公告本

I229320

申請日期	91. 8. 7
案號	91119414
類別	G11B 20/00

A4
C4

（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	重現使用者資料之裝置及方法
	英文	"APPARATUS AND METHOD FOR REPRODUCING USER DATA"
二、發明 創作 人	姓名	1.法蘭西斯克斯 魯卡斯 安東尼奧斯 約翰尼斯 坎培曼 FRANCISCUS LUCAS ANTONIUS JOHANNES KAMPERMAN 2.安東尼奧斯 艾德里安 瑪利亞 史達林 ANTONIUS ADRIAAN MARIA STARING 3.約翰 保羅 瑪利 吉拉德 林納茲 JOHAN PAUL MARIE GERARD LINNARTZ
	國籍	1-3.均荷蘭 THE NETHERLANDS
	住、居所	均荷蘭愛因和文市普羅何斯蘭路6號 PROF. HOLSTLAAN 6, 5656 AA EINDHOVEN, THE NETHERLANDS
三、申請人	姓名（名稱）	荷蘭商皇家飛利浦電子股份有限公司 KONINKLIJKE PHILIPS ELECTRONICS N. V.
	國籍	荷蘭 THE NETHERLANDS
	住、居所（事務所）	荷蘭愛因和文市格羅尼渥街1號 GROENEWOUDSEWEG 1, 5621 BA EINDHOVEN, THE NETHERLANDS
	代表人姓名	J. L. 凡 德 渥 J. L. VAN DER VEER

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）　申請專利，申請日期：　　案號：　　，□有　□無主張優先權

歐洲專利機構	2001年07月19日	01202770.2	□有☑無主張優先權

有關微生物已寄存於：　　寄存日期：　　，寄存號碼：

五、發明說明（1　　）

本發明說明一種用以將以加密形式儲存在一個記錄媒體上之使用者資料重現之裝置及方法，又說明一個用於該一種裝置或方法中之積體電路；特定言之，本發明論及保護儲存在可移式記錄媒體上的資訊(像是一個DVD(數位影音光碟)上的視訊資料)。

如使用者資料(例如視訊資料、聲音資料、軟體或應用資料)係以一種加密形式儲存在一個可移式記錄媒體上時，則往往會要求一個授權的應用才可在不需自另一個位置(像是網際網路)中擷取該解碼鍵值的情況下、自該可移式記錄媒體中讀取和使用該使用者資料(若容許的話)。因此，須將該解碼鍵值、連同該加密之使用者資料一起儲存在該媒體上。

然而，須隱藏該解碼鍵值、以阻止一個無授權存取。已知用以隱藏該解碼鍵值之技藝係利用一個具有秘密播放器基碼之媒體鍵值區段，其中該等秘密播放器基碼係用於例如"該已知的內容密碼形式系統(CSS)"和"可記錄媒體的內容保護(CPRM)"中。可從美國專利6,157,606中知悉另一種用以利用秘密信號處理方法、而以電子信號隱藏該解碼鍵值之方法，其中利用一個主鍵值、並藉由變更一個雷射光束的光量而以一個凹陷寬的方向加密主資料，並繼之將該加密之主資料記錄在一個光學記錄媒體上。

於該等現今用的保護系統中(像是CSS和CPRM)，係在一個PC其一個應用單元中所執行之一個授權的PC應用內部計算該解碼鍵值。該等授權的應用含有防備析取秘密

五、發明說明（2　　）

(像是計算媒體鍵值區段時所需的播放器基碼)和防備修正該應用其任何行為(像是將任何內寬的受保護資料提供給其它應用)之保護機制。然而，已知該等PC軟體應用的保護機制較差、且經常故障。如電腦駭客竄改該授權的應用和/或該應用單元時，則反而可能變成"將該受保護之使用者資料的解碼鍵值提供給該電腦駭客"。此時，該電腦駭客將能夠析取和公告該等許多公開之記錄媒體的解碼鍵值，而容許其它的電腦駭客利用無授權的應用輕易地存取該受保護之使用者資料。

此為一項很嚴重的安全問題。非法散佈解碼鍵值所產生的損害確實有可能比非法散佈內寬的受保護使用者資料來得大，此係因該受保護之使用者資料包含大量的資料(通常為數百萬個位元組)，導致散佈時非常費時。相比之下，該等解碼鍵值僅包含少量的資料(通常少於一千個位元組)，故而可快速和廣泛地散佈。

