（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

德

2000 年 08 月 21 日　100 40 854.0

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)

本發明是有關於尤其是用於付費-電視-應用之晶片卡，中避免沒有經由晶片卡之編碼(encode)而將資料信號解碼(decode)。

付費-電視-使用之基本功能在於須將電視信號編成密碼，使其不可由電視機產生。此等電視信號之解碼(decode)是在解碼器(decoder)中進行，其作爲所謂的設定-頂-盒(Set-Top-Box)而爲熟知。爲了可以使用某個程式所用的解碼器，使用者必須擁有晶片卡，其由供應商以使用者付費的方式發給客戶使用。

爲了在技術上實現此功能而在電視信號的空白間隔(blank interval)中傳送所謂的"詢問－值"，並且由解碼器繼續傳送給晶片卡。在此晶片卡中或在包含於其中的微處理器中，將密碼之算法在使用所儲存鑰匙的情況下使用於"詢問－值"中，並且將"回覆－值"傳送回解碼器。這於是可以進行電視信號之解碼(decode)。在此解碼器中大部份是涉及標準的裝置，因此幾種不同的付費-電視-節目使用不同的卡片卡可以相同的解碼裝置解碼。

因爲用於電視節目解碼之卡片對於所有的使用者爲相同，它証明對於入侵者有利，將此等仿冒仿製的晶片卡功能模擬並且銷售。此種仿製使用傳統之微處理器，並且經常具有所配置之付費-電視-卡片之原來軟體的大部份。因此，此在防止仿冒仿製中的技術問題來自於這些系統所有的卡片的功能相同，並且因此可以相當容易仿製。

五、發明說明(2)

截至目前爲止嘗試，藉由有規律地更換秘密鑰匙而縮短卡片之非法模擬器之使用壽命期限。然而較新的模擬器允許經由鍵盤或個人電腦(PC)-截面部位來更換鑰匙。此新鑰匙可以再度經由網際網路繼續傳送。

另一個用於防止仿冒仿製的方法是將整合客戶規格的單元(ASICs)作爲在晶片卡模組中的第二晶片。然而此單元仍然可以在硬體中的一次可逆工程製程之後在模擬器中模仿仿製。

有關於在電話卡或付費-電視-使用中晶片卡使用的問題是在"卡片"雜誌中 26-27/97 發行，第 315 頁正確地說明。在其中建議此晶片卡具有所配備的秘密共同處理器，以便能夠防止仿冒仿製。因爲其資料產量相較於外部邏輯爲高，其被使用於其功能之仿製，其仿製只有在使用相同的秘密共同處理器的情況下才可實施。雖然這使得仿製複雜且困難，然而此被禁止的仿製由於其大量的件數而可獲利。

因此，本發明的目的是說明一種晶片卡，其使得非法的仿製更加困難，並且它不可藉由上述的方法仿製。此外應說明一種方法將資料信號解碼，其使得可以使用防止仿製的晶片卡。

此目的是藉由晶片卡而達成，其具有微控制器與可功能程式化之硬體元件，此硬體元件與微控制器形成-單元。

此晶片卡包含一可功能程式化之硬體元件，因此在

五、發明說明(3)

晶片卡的分析中，只可偵測到瞬間的硬體狀態。然而因爲這在程式方法中可以重新確定，晶片卡之仿製只有用於時間的功能能力，一直至實施硬體元件之新的程式化爲止。

在使用解碼器的情況下，以晶片卡將資料信號解碼之方法具有以下之方法步驟：

— 將資料信號與"詢問－值"傳送給解碼器，

— 將此"詢問－值"傳送給晶片卡，

— 在晶片卡中將秘密算法使用於"詢問－值"，並且將"回覆－值"送回解碼器，

— 在使用"回覆－值"的情況下將資料信號解碼，其中此秘密算法是在可功能可程式化之硬體元件中實施，並且藉由發出控制指令給晶片卡而可修正。

此用於可功能程式化之硬體元件之新的程式化之控制指令，因此同樣地如通常使用之"詢問－值"與資料信號一起到達解碼器。因此可以有在小的時間間隔中規律地實施新的程式化而沒有浪費。在付費-電視-使用中例如可以每一小時一次新的程式化而沒有問題，其中使用者一點也沒有察覺。

