公告本

381057

申請日期	87 年 7 月 29 日
案號	87112494
類別	B42D 15/10

A4
C4

（以上各欄由本局填註）

381057

發明 新型 專利說明書

一、發明 新型 名稱	中文	半導體裝置
	英文	
二、發明 創作 人	姓名	(1) 宇佐美光雄
	國籍	(1) 日本
	住、居所	(1) 日本國東京都立川市高松町三－二一－三矢嶋大廈一〇二號
三、申請人	姓名（名稱）	(1) 日立製作所股份有限公司 株式会社日立製作所
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都千代田區神田駿河台四丁目六番地
	代表人姓名	(1) 金井務

裝 訂 線

經濟部中央標準局員工消費合作社印製

（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	1998 年 3 月 26 日	10-078212	☑有主張優先權
日本	1997 年 8 月 7 日	9-212881	☑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）

（技術領域）

本發明有關於防止僞造或變造之半導體裝置，特別是有關於ＩＣ卡。

（背景技術）

關於以往之ＩＣ卡之僞造・變造技術揭示於「Proceedings of the 2nd Workshop on Electronic Commerce, Oakland California, Nov. 18-20, 1996」。之文獻上。

揭示於上述文獻之防止僞造技術乃在ＩＣ卡之晶片內記憶有可限定其處理之所謂擔任鑰匙之職務之「鍵碼」（Key Code）。

此鍵碼乃做爲接受服務（例如公用電話、通訊、遊戲等）之應付費之使用者之ＩＤ來使用。例如對應於信用卡之號碼者。各服務系統乃從使用者所持有ＩＤ之金融機構隨應於該服務的領去服務費等。再者，此鍵碼亦可使用做使用者之信用之校對。

此鍵碼雖然收容於存儲區域之內，惟由第三者所窺閱時即同類之卡將被僞造・變造。

又ＩＣ卡有與讀取・寫入器接觸而實施資料之交換等之接觸型，及藉由無線技術來交換資料之非接觸型，兩者均於ＩＣ卡之中具有存儲區域以及對該存儲區域實施資料交換之輸出・輸入區域。在此輸出、輸入區域上設有處理器電路。由而可實施複雜的密碼處理。

接收容於該存儲區域之鍵碼乃具有將ＩＣ卡、電氣的

五、發明說明（2）

、物理的或化學的予以分析之後被讀取之危險性。鍵碼乃電氣的存儲於存儲區域之存儲單元中，換言之，存儲單元乃冲電（電子（電荷））而保持記憶（存儲）。因此例如提高電子顯微鏡之分解能即得以圖樣之方式讀取。再者藉由使用微細加工裝置來加工存儲單元周邊使連接於周邊電路之配線露出，以資驅動存儲器之周邊電路本身而可讀取儲存單元。

爲了防止此種碼之讀取之先前技術乃，常備有電池，而有以任何電氣的、物理的、化學的操作而對ＩＣ晶片有侵犯時，藉由電池之機能由電源降低等而使記憶消除等方法。

例如使用電池時，在ＩＣ卡之晶片周邊設置用於感測出有分解的侵犯之感測器，而可以連動於此感測器之輸出而可消去存儲（記憶）內容之電路啓動。如使用ＳＲＡＭ爲存儲單元時，ＩＣ卡被分解時，電源ＯＦＦ而記憶內容會消除。

又爲了防止僞造而形成碼之先前技術係例如揭示於日本專利公報特開昭５９－１０９３７號。這是爲了提高對於僞造等之安全性起見，測定天線之諧振頻數及該返送波之振幅及相位偏差，依照保持秘密之算式將該測定值變換爲對應之數值，而將該數值及被秘密保持之編號予以結合做爲碼號而予以記憶者。

此碼號係永續的記憶於ＩＣ晶片之存儲區域中。

以往之，使用電池之防止僞造之技術時，須在每一個

五、發明說明（3）

ＩＣ卡上備設電池，ＩＣ卡之成本會增大，又ＩＣ卡之使用期間即依存於電池之壽命。又藉由衝擊之電池之破損或接點不良而使可靠性降低。電池之薄膜化困難，有ＩＣ卡變厚等之問題存在，阻礙其實用化。

又依照電氣的各性質來決定碼之先前技術時，例如偏差之對象而採用電路之特性偏差時，偏差之範圍窄狹而容易僞造，又由外部容易測定特性偏差，以及對於藉由分解積體電路來解讀上，並沒有考量等等對於僞造之效果並不充分。

本發明之目的乃提供一種低成本且可靠性高之僞造變造防止方法以及使用它之半導體裝置。

（發明之揭示）

上述目的乃由，在ＩＣ晶片及基板側分別備設有一個或複數個之其表面備有不定形之凹凸之電極，而以倒裝法將ＩＣ晶片及基板之各電極與電極予以連接，並將該連接阻抗予以類比／數值變換後做爲鍵碼而可達成。

換言之，由於電極表面呈顯不定形凹凸之緣故，所以將連接之電極一經拉開時即無法成爲與離開前相同之接觸狀態，因此由而可能推定有破壞的侵犯。

又上述目的乃由，在ＩＣ晶片及基板側，分別設有一個或複數個之電極，而以倒裝法將ＩＣ晶片及基板之各電極與各電極藉由導電性接著劑而予以連接，將該連接阻抗（電阻）予以類比／數值變換，做爲鍵碼而更有效果的達