因此本發明的一個目的為提供一種用以將以加密形式儲存在一個記錄媒體上之使用者資料重現之裝置及方法，其中該等裝置及方法提供一個高階保護(特定言之，對"該解碼鍵值"提供一個高階保護)，以防經由入侵一個PC應用和/或應用單元作竊取破壞。藉由提供一種如申請專利範圍第1項之裝置達成該目的，其中該裝置包括：

- 用以自該記錄媒體讀取使用者資料和鍵值資料之裝置；
- 一個整合單元，包含：
  - 用以利用該鍵值資料計算一個解碼鍵值之裝置；

五、發明說明（3　　）

- 用以利用該計算而得的解碼鍵值將自該記錄媒體中所讀取的使用者資料解碼之裝置；及
- 用以利用一個重新加密鍵值將該解碼之資料重新加密之裝置；

- 用以將該重新加密之資料自該整合單元中傳輸給一個應用單元之裝置；及
- 一個"用以利用該重新加密鍵值將該重新加密之資料解碼"和"用以重現該解碼之資料"的應用單元。

更進一步藉由一種如申請專利範第8項之相對應的方法達成該目的。一如申請專利範圍第9項之用在該一個用於該一種方法中之裝置中的積體電路包括：

- 用以利用自該記錄媒體中所讀取的鍵值資料計算一個解碼鍵值之裝置；
- 用以利用該計算而得的解碼鍵值將自該記錄媒體中所讀取的使用者資料解碼之裝置；及
- 用以利用一個重新加密鍵值將該解碼之資料重新加密之裝置，以獲得重新加密之資料、並傳輸給一個應用單元，其中該應用單元"用以利用該重新加密鍵值將該重新加密之資料解碼"和"用以重現該解碼之資料"。

本發明係以下面的觀念為基礎：在該驅動器中的一個整合單元內部將自該記錄媒體中所讀取的使用者資料解碼和重新加密，而非像往常一樣利用一個PC應用在一個應用單元內部解碼和重新加密。竊取破壞一個整合單元比竊取破壞一個應用單元困難的多，且如是對該解碼鍵值提供一

五、發明說明（4　）

種改良式的保護。此外，亦在該整合單元內部計算用以解碼該使用者資料之該解碼鍵值和一個用以將該解碼之使用者資料重新加密之重新加密鍵值，此甚至對該解碼鍵值提供了更高的保護。如是，不管該解碼鍵值係在加密形式亦或解碼形式下，該解碼鍵值都決不會脫離該整合單元。此外，在該整合單元外部絕對看不見該介乎解碼與重新加密間所存在的解碼之使用者資料，此亦提供了一個更高階的保護、防護使用者資料不受到竊取破壞。

為了致能該應用單元將該整合單元提供給它的使用者資料解碼、並繼之重現該解碼之使用者資料，需將該重新加密鍵值或任何用以計算該重新加密鍵值之資料提供給該應用單元。可藉由不同的方法完成，例如利用公用鍵值密碼學、或藉由一個安全的確認通道(SAC)將該重新加密鍵值自該整合單元中傳輸給該應用單元。或者，亦可利用一種對稱密碼編譯法達成此目的。

於該等附屬申請項中包含本發明的較佳具體實施例。應瞭解，可更進一步發展如申請專利範圍第1項之裝置、如申請專利範圍第7項之方法及如申請專利範圍第8項之積體電路，且該等裝置、方法及積體電可具有完全相同或類似的具體實施例。

該整合單元較佳包含在一個用以讀取記錄媒體之驅動單元中，且該驅動單元和該應用單元較佳包含在一個電腦中(像是一台個人電腦)。又該記錄媒體最好為一個光學記錄媒體(特定言之"一個磁碟")，其中可為可記錄和可重寫

五、發明說明（6　　）

接著，將該讀取之資料輸入一個整合單元6中，其中較佳由一個積體電路(IC)實行，及其中該積體電路包括各種用以計算鍵值和用以解碼並且加密使用者資料之裝置。最初，利用自讀取裝置5中所輸入之該讀取的鍵值資料於一個鍵值計算單元7中計算該解碼鍵值。要求該解碼鍵值(DK)將讀取裝置5輸入給解碼單元8之該讀取的使用者資料解碼。該解碼鍵值(DK)與一個加密鍵值完全相同，其中在將該使用者資料儲存在媒體4上之前、已先利用該加密鍵值加密該使用者資料；或該解碼鍵值(DK)為該加密鍵值的一個對應鍵值。

