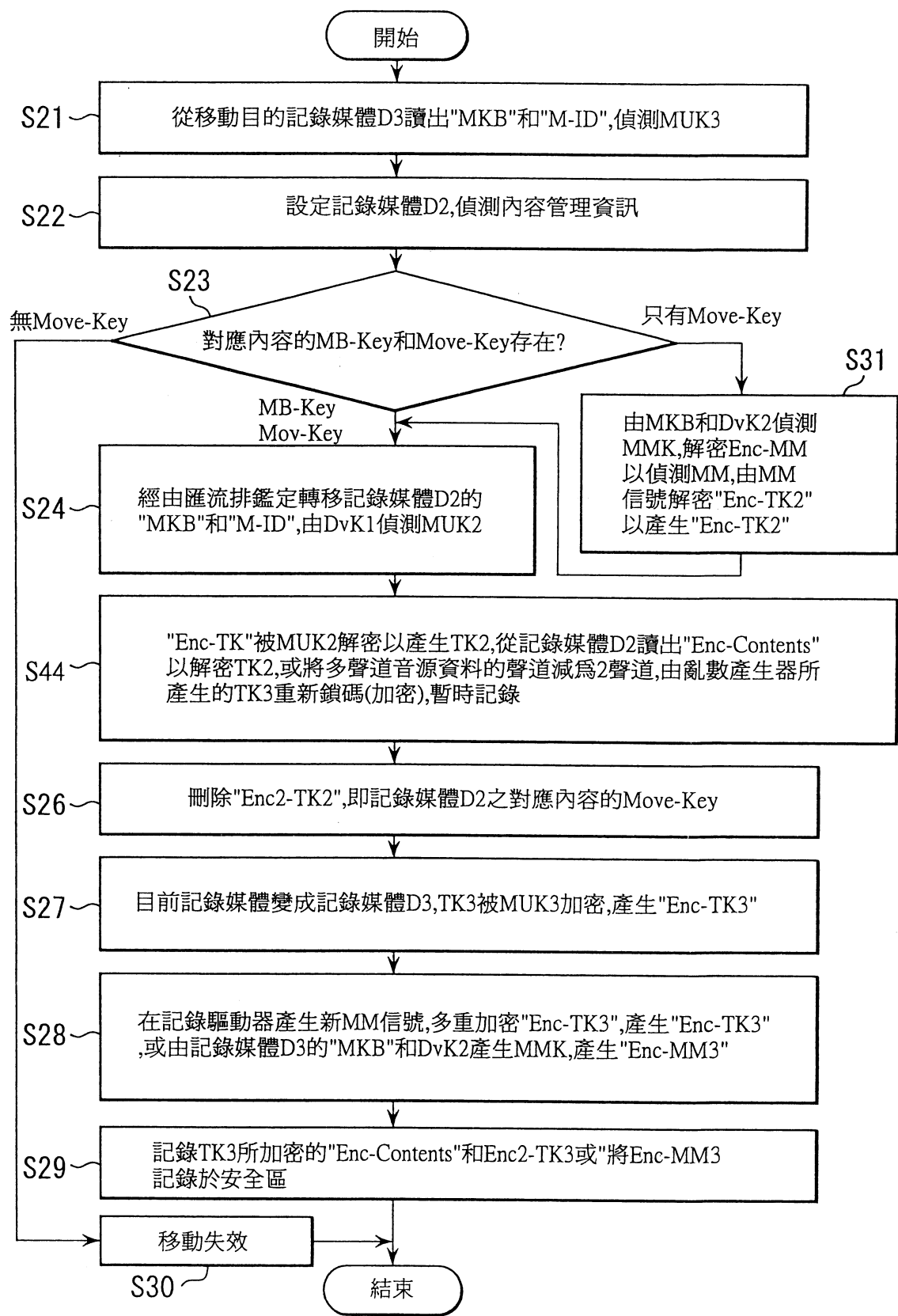


圖13

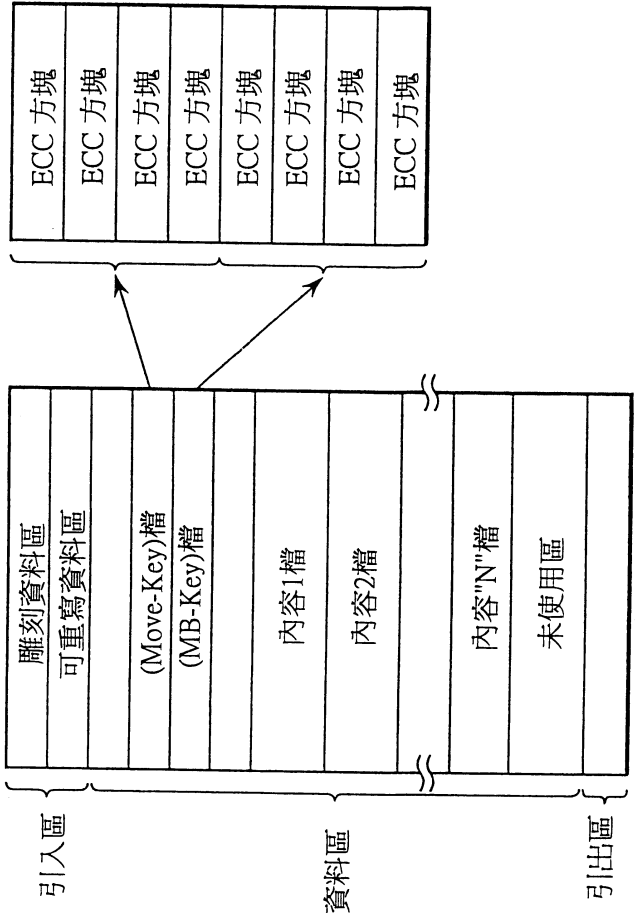
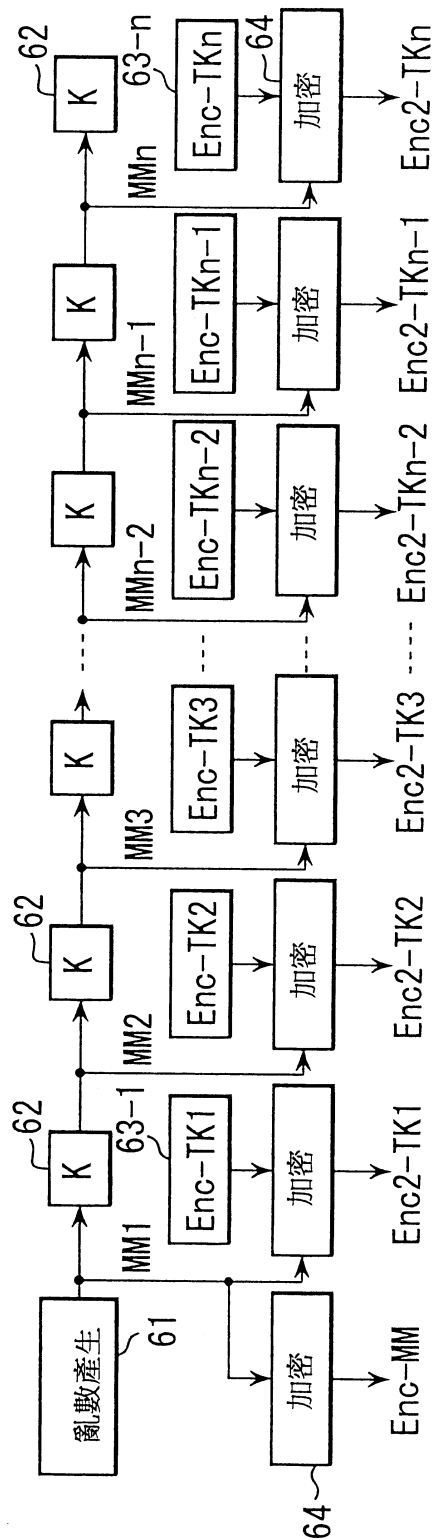


圖14

圖15

MB-Key 表				Move-Key 表			
加密之加密鑰(MB-Key)的檔識別				加密之加密鑰(Move-Key)的檔識別			
加密之加密鑰的數目				加密之加密鑰的數目			
Cont-1	Enc-TK	Cont-1 記錄數字	○	Cont-1	Enc2-TK	Cont-1 記錄數字	○
Cont-2	Enc-TK	Cont-2 記錄數字	○	Cont-2	Enc2-TK	Cont-2 記錄數字	○
Cont-3	Enc-TK	Cont-3 記錄數字	×	-	-	Cont-3 記錄數字	○
Cont-(n-1)	Enc-TK	Cont-(n-1) record number	○	Cont-(n-1)	Enc2-TK	Cont-(n-1) record number	○
Cont-n	Enc-TK		○	Cont-n	Enc2-TK	Cont-n record number	○
RSB	RSB	RSB		RSB	RSB	RSB	
RSB	RSB	RSB		RSB	RSB	RSB	

(a)Enc-2TK是否存在的資訊

(b)Enc-TK是否存在的資訊

(-表分配給-ECC方塊,各表寫入4個ECC方塊)

柒、（一）、本案指定代表圖為：第 1 圖

（二）、本代表圖之元件代表符號簡單說明：

- 11 中央處理單元
- 12 唯讀記憶體
- 13 隨機存取記憶體
- 14 通訊介面
- 15 硬碟
- 16 匯流排
- 17 MKB 處理
- 18 亂數產生器
- 19 MID 處理
- 20 解碼器電路
- 21 中央處理單元
- 22 唯讀記憶體
- 23 隨機存取記憶體
- 24 通訊介面
- 25 硬碟
- 26 匯流排
- 27 選擇器
- D 光碟
- V1 驅動器

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：