成。

即由於藉由導電性接著劑（之接著），所以該類比量之電阻值更呈顯不定狀態，接觸電阻之偏差將被擴大。

又上述目的乃由在ＩＣ晶片及基板側，分別設有一個或複數個之電極，而以倒裝法將ＩＣ晶片及基板之各電極與各電極藉由含有導電微粒子之異方導電接著劑來連接，將該連接電阻予以類比／數值變換，做爲鍵碼而更有效的達成。

即在異方導電性接著劑中，於接著劑之中有金之微細粒子（５～１０μｍ）之分散狀態，將它挾於電極間而有使電阻值產生偏差之效果。

使上述電極之材料與異方導電性接著劑之導電微粒子之主成份相同時，更可獲得大的效果。

又上述目的乃由在ＩＣ晶片及基板側，分別設有其表面備有不定形之凹凸之一個或複數個之電極，而在ＩＣ晶片上罩蓋薄片以資分別連接各電極與各電極，將該連接阻抗予以類比／數值變換，做爲鍵碼而可達成。

即以往之正裝方式之ＩＣ卡用晶片之下，在其表面貼合薄片即直接可以用ＩＣ晶片之過程因此可實現低成本。

上述目的乃上述被類比／數值變換之碼之被讀出於ＩＣ卡之外，被密碼處理再寫入於該ＩＣ卡之ＩＣ晶片之存儲區域，由而更有效果的達成。

即以正常的手續所形成之變換碼之被寫入於晶片內即可以認識它正當（真）之卡。

五、發明說明（5）

上述目的乃上述被類比／數值變換之碼之在ＩＣ卡之該晶片內而被密碼處理而讀出於ＩＣ卡外而經密碼處理，再度寫入於該ＩＣ卡之ＩＣ晶片之存儲區域由而更有效果的達成。

即由於在ＩＣ晶片內予以密碼處理，由而以線路監視器而被讀出資料之下，由於ＩＣ晶片之鍵碼仍然不會被讀出所以會增加其安全性。

上述目的乃由於被形成之ＩＣ卡之鍵碼之由讀取・寫入器所讀取，與ＩＣ卡之登錄碼一齊保存於資料庫，而更有效果的達成。詳言之，ＩＣ卡乃由系統之支持而被實用化，而如果ＩＣ卡上之鍵碼之被登錄於系統之資料庫時即可以安全的運用而可能使用於認證系統上。又登錄碼可以有，ＩＤ號碼、姓名、密碼編號、個人之屬性資料、服務之來歷資料、信用卡、帳號資料、信用水平等等。

上述目的乃所形成之ＩＣ卡之鍵碼之使用防止ＩＣ卡之僞造及變造之用而更可達成效果。

即鍵碼係由接觸電阻之偏差來實施，因此成爲同一鍵碼之或然率極小，製作同一卡乃非常困難。

上述目的乃所形成之ＩＣ卡之鍵碼係使用於ＩＣ卡與讀取・寫入器之互相認證由而更有效率的可以達成。

即在本發明所使用之鍵碼乃由於再現非常困難，所以可使用於互相認證之用。

上述目的乃將所形成之ＩＣ卡之鍵碼與密碼或與生物的特徵碼相連結而使用於本人之認證而更有效率的達成。

五、發明說明（6）

即將人體特徵於ＩＣ卡中與鍵碼一齊記憶，即很難僞造，可以提供該人固有之個人認證卡者。

上述目的乃由使用生物特徵碼（掌紋碼、指紋碼、嗅覺碼、臉碼、聲音碼、靜脈碼、瞳孔碼、ＤＮＡ碼）爲碼而更有效果的可達成。

即以上述生物統計學上所可想到之該人之個人碼，由而安全的可實現個人認證。

上述之目的乃公開鍵密碼之解讀或共同鍵碼之解讀並不是藉介讀取・寫入器而藉由上位之系統來實施由而更有效率的可達成。

即以多數設置之讀取寫入器來予以實施時即該讀取・寫入器之被第三者所分解而有密碼系統之被解讀之可能性。而以數量少之上位系統來嚴重的予以管理即可減低此危險。

上述目的乃由所形成之鍵碼之做爲電子貨幣而ＩＣ卡之被使用時之本人認證或僞造之校對或ＩＣ卡與讀取・寫入器之互相認證上之使用而更有效率的達成。

即安全的實施ＩＤ時，即可應用於付款等系統，可使用ＩＣ卡做爲電子貨幣。

上述目的乃由於該類比／數值之變換之分解能之四階段以下而有效果的達成。

即將分解能抑制於四階段以上之結果，雖有歷時性之接觸電阻之變動之下，仍然可靠性良好的使之再現。

上述目的乃由一個各電極與各電極之連接部份之尺寸

五、發明說明（7）

爲１５μｍ以下而更有效率的達成。

即使電極成爲複數之小墊陣列之結果，經濟性良好的可提供小面積且安全性高之鍵碼。

上述目的乃藉由複數之各電極與各電極之接觸部份之矩陣狀的被排列而成而更有效率的達成。

即可以提供，緊湊小型化之連接陣列。

上述目的乃由所形成之鍵碼之使用於複數之卡之同時回答時之鑑別用之碼，由而更有效率的達成。

即由於幾乎沒有同一鍵碼之存在因此可用於認識複數之卡之碼之用。

上述目的乃，在ＩＣ晶片及基板側，分別具有其表面備有不定形之凹凸之一個或複數個之電極，將該ＩＣ晶片以倒裝法且分別令各電極與各電極予以連接，而將其連接阻抗予以類比／數值變換時，該類比值乃迴避了該據於境界領域者而更有效率的達成。