在將該使用者資料解碼之後，應於一個重新加密單元10中將該使用者資料重新加密，而非藉由一個匯流排16將該內寬的使用者資料直接輸出給應用單元3，此係因在一個匯流排上傳輸內寬的使用者資料非常危險，且會給與電腦駭客讀取和複製該使用者資料的機會。

亦由一個適當的鍵值計算單元9在整合單元6內部計算該用以重新加密該使用者資料的重新加密鍵值(RK)。因該重新加密鍵值(RK)亦為應用單元3所已知的、以便在其中解碼該使用者資料，故在驅動單元2與應用單元3之間設立安全確認通道17、18。為了授權該在應用單元3上執行的應用，故一個證明授權15證明該應用的公用鍵值。

如因而將一個有關該應用之相對應指示授權該應用時；特定言之，如自應用單元3中將該應用的一個公用鍵值傳

五、發明說明（7　）

輸給驅動器2(特別是整合單元6的鍵值計算單元9)時。接著，鍵值計算單元9可接著"藉由一個公用鍵值特許授權14檢查該公用鍵值應用的憑證"和"藉由檢查該應用是否擁有該SAC機能其一部分的對應專屬基碼"以授權該應用。

於最後授權了該應用之後，則經由傳輸線路18將該加密之重新加密鍵值(RK)或其它任何關於該重新加密鍵值的資料自鍵值計算單元9中傳輸給應用單元3的鍵值計算單元11。如是，鍵值計算單元11能夠計算該重新加密鍵值(RK)，致使解碼單元12可將該經由傳輸線路16所提供的重新加密之使用者資料解碼。請注意，傳輸線路16、17及18係包含在電腦1的PC匯流排中。

當在解碼單元12中將該使用者資料解碼之後，則可將該使用者資料完全地重現，且供呈報單元13播放。

如是，本發明提供一個高階保護、以防使用者資料和/或解碼鍵值被竊取，其中在將該使用者資料儲存在該記錄媒體上之前、先利用該等解碼鍵值加密該使用者資料。不在該電腦的一個匯流排上傳輸該使用者資料和該等解碼鍵值；或該使用者資料和該等解碼鍵值兩者都不在該內寓之整合單元的外部。如是，則可能藉由竊取破壞在該電腦上執行的應用以擷取該解碼鍵值。

A5
B5

四、中文發明摘要（發明之名稱：重現使用者資料之裝置及方法）

本發明說明一種用以將以加密形式儲存在一個記錄媒體上之使用者資料重現之裝置及方法。為了提供一個高階保護、防護使用者資料不受到竊取破壞；特定言之，防護用以加密該使用者資料、且亦儲存在該記錄媒體上的解碼鍵值、使不受到竊取破壞，故根據本發明建議一種裝置，其中該裝置包括：

- 用以自該記錄媒體讀取用者資料和鍵值資料之裝置；
- 一個整合單元，包含：
  - 用以利用該鍵值資料，計算一個解碼鍵值之裝置；
  - 用以利用該計算而得的解碼鍵值，將自該記錄媒體中所讀取的使用者資料解碼之裝置；及
  - 用以利用一個重新加密鍵值，將該解碼之資料重新加密之裝置；

英文發明摘要（發明之名稱："APPARATUS AND METHOD FOR REPRODUCING USER DATA"）

The invention relates to an apparatus and a method for reproducing user data stored in encrypted form on a recording medium. In order to provide a higher level of protection against hacking of user data and, in particular, of decryption keys, which are used for encrypting said user data and which are also stored on the recording medium, an apparatus is proposed according to the invention, comprising:

- means for reading user data and key data from said recording medium,
- an integrated unit including
  - means for calculating a decryption key using said key data,
  - means for decrypting user data read from said recording medium using said calculated decryption key, and
  - means for re-encrypting said decrypted data using a re-encryption key,

A5
B5

四、中文發明摘要（發明之名稱：　　）

- 用以將該重新加密之資料自該整合單元中傳輸給一個應用單元之裝置；及
- 一個利用該重新加密鍵值將該重新加密之資料解碼和用以重現該解碼之資料的應用單元。

英文發明摘要（發明之名稱：　　）

- means for transmitting said re-encrypted data from said integrated unit to an application unit, and
- an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

五、發明說明(5)