當須配置秘密算法，使它可在硬體元件中基本上較在軟體中執行得快時則爲有利。它因此防止晶片卡的功能藉由可程式化之微控制器而可被仿製。

本發明配置之其他的優點是在申請專利範圍附屬項中說明。

五、發明說明(4)

本發明以下根據實施例作更進一步說明。

圖式之簡單說明

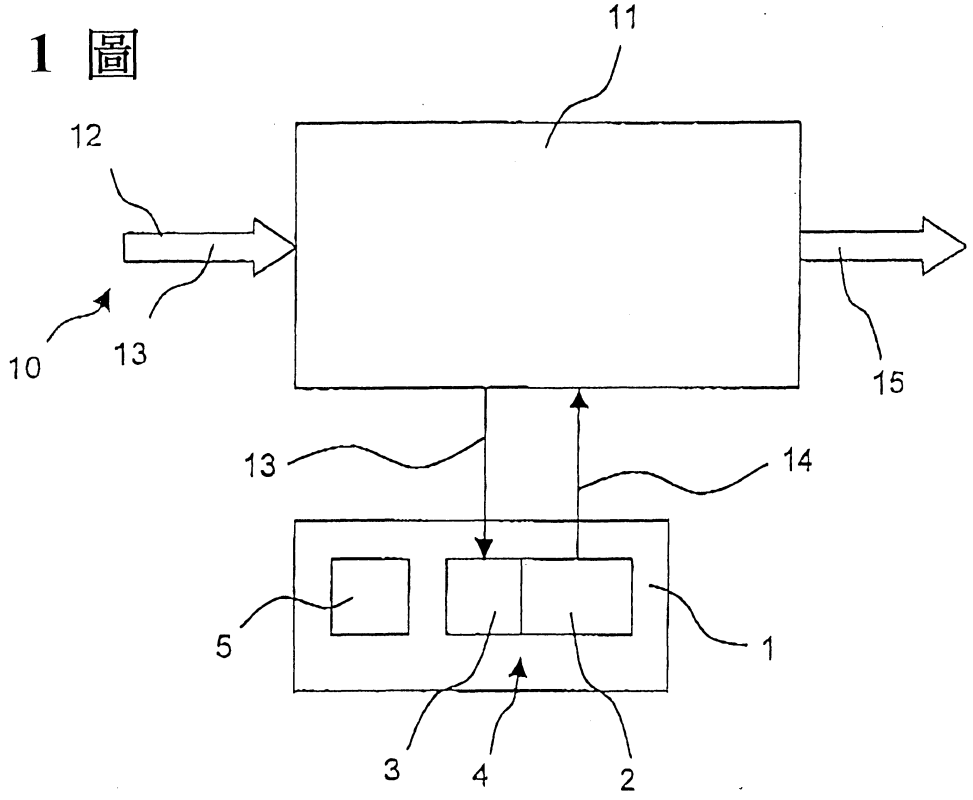
第 1 圖顯示在正常作業中具有根據本發明之晶片卡之配置之方塊圖。

第 2 圖顯示在新的程式化中具有根據本發明之晶片卡之配置之方塊圖。

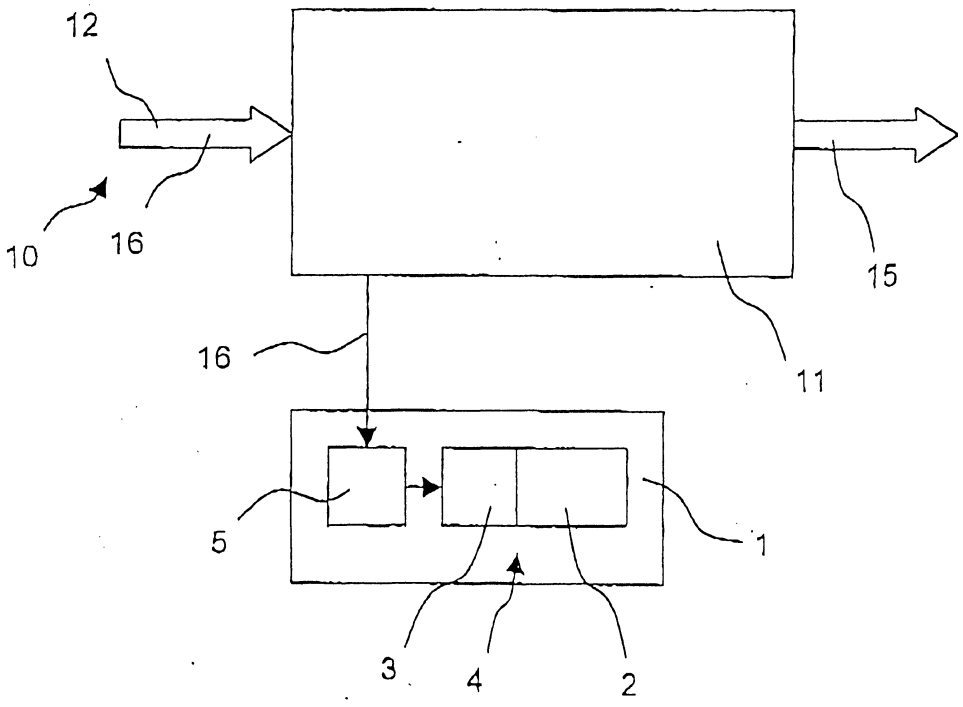
第 1 圖顯示根據本發明具有解碼器之晶片卡之使用。此晶片卡 1 具有微控制器 2 與功能可程式化(programmable)之硬體元件 3，例如是 FPGA。此微控制器 2 與功能可程式化之硬體元件 3 形成單元 4。爲了將此功能可程式化之硬體元件 3 程式化而設有程式化裝置 5。在正常作業中，將電視信號 10 傳送給解碼器 11。此電視信號 10 不但包括用於說明電視影像的資信號 12，還包括詢問值 13，其如在一開始所說明，繼續傳送給晶片卡。此秘密算法在詢問值 13 中的使用是藉由微控制器及/ 或功能可程式化之硬體元件提供回覆值 14，其被傳送回解碼器 11，並且它可以由於此回覆值的鑰匙功能或是起始(initial)值的設定，將資料信號 12 解碼並且作爲視訊信號 15 繼續傳送給電視機。

此第 2 圖顯示，像是實施功能可程式化之硬體元件 3 之新的程式化。在此情況中，與此資料信號 12 一起的程式化指令 16 是在空白間隔中傳送，因此使用者對此沒有察覺。解碼器將程式化指令 16 繼續傳送給晶片卡，因此在那裡此程式化裝置 5 回應(response)，其將功