即實施Ａ／Ｄ變換時，據位於類比值至數值變換之境界者時即由歷時之變化而數值值有變動之可能，因此據位於境界者不予使用，或改變境界值而可以增加可靠性。

再者，爲了達成上述目的之本發明之ＩＣ卡乃，具有：互相對向地配置之基板及半導體晶片，及分別互相對向且離開的配置於該基板及半導體晶片之互相對向之側之表面上之電極，將形成於上述電極間之容量之容量值之予以數值化者使用於ＩＣ卡之鍵碼。

即本發明中，令形成於分別互相對向且離開的予以配

五、發明說明（8）

置而成之電極之間之容量之容量值予以數值化，而將該被數值化之容量值使用爲ＩＣ卡之鍵碼，上述容量值乃隨機的不同，並且依公開鍵之算式地被密碼化，因此得由第三者來僞造或變造ＩＣ卡之可能性很少。

上述半導體晶片上形成上放大器，以分別連接於該放大器之上述容量及規定之電阻而形成了積分電路，上述容量值之數值乃將由上述積分電路而出現之電壓值之被類比・數值變換來實施。不但是上述放大器，上述電阻（阻抗）當然亦可以預先設置於上述晶片內。

於上述基板及半導體晶片之上分別形成複數之上述電極，形成於互相對向且離開地被配置於上述電極之間之容量令該容量值係隨機的不同者。如上述容量值爲隨機的不同之情形下設如有一個容量值被第三者所知曉之下，其他容量被知曉之可能性幾乎不會有，由第三者之ＩＣ卡之僞造或變造就非常困難。

如上述容量值之隨機的不同之容量乃得由：例如於上述互相對向且離開而配置之電極之間，介置有由相同之種類之電介質所成厚度互相不同之電介質膜，於上述互相對向且離開而配置之電極之間，介置有由不同之種類之電介質所成之電介質膜　。

上述互相對向且離開而配置之電極之間之距離乃互相不同者，等等手段即可形成。爲了實現電極間之距離互相不同之構造之一手段乃令上述互相對向且離開地被配置之電極之厚度係至互相不同者就可以。

五、發明說明（9）

爲形成容量值之隨機的不同之容量，可能使用種種手段，例如於上述互相對向且離開的予以配置之上述電極之間，介置有直徑之互相不同，且同一種類之粒子狀之電介質體就可以。

本發明中上述介置於互相對向之電極之間之上述電介質膜乃可使用由，$BaSrTiO_3$膜、PST膜、$CaTiO_3$膜及KH_2PO_4膜所成之群中所選用。

依本發明鑑別IC卡之正否（真僞、有無變造）乃以下列方法實施。

首先對於具有形成有姓名區域及鍵碼之半導體晶片之IC卡，以讀取・寫入器質詢該IC卡之所有者之姓名。IC卡即對於此質詢回答讀取・寫入器該IC卡所有者之姓名。讀取寫入器即依據此回答將姓名送至資料庫質問其鍵碼，讀取寫入器乃再使用隨機數產生公開鍵碼，送至IC卡，而IC卡即將上述容量值予以數值化，將　得之隨機數值予以密碼化之後回答於讀取寫入器・讀取寫入器，乃解讀由上述IC卡之密碼化之回答，對比上述資料庫之鍵碼做對比，由而鑑定上述IC卡之正否（真僞、有無變造）。

由於，容量值之隨機的被形成之容量來形成該鍵碼，並且由IC卡而被密碼化，所以由第三者來解讀其鍵碼之可能性非常少。

於上述資料庫中，與上述使用者之姓名與上述IC卡之鍵碼之數值一齊預先予以登錄。

五、發明說明（10）

本發明中，爲了形成容量值之隨機的不同之容量可採用很多方法，惟最代表性的方法乃改變容量之電介質膜之厚度或種類之方法。

爲了形成厚度之隨機的不同之電介質膜乃，例如以習知之方法形成ＢＳＴ膜等之電介質膜之後，施予雷射光之照射隨機的改變雷射之強度而實施掃瞄，即會發生隨機的程度不同之蒸氣（氣化），可獲得厚度之部份地隨機的不同之電介質膜。再者將粒狀之電介質膜介置於兩電極之間，在兩電極之間，施加隨機的不同之壓力也可獲得其厚度之隨機的不同之電介質膜。

實施發明之最佳之形態。

＜實施例１＞

使用第１圖說明本發明之一實施例。在ＩＣ卡之基板１４上形成有基板電極１３。另一方面在ＩＣ晶片１１上也形成有晶片電極１２。於這些電極１２、１３之表面形成有不確定之凹凸面。例如這樣表面之電極與電極密接時，凸之部份乃不規則的相接觸，因此導通電阻乃與表面之狀態有所關連而呈顯隨機值。本例中凹凸乃備有±１ｎｍ～±１００μｍ之大小。

將此狀態之接觸阻抗（電阻）值予以類比・數值變換時，即可獲得１位元至約１０位元之資料量。即Ａ／Ｄ變換之位元數而例如ＯＮ／ＯＦＦ即１位元，將電阻值以１０位元之精度地予以數值變換即可獲得１０位元之數據

五、發明說明（11）

。

電極乃採用複數個也沒有妨礙，因此很容易獲得電氣的大量之隨機圖樣（Ａ／Ｄ變換之電阻（阻抗）值之偏差）。獲得相同之圖樣乃非常稀少，實用上不會再現之程度。又計測器之精度良好時，電阻值就不會再現，又起於溫度變化之溫度漂浮應設法消除才行。