的，且較佳為一個儲存任何使用者資料種類的光碟或DVD。或者，該記錄媒體亦可為另一種可比較的媒體，例如一個固態記憶卡。

又於一更佳的具體實施例中，將該整合單元實現成一個無法輕易從外部竊取破壞之積體電路。然而，亦可將該整合單元釋義成另一種整合零件，例如像是一個光學驅動單元。如判定該一個整合零件十分安全時，則可在硬體和韌體中局部地執行"重行加密"。例如可在韌體中執行重新加密鍵值產生。從一個安全性的觀點來看，此可能為可接受的，因該重新加密鍵值亦會出現在該應用單元中，然而就該一種像是一個光學驅動單元的整合零件而言，該應用單元為一個較不安全的環境。

圖式簡單說明

圖1繪示根據本發明一重現裝置之一方塊圖。

圖1中顯示一台個人電腦1，其中包括一個驅動單元2和一個應用單元3。如一使用者想要重現儲存在一個記錄媒體4(像是一個DVD-ROM(唯讀型DVD))上的使用者資料時(例如(重播儲存在一個DVD中之MPEG(動態圖形專家小組)格式的視訊資料)，則將媒體4插入驅動器2中，其中讀取裝置5讀取該使用者資料和該鍵值資料。請注意，該使用者資料和該鍵值資料均以加密形式儲存在媒體4上。另外請注意，有各種方式將使用者資料和鍵值資料加密、以儲存在記錄媒體上，至於使用何種特殊方式則與本發明無關。

修正替換頁
民 93 7 9
年 月 日
A7
B7

五、發明說明（ 8 ）

圖式元件符號說明

1	個人電腦
2	驅動單元
3	應用單元
4	記錄媒體
5	讀取裝置
6	整合單元
7	鍵值計算單元
8	解碼單元
9，11	鍵值計算單元
10	重新加密單元
12	解碼單元
13	呈報單元
14	公用鍵值特許授權
15	證明授權
16	匯流排
17，18	安全確認通道(傳輸線路)

六、申請專利範圍

1. 一種用以將以加密形式儲存在一個記錄媒體上之使用者資料重現之裝置，包括：

- 用以自該記錄媒體讀取使用者資料和鍵值資料之裝置；

- 一整合單元，包含：

  - 用以利用該鍵值資料計算一解碼鍵值之裝置；

  - 用以利用該計算而得的解碼鍵值，將自該記錄媒體中所讀取的使用者資料解碼之裝置；及

  - 用以利用一重新加密鍵值，將該解碼之資料重新加密之裝置；

- 用以將該重新加密之資料自該整合單元中傳輸給一應用單元之裝置；及

- 一用以利用該重新加密鍵值，將該重新加密之資料解碼和用以重現該解碼之資料的應用單元。

2. 如申請專利範圍第1項之裝置，其中該整合單元和/或該應用單元包括用以計算該重新加密鍵值之裝置。

3. 如申請專利範圍第1項之裝置，其中尚包括用以交換該重新加密鍵值資訊之公用鍵值密碼學裝置。

4. 如申請專利範圍第3項之裝置，其中利用該公用鍵值密碼學裝置設定一個安全的確認通道，用以將該重新加密鍵值自該整合單元中傳輸給該應用單元。

5. 如申請專利範圍第1項之裝置，其中該整合單元係包含在一個用以讀取記錄媒體之驅動單元中，及其中該驅動單元和該應用單元係包含在一個電腦中。

六、申請專利範圍

6. 如申請專利範圍第1項之裝置，其中該記錄媒體為一個光學記錄媒體，特定言之為一個CD或一個DVD。

7. 如申請專利範圍第1項之裝置，其中該整合單元為一個積體電路。

8. 一種用以將以加密形式儲存在一個記錄媒體上之使用者資料重現之方法，包括以下步驟：
   - 自該記錄媒體讀取使用者資料和鍵值資料；
   - 利用該鍵值資料計算一解碼鍵值；
   - 利用該計算而得的解碼鍵值，將自該記錄媒體中所讀取的使用者資料解碼；
   - 利用一重新加密鍵值，將該解碼之資料重新加密；
     其中於一個整合單元中進行該計算步驟、該解碼步驟及該重新加密步驟，
   - 將該重新加密之資料，自該整合單元中傳輸給一應用單元；
   - 於該應用單元中利用該重新加密鍵值，將該重新加密之資料解碼；及
   - 重現該解碼之資料。

9. 一種用於一如申請專利範圍第1項之裝置中的整合單元，其中該裝置用以將以加密形式儲存在一個記錄媒體上之使用者資料重現，及其中該整合單元包括：
   - 用以利用自該記錄媒體中所讀取的鍵值資料，計算一解碼鍵值之裝置；
   - 用以利用該計算而得的解碼鍵值，將自該記錄媒體中