第 1 圖



第 2 圖



申請日期	90、8、14
案　　號	90119872
類　　別	G06F 17/60

(以上各欄由本局填註)

92年1月7日修正補充

535085

公告本

發明 新型 專利說明書 (92年1月修正)

一、發明新型名稱	中　文	晶片卡及資料信號之解碼方法
	英　文	Chip Card and method to decode a data-signal
二、發明創作人	姓　名	1.葛德迪爾史契爾(Gerd DIRSCHERL) 2.彼得拉亞克曼(Dr. Peter LAACKMANN) 3.湯姆斯羅斯泰克(Thomas ROSTECK) 4.克麗絲汀史契奈肯布魯格 (Christian SCHNECKENBURGER) 5.布萊吉特威爾茲(Dr. Brigitte WIRTZ)
	國　籍	1.德國 2- 5.皆屬德國
	住、居所	1.德國慕尼黑 81543 艾汀格爾布拉茲 1 號 2.德國慕尼黑 81541 史契萊爾西街 11 號 3.德國奧特芬 83624 伯格哈姆 8B 號 4.德國霍亨基欽 85635 安姆甘特 9 號 5.德國荷爾基欽 83607 厄爾卡姆街 3 號
三、申請人	姓　名 (名稱)	印芬龍科技股份有限公司 Infineon Technologies AG
	國　籍	德國
	住、居所 (事務所)	德國慕尼黑 D-81669 聖馬丁街 53 號
	代表人 姓　名	1.麥可勾威什(Michael Gollwitzer) 2.荷斯特卻佛(Dr. Horst Schäfer)

92.1.7

五、發明說明(5)