依此方法時，如電極一經被分離時，即連繫之狀態會分離，因此再度將電極予以連結也很難使之再現原來樣式之連繫狀態。換言之施予晶片之分解時，在晶片上之各所被實施相同之非再現分離，因此做爲對於物理性化學性之晶片操作之僞造防止策而非常有效，且此方法時施予破壞即可視做記憶會消失，因此可以說屬於不需要電池之一種自爆型存儲器。

使用第２圖說明將本發明適用於ＩＣ卡時之實施例。

在本例中，於ＩＣ卡２１之角隅部設有ＩＣ晶片載置部２２，載置於此處之ＩＣ晶片２４之中，設有電極載置部２５及存儲區域２３。在電極載置部２５上有複數之電極２６，介著含於異方導電性接著材中之導電微粒子２７而連接於對向於上述電極２６地設置之ＩＣ卡基板側之電極（不圖示），導電微粒２７係具有放大電極之表面之凹凸之職責。將由此導電粒子２７之電極間之連接阻抗予以類比／數值變換後用於鍵碼。又本例中以複數之電極爲例，惟一個之電極亦可以。又ＩＣ卡基板上所設之電極與ＩＣ晶片之電極之連接係，對於設於ＩＣ卡基板之電極上

（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）

以倒裝法將ＩＣ晶片定位而予以連接。此時令電極材料之主成份與異方導電性接著劑之導電微粒子之材料之主成份相同，換言之例如金墊即用金粒子、鋁墊即鋁粒子，由而可提高對於凹凸之放大效果，且可防止以化學的或透過型觀察來讀取存儲之內容。所以採用此方法時很容易獲得將連接阻抗之Ａ／Ｄ變換所獲得之隨機數之隨機圖樣。

將此產生鍵碼之部份使之爲小面積，且將微小粒子之尺寸爲１５μｍ以下，最好由５～１０μｍ，就可以實現將電極陣列緊湊化小形化，進一步將複數之電極與電極之連接部份排列成矩陣狀，就更能以小面積地（面積效率良好地）可形成電極也。

使用第３圖說明在第２圖所示之電極之電極接觸電阻３２變換成鍵碼之方法。

以電流源３１而使電極接觸電阻３２發生電壓，以放大器３３放大，以Ａ／Ｄ（類比／數值）變換器３４而予以數值變化。於輸出端子３５發生電壓訊號。以此電壓訊號做爲「鍵碼」。例如Ａ／Ｄ變換器爲９位，而ＭＡＸ值爲約１Ｖ，分解能爲１ｍＶ，即１～１０２３Ｖ，以二進數即１１１１１１１１１１（＝１０２３）。類比／數值變換器３４即設置於被形成該電極之ＩＣ晶片之中。

使用第４圖說明將鍵碼寫入於ＩＣ晶片之存儲區域之順序。被變換類比・數值之鍵碼乃以讀取寫入器（３ＷＵ）而讀出於ＩＣ卡外，在讀取・寫入器側而被施予密碼處理。例如鍵碼１１１１１１１１１１被讀出被密碼處理成爲

五、發明說明（13）

例如１０１０１０１０１。而後該被密碼處理之碼１０１０１０１０１即寫入於該ＩＣ卡之ＩＣ晶片之存儲區域。

或，被類比／數值變換之碼不在讀取・寫入器側被密碼處理，而是在ＩＣ卡之該晶片內被密碼處理後讀出於ＩＣ卡外，而被密碼處理之後，再度寫入於該ＩＣ卡之ＩＣ晶片之存儲區域。如將該晶片內之密碼處理係公開鍵密碼處理，即只有當事人可能讀取被Ａ／Ｄ變換之內容。本案中所指之公開鍵密碼處理乃，鍵成爲公開，而密碼化即任何人均可做惟無法回復之密碼處理。例如從很多人拿到密碼化之文書之結果也只有特定之人才能解讀。

被密碼化者或未經密碼化之原狀之Ａ／Ｄ變換之內容係由卡讀取器或由更上位之系統而被密碼化之後，再度送入於ＩＣ卡之晶片內，寫入於ＩＣ晶片內之存儲區域。

被密碼化者之再被密碼化之例子有，首先以自己之鍵施予密碼化後將它以公開鍵送入之方法。由對手看來，只有特定之人才能做到之方法，電子簽名是其一例子，被密碼化之內容之被密碼化之例子係，衛星傳送或付費電視頻道上所使用。有鎖碼之密碼方式。

該存儲內容係，例如寫入於不揮發性存儲器，成爲ＩＣ卡之ＩＤ號碼。此ＩＤ號碼乃在每一次使用時每一對實施校對（照合）。又上述碼由於實質上不可能形成同一碼，因此可以將此碼用做ＩＤ號碼，而可顯示卡之正當性。

五、發明說明（14）

又模擬A／D變換之値之狀態之下，由於上位之系統之密碼非公開因此無法製作ＩＤ號碼，因此僞造乃成爲困難。

即，雖可讀出存儲內容，但是由於從隨機數之發生到A／D變換以及密碼化之部份不能再現，因此如予以僞造即以系統校對而可發覺。

再者，由於使用校對定序來實施卡之校對，因此被變造之卡片會被拒絕。將讀出在於卡內之連接電阻之被A／D變換之數値，而以系統內之密碼鍵予以密碼化者，與存於卡內之存儲器內之碼予以對照校對，即可判斷該碼是否正當之卡。