六、申請專利範圍

所讀取的使用者資料解碼之裝置；及

- 用以利用一重新加密鍵值，將該解碼之資料重新加密之裝置，以獲得重新加密之資料、並傳輸給一應用單元，其中該應用單元用以利用該重新加密鍵值，將該重新加密之資料解碼和用以重現該解碼之資料。

10. 如申請專利範圍第9項之整合單元，其中該整合單元為一個積體電路。

第 091119414 號專利申請案
中文圖式替換本(93 年 7 月)

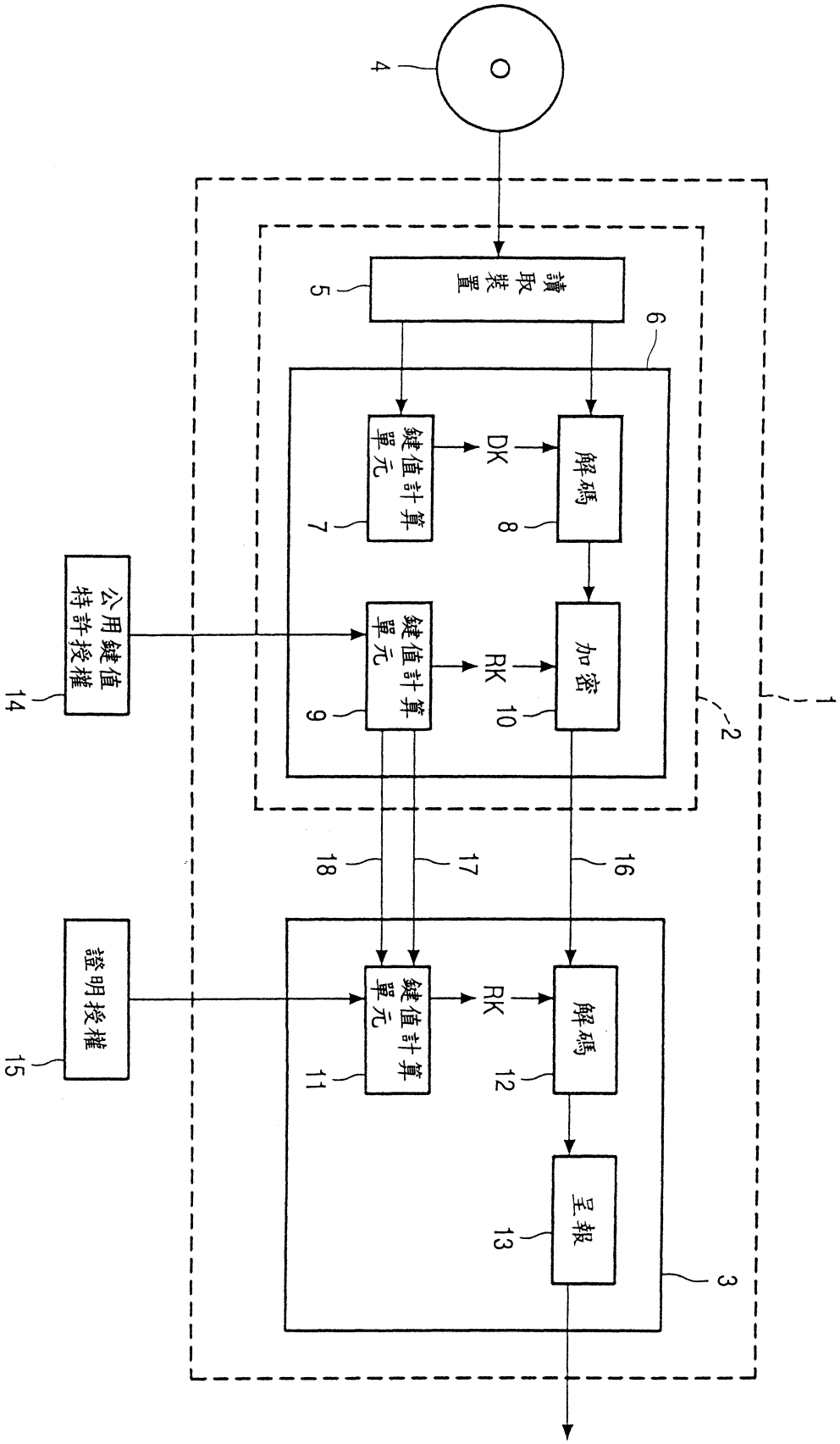

圖 1