能可程式化之硬體元件3重新程式化。此發射裝置此時具有此可能，其將電信號改變成不同於編碼或詢問值，因此只有在新的程式化功能的使用下才可以解碼。當此重新程式化的過程是經常例如每個小時實施時，而對於非法入侵者少有實用性，因爲他必須每一次分析新的演算法(Algorithm)，並且將FPGA相對應地程式化。

此外，爲了直接仿製此付費-電視-晶片卡，此侵入者可以甚至不使用商業上通用之微控制器，而是必須進行整個的逆向工程，以及具有微控制器2與功能可程式化硬體元件3之製造。

本發明之晶片卡的應用或本發明的方法對於付費-電視-使用當然不會造成限制，而是可以在所有的系統中使用，其中以詢問/回覆方法運作。

參考符號說明

1．．．．．晶片卡

2．．．．．微控制器

3．．．．．硬體元件

4．．．．．單元

5．．．．．程式化裝置

10．．．．．電視信號

11．．．．．解碼器

12．．．．．資料信號

13．．．．．詢問值

14．．．．．回覆值

15．．．．．視訊信號

16．．．．．控制指令

92.17 修正補充

A5
B5

四、中文發明摘要（發明之名稱：晶片卡及資料信號之解碼方法）

本發明是關於尤其是用於付費-電視-應用之晶片卡，其具有微控制器與功能可程式化之硬體元件(3)此硬體元件與微控制器(2)形成單元(4)。藉由功能程式化之可能性而可以將秘密算法(Algorithm)持續地改變，因此可以顯著地防止或妨礙晶片卡之仿製。在此根據本發明的方法中，使用具有用於付費-電視-發射器之解碼器之晶片卡。在此方法中，在電視信號中傳送控制指令，其導致功能可程式化之硬體元件(3)之重新程式化(re-programming)。

英文發明摘要（發明之名稱：Chip Card and method to decode a data-signal）

The present invention relates to a chip card, especially for pay-TV-application, with a micro-controller and a functions programmable hardware component(3), which forms the unit(4) with the micro-controller(2).
Through the possibility of the functions-programming the secret algorithm can be changed constantly, therefore the imitation of the chip-card is considerably prevented or impeded. In a method according to this invention the chip-card with a decoder for pay-TV-sender is used , in this method a control command is transmitted in the television signal, which causes the reprogramming of the functions programmable hardware components(3).

六、申請專利範圍

92.1.7

第 90119872 號「晶片卡及資料信號之解碼方法」專利案

（92 年 1 月修正）

六申請專利範圍：

1. 一種具有微控制器(2)與功能可程式化硬體元件(3)之晶片卡，其特徵爲此硬體元件與此微控制器形成單元(4)。
2. 如申請專利範圍第 1 項之晶片卡，其中此晶片卡(1)具有程式化裝置(5)，用於將功能可程式化之硬體元件(3)程式化。
3. 如申請專利範圍第 1 項之晶片卡，其中此功能可程式化硬體元件(3)藉由晶片卡所供應之控制指令(16)而可程式化。
4. 如申請專利範圍第 1 項之晶片卡，其中藉由功能可程式之硬體元件(3)而實施秘密演算法。
5. 一種資料信號之解碼方法，其以

—解碼器(11)與

—晶片卡(1)來進行，

其具有以下步驟：

—將資料信號(12)與詢問值(13)傳送給解碼器(11)，

—將詢問值(13)傳送給晶片卡(1)，

—在晶片卡(1)中將秘密演算法應用於詢問值(13)中，並將回覆值(14)回送給解碼器(11)，

—在使用回覆值(14)的情況下將資料信號(12)解碼

六、申請專利範圍 91年1月7日修正補充

，其特徵爲，

此秘密演算法在功能可程式之硬體元件(3)中實施，並且藉由發出控制指令(16)給晶片卡(1)而可修正。

6. 如申請專利範圍第 5 項之解碼方法，其中

此控制指令(16)由解碼器(11)接收，且隨後繼續傳送給晶片卡(1)。

7. 如申請專利範圍第 6 項之解碼方法，其中

在電視信號之空白間隙中的控制指令(16)是由解碼器(11)接收。

8. 如申請專利範圍第 4 項之解碼方法，其中

硬體元件(3)中的秘密演算法基本上可較軟體中的秘密演算法執行得更快。