以圖5說明，電極間之連接上使用含有導電微粒子51之異方導電性接著之實施例。在電極之間挾接有較電極表面之凹凸大之導電微粒子，此導電微粒子係隨機的被分散，達成形成於電極表面之凹凸相同之職責。1μm以下之凹凸或平坦性高之各電極之間即不容易發生接觸電阻之差異，此時如有5～10μmø之導電粒子存在時即由於導電粒子之受形之程度而容易發生偏差。

又，電極之表面狀態，導電微粒子之表面狀態，連接場所，連接時之變形、數量、電極之面積等等可發生隨機的電阻値之要因有多種多樣。此導電微粒子乃對於塑膠粒子施予鈦金鍍金，或鎳粒子等種種粒徑以及該混在均可能。又此導電粒子乃維持分散之狀態下以環氧接著樹脂而牢固地予以接著，因此可以安定地維持連接狀態。

五、發明說明（15）

圖６乃表示，在ＩＣ晶片及薄片上分別備有一個或複數個之表面不定形而備有±ｎｍ～±１００μｍ之間之大小之凹凸之電極。以各電極之能分別對向地在ＩＣ晶片上罩蓋薄片以資連接各電極與電極，而將該連接阻抗（電阻）予以類比／數值變換，做爲鍵碼之ＩＣ卡之實施例。又薄片乃可以使用ＰＥＴ。

圖６（ａ）乃平面圖。在ＩＣ晶片６１之上方之晶片電極６５之方面設置薄片６２。設於該薄片之薄片電極６３與晶片電極６５係被連接。圖６（ｂ）即表示圖６（ａ）之Ａ－Ａ´之一部份剖面圖。

此構成係與第１圖相同，與前面之實施例相同，利用電極之表面之凹凸所致之接觸電阻之隨機性及使它分離時之狀態消除。

再者，薄片與該ＩＣ晶片之一部份上設有貫穿電極６４，以資監視備有凹凸之電極間之接觸電阻。本例中，電極間之連接乃以互相各一爲例。惟如圖２所示之複數個時亦可以，使之成爲如圖６所示之構造，由而以通常之正裝法而實裝並且予以結線之ＩＣ卡之下，亦可適用此防止僞造技術。即不依ＩＣ晶片之實裝方法，任何ＩＣ卡也可以備有使用連接電阻之資訊之鍵碼。以使用薄片之本技術而可能安全的享受ＩＣ卡之方便性。

圖７係表示，使用本發明之鍵碼以確認爲該ＩＣ卡之是否僞造用之流程圖。按適用ＩＣ卡之系統之運用對稱之金額都是顯著的與磁卡相比較多額者，所以（１）ＩＣ卡

之使用者是否本人之確認，（２）ＩＣ卡是否被僞造之確認。（３）爲了判斷ＩＣ卡之正當性必要與讀取・寫入器（系統）之互相認證。而本發明中（１）～（３）均可能做確認。

圖７之流程乃關於（２）確認是否被僞造者之用。首先以公開鍵密碼處理ＩＣ卡內晶片小墊之連接電阻Ａ／Ｄ變換之鍵而以讀取・寫入器來讀取。鍵乃以隨機數的被產生，所以此鍵碼即以一義的賦予具有同一之鍵碼之ＩＣ卡很少有存在之機會。

再者，此鍵碼乃由微小部份之接觸電阻之Ａ／Ｄ變換而成者，由ＩＣ卡內部之微細元件及配線來數值變換，因此以接觸於ＩＣ晶片而直接採電氣的方法看出該鍵碼乃屬於非常困難之事情。

惟如果被數值變換之鍵碼，如果對於讀取・寫入器之質問而原狀之位元列的被讀出時，即會被線內監視，很容易由第三者獲取鍵碼失去防止之機能。因此對於ＩＣ卡賦予公開鍵，在ＩＣ卡內對該鍵碼施予密碼化，以資由ＩＣ卡獲得被密碼化之資料，由而使之雖經線內監視之下，仍然無法讀取該鍵碼也。

接著，將鍵碼解讀，而以共同鍵密碼方式，例如以２０００位元共同鍵而施予密碼化。將它設爲Ａ，接著直接讀出該ＩＣ卡內之存儲區域內之資料，將它設爲Ｂ、Ａ與Ｂ相一致時，即可確認ＩＣ卡並非僞造。

此時之公開鍵密碼之解讀或共同鍵密碼之解讀得由讀

五、發明說明（17）

取・寫入器來實施。再者如此解讀於上位之系統來實施即可以做爲，以讀取・寫入器內以公開鍵或共同鍵中予以解讀密碼而讀取・寫入器之被分解影響系統之安全性之問題。

如上所述，在ＩＣ卡內而以本發明之方法所形成之ＩＣ卡之鍵碼乃可使用於防止ＩＣ卡之僞造及變造也。

圖８乃表示上述（３）所示之ＩＣ卡與讀取・寫入器間之互相認證之流程。以實施例揭示二個方法。８（ａ）所示之第１方法乃，首先以該ＩＣ卡內之晶片小墊（以線接等較墊爲小之墊而１００μｍ以下）之連接電阻之類比／數值變換之鍵碼在ＩＣ卡內施予公開鍵密碼處理而以讀取・寫入器來讀取。

在讀取・寫入器側即解讀此鍵碼，而由存在於系統之資料庫讀出該ＩＣ卡之鍵碼，如相一致時即互相認證完成。

在資料庫內登錄有ＩＣ卡之使用者之鍵碼，再附隨於鍵碼而記錄有使用者之各種資料，使用記錄（何時，何用途，多少錢，在何處使用等）。被系統管理之鍵乃以嚴格的被管理。

以圖８（ｂ）說明第二之方法，首先使用讀取・寫入器內之ＭＰＵ（微處理器）之隨機數算式而製成隨機數，對於ＩＣ卡賦予隨機數，而將ＩＣ卡內晶片小墊之連接電阻之類比／數值變化之鍵碼之密碼化之資料送回至該讀取・寫入器。該讀取・寫入器中即產生隨機之後，由對於讀

五、發明說明（18）

取・寫入器以ＬＡＮ，無線，網路等連接之應用系統之資料庫所獲得之鍵而製作同樣的予以密碼化之資料，與上述之資料相對比校對，如果相一致即互相認證完成。

使用圖９而以一個讀取・寫入器而讀取複數之無線式之ＩＣ卡時，分別的鑑別ＩＣ卡之方法。本發明中賦予同一ＩＤ碼乃非常的少，因此有效的可活用此ＩＤ碼。在ＩＣ卡９１上載置有ＩＣ晶片９２而此晶片備有鍵碼產生部９３。另一方面他之ＩＣ卡９４中載置有其他之ＩＣ晶片９５，同樣備有鍵碼產生部９６，各自之鍵產生部份之鍵碼不同，因此將此碼用做ＩＤ碼，就可以區別ＩＣ卡９１與９４，鍵碼乃增加其位元數即可無限制地可增加ＩＤ數，因此可區別近乎無限之ＩＣ卡。

圖１０表示爲了備有依本發明之鍵碼之ＩＣ卡用之系統之構成。系統乃備有ＩＣ卡１０２，讀取・寫入器１０１以及資料庫１０７。依據動作程序說明各機能部份。首先，

（１）由讀取・寫入器側對於ＩＣ卡詢問，特定該卡之管理責任者用姓名碼或認識碼１０４。此姓名碼或認識碼１０４乃被收容於ＩＣ晶片１０３中之存儲之規定區域。又讀取・寫入器待以ＬＥＤ感測器來感測卡片之存在。對於卡片之電源供給乃如在於非接觸式卡之時即以電磁波所實施。又，卡之是否在能正常的動作之狀態乃，首先由ＩＣ卡向讀取寫入器返送對讀取寫入器送出複位訊號即可知ＩＣ卡之狀態之碼（Answer to Reset）由而做校驗。

五、發明說明（19）

又使ＩＣ卡之電源ＯＮ，而使之成復位（Reset）狀態，由ＩＣ卡向讀取寫入器以附地址的送出讀指令，即由ＩＣ卡將姓名碼送至讀取・寫入器。由而可以確認姓名碼也。接著

（２）ＩＣ卡乃將姓名碼１０４回答於讀取・寫入器１０１。即由讀取・寫入器指令而ＩＣ卡內之電路動作，由存儲器讀取姓名碼，將姓名碼回答於讀取・寫入器。

（３）讀取寫入器乃檢索在於資料庫１０７內之資料庫上之姓名碼１０８而獲得資料庫上之鍵碼１０９。又讀取・寫入器即指定記憶有姓名碼之存儲地址，以讀指令來讀出姓名碼。又卡片有複數存在時即藉由輻輳控制來選出一個卡。接所謂輻輳控制係，對於卡而由各位元之端而詢問〝０〞，〝１〞，而從複數之卡中選擇出之１卡之控制法，使複數之卡不致於同時回應者。

（４）讀取・寫入器乃將隨機數送至ＩＣ卡。此隨機數乃例如由讀取・寫入器內之ＭＰＵ而以電路的產生。由ＬＡＮ或網路從服務部份供給隨機數亦可以。

（５）ＩＣ卡乃於接受了隨機數之時點而依指令受讀取寫入器之指示，製作依照鍵碼產生部１０５所產生之鍵碼所密碼化之隨機數。另一方面讀取・寫入器乃與ＩＣ卡同樣使用由資料庫所獲得之鍵碼１０６，而將送至ＩＣ卡之同一隨機數予以密碼化，對照由此所獲得之被密碼化之隨機數之結果，與前述之由ＩＣ卡之密碼化之隨機數，如兩者一致即完成ＩＣ卡與讀取・寫入器之互相之認證由而

五、發明說明（20）

可認定ＩＣ卡之正當性。

又讀取・寫入器係與ＬＡｙ或網路，電路等而與服務設備連接，在該服務設備內設有資料庫。又服務設備上連接多數之讀取・寫入器。

所形成之ＩＣ卡之鍵碼（ＩＤ碼）乃與姓名碼或認識碼一齊收容於資料庫。

所形成之ＩＣ卡之鍵碼（ＩＤ碼）乃使用於ＩＣ卡與讀取・寫入器之互相之認證之用。又所形成之ＩＣ卡之鍵碼乃併用密碼或生物的特徵碼而可用於實施本人之認證之用。

生物的特徵碼乃可使用，將手掌予以圖樣化之掌紋碼，指紋之圖樣化之指紋碼，由人體所發生之氣味之嗅感碼、臉形圖樣化之臉碼、聲音之資料之圖樣化（數值化）或依分析值之聲音碼、靜脈之脈衝圖樣化之靜脈碼、眼睛之色彩或形狀圖樣化之瞳孔碼、ＤＮＡ之資料圖樣化之ＤＮＡ碼等等。

所形成之鍵碼乃可以用在ＩＣ卡之使用做電子貨幣時之本人認證或僞造之校對，或ＩＣ卡與讀取・寫入器之互相認證等等。由而可以免除被他人偷用卡之虞，安全的可實施財產或個人資料之管理。

上述系統內可以應用於，例如一般商店之付款、車票等購買、定期車票之剪票、許可證之校對、電話卡等之電話等之很多領域（交通、運輸、金融等等）。由而在商店提示卡即可購買商品，又看電影時不需要排隊購票而可以

五、發明說明（21）

觀賞可以預約旅館並付款。又經網路只影印雜誌之必要部來付款。可鑑賞付費頻道，人對人之英語會話之付款。又可替代信用卡，也可用於零星款項之清算，也可用於電腦系統或場所之進入等。

圖１１表示適用本發明之非接觸ＩＣ卡之構成例。ＩＣ晶片１１１乃在非接觸ＩＣ卡１１３之厚度方向之大中約中立面。而與形成於卡之大約中立而之線圈圖樣１１２相連接。線圈圖樣之會交叉之部份設有絕緣膜以資防止短路。

圖１２顯示，連接ＩＣ晶片之具有凹凸之電極與基板上之具有凹凸之電極，而發生於其間之接觸阻抗（電阻）之特性圖。

在橫軸上顯示流通於接觸阻抗部份之電流，於縱軸顯示發生之電壓。本例中乃以一例而顯示四條之代表特性，惟這些特性乃非常隨機的發生，因此有複數之電極間之電阻值之特性均不相同，又電流值係使用０．１～１ｍＡ之範圍之值，即電壓值上很容易有所差異。

本發明乃應用此種特性之偏差者。惟類比／數值變換時之分解能之任意設計乃不妨者。本例中，將分解能分爲四水準，由而再現性良好的可獲得電阻值，而很有效。

使電極之尺寸爲１～１５μｍ四方，而在其上面配置可以增加接觸電阻之偏差之要素（異形狀之粒子），而對於對向之各電極之間通過電流使電阻值變換成電壓，將此電壓值使用２位元之Ａ／Ｄ變換器而予以數值化而很容易

五、發明說明（22）

獲得四水準。即成爲，００、０１、１０、１１之圖樣。

這是由於接觸電阻乃隨由表面狀態所決定，因此對於歷時之變化亦應預先對處才行。將它可靠性良好地實現起見以不要令它必要以上的提高分解能，使之具有餘裕而可增加穩定性。

分解能乃由，連接電阻值變換爲電壓，又將Ａ／Ｄ變換時之電路之精度所決定者，而由溫度漂浮，應力，歷時變化而使再現性劣化。分解能可採取２～１００００程度之範圍之值。

再者，設定類比／數值之動作帶，將境界領域之接觸電阻即選擇據位於穩定點者，以求安定化。本例中所謂境界領域乃使之數值化時之境界，例如１０與１１之間。

將類比／數值變換之分解能定爲四階段（２～４階段）由而可使再現性提高。

又將所形成之鍵碼，用於複數之卡之同時回答時之判別用之碼，由而可以提供可靠性及安全性均優異之ＩＣ卡。

＜實施例２＞

圖１３表示本發明之第２實施例之剖面構造圖。如圖１３所示，本實施例乃該，形成於半導體晶片２１２上之厚度０．１～５０μｍ之金所成之晶片電極２１３，及由厚度０．１～１０ｍｍ之ＰＥＺ所成之基板２１５上所形成之由銀糊所成之基板電極２１４即互相對向地被配置而

五、發明說明（23）

成，上述晶片電極２１３與基板電極２１４之間介置有由ＢＳＴ（ＢａＳｒＴｉＯ$_3$）所成之電介質膜２１１。

上述晶片電極２１３與基板電極２１４之間之容量係依存於電介質膜２１１之材質，厚度及平面積。而此電介質膜２１１即得以粒狀，液狀或凝膠狀等等種種之形狀。本實施例即以粒狀之ＢＳＴ膜用做電介質膜２１１，在兩電極２１３、２１４間施加互相不同之壓力以資改變電介質２１１之厚度及形狀，由而很廣之容量之值之範圍而形成隨機的不同之容量。例如上述粒狀之ＢＳＴ膜之直徑爲１μｍ，施加壓力後之電介質膜２１１之厚度爲１０００μｍ電極面積１×１０^{4}μｍ^{2}時所獲得之容量值係４５ＰＦ。

使電介質膜２１１變形獲得規定之值之容量後，電極２１３、２１４及電介質膜２１１乃藉樹脂（不圖示）而使之固定而確定。

又此樹脂乃以在電電極２１３、２１４間分散電介質粒膜２１１以資形成電介質膜用之媒體而使用亦可以。或預先於電極２１３、２１４之間形成電介質膜２１１之後，以固定所獲得之構造地注入樹脂亦可以。任何一者均可獲得廣範圍的容量之值之隨機的不同之容量。

本實施例乃如上述使粒狀之ＢＳＴ變形以資形成電介質膜，因此，具有該斷面形狀之測定困難之電介質膜之面積或厚度之變更或設定很容易，及製造簡單及容易之利點。

五、發明說明（24）

再者，本實施例乃在電極２１３、２１４之間固定了一個電介質膜２１１，惟使用複數個之電介質膜２１１也可以。又各電極２１３、２１４，分別爲複數個亦可以。或電極２１３、２１４之面積互相不同亦可以，任何一者均能變更兩電極２１３、２１４間之由ＢＳＴ膜所成之電介質膜２１１之厚度及面積而隨機的實現了很多之容量值。

＜實施例３＞

使用圖１４說明本發明之第３實施例，圖１４（ａ）乃表示本實施例之平面圖。圖１４（ｂ）即其Ａ－Ａ´剖面圖，第１之電極２２１及第２之電極２２２均與第３電極２２３分別成對向地被配置，各粒子２２３、２２４均由ＢＳＴ所成之電介質粒子，惟在第１電極２２１與第３電極２２３之間也介置有小粒子２２４，第２電極與第３電極２２３之間也介置有比上述粒子２２４之粒子大之粒子２２５。

上述粒子２２４、２２５乃使用習知之氣體沈著法而形成，因此粒徑乃隨機的有所不同。電介質不等而直徑而不同，因此第１電極２２１與第３電極２２３之間之容量值，與第２電極２２２與第３電極２２３之間之容量值互相不同。因各電介質粒子之粒徑乃隨機的被分散，因此隨機的可獲得各電極的各不同之容量值。又只要能形成容量，各電極２２１、２２２、２２３之材質或形狀並不特別

五、發明說明（25）

的限定。

＜實施例４＞

使用圖１５說明本發明之第４實施例。圖１５（ａ）乃表示本實施例之平面圖。圖１４（ｂ）即其Ａ－Ａ´剖面圖。

第１之電極２３１及第２之電極２３２與第３電極２２３乃分別互相對向地被配置。在第１之電極２３１與第３之電極２２３之間介置有小的電介質之粒子２２４，惟如圖１５（ｂ）所示，由於第２之電極２３２較薄，因此第３之電極２２３與第２電極２２３之間之間隙很大，因此兩者之間不能保持電介質之粒子。該結果第２電極２３２與第３電極２３２之間之容量乃與第１電極２３１與第３電極間之容量顯著地變小。

由於各電極２３１、２３２之厚度乃隨機的不同，所以各電極２３１、２３２與第３電極２３３之間之間隙也隨機的不同，由而在各電極２３１、２３２獲得了隨機的不同之容量。關於厚度之隨機的不同之電極２３１、２３２，在本實施例中係採用形成電鍍電極之後，再使用以雷射來去除表面之方法來形成。

又在本實施例中，關於各電極２２３、２３１、２３２乃只要在此電極之間可以形成容量之條件下，關於其材質、形狀、以及尺寸並不特別的予以限定。

五、發明說明（26）

＜實施例５＞

使用圖１６說明本發明之第５實施例。容量２４１乃於上述實施例１所獲得，放大器２４２即形成於與上述容量２４１電氣的予以連接之半導體晶片之中。容量２４１乃與電氣的連接於放大器２４１之電阻形成積分電路而出現電壓值，此電壓值乃被類比・數值變換而被數值化。

如上述由於容量２３１之值係隨機值，因此將所出現之電壓值以及將此電壓值予以類比／數值變換而獲得之數值也隨機值。再者，此容量值乃由疊層而成之半導體晶片與基板之縱向構造（疊層構造）所決定者，因此如由第三者之ＩＣ卡之分解等而破壞此縱向構造或予以剝離時，當然不可能再現容量值也。

＜實施例６＞

圖１７乃以利用本發明之ＩＣ卡之，以ＩＣ卡來實施商品之購買或清算（付款）之系統之概念圖。在ＩＣ卡２５１之內配置有半導體晶片，在此半導體晶片內形成有姓名區域及鍵碼。

首先以讀取・寫入器２５２向ＩＣ卡２５１詢問所有者之姓名（步驟（１）），對於此詢問ＩＣ卡２５１即向讀取・寫入器２５２回答姓名Ａ（步驟（２））。此姓名Ａ乃由讀取・寫入器２５２送到資料庫２５３詢問該鍵碼。

接著讀取・寫入器２５２即使用隨機數而產生公開鍵

五、發明說明（27）

碼，將此公開鍵碼送至ＩＣ卡２５１（步驟（３））。

ＩＣ卡２５２即將依本發明所實現之隨機數值（將隨機之容量值予以數值化者）依照上述公開鍵碼之算式予以密碼化，將密碼化之鍵碼回答於讀取・寫入器２５２（步驟（４））。讀取・寫入器２５２乃解讀上述被密碼化之鍵碼而與資料庫２５３之鍵碼Ｂ實施對照校對，如果相一致即認定爲正當之ＩＣ卡。

由於鍵碼乃依照隨機之容量值之數值化者而定，並且使用隨機數而將所發生之公開鍵碼之算式而予以密碼化，因此沒有由第三者來僞造或變造之可能性。

資料庫２５３之鍵碼Ｂ乃預先讀取ＩＣ卡２５１之鍵碼之數值而予以登錄存檔。再者，藉由線內監視器來被模擬之危險性即藉由隨機的產生公開鍵碼來得於防禦也。

＜實施例７＞

使用圖１８說明本發明之其他實施例。圖１８係表示不正當使用者之侵犯ＩＣ卡而欲電氣的讀出容量值時，容量之被破壞之狀態。爲了讀出容量值而於電極２１３、２１４之間施加０．１～１Ｖ程度之高電壓時，電介質膜２１１即被部份地破壞而發生短路２６１，而電極２１３、２１４即電氣的被短路。

如此時電極２１３、２１４之電位差乃幾乎相等，電極２１３、２１４間之電氣力線消滅，不會發生容量。所以容量之再現變爲不可能，由分解ＩＣ卡而被讀取鍵碼之

五、發明說明（28）

危險即消失。

本實施例乃顯示了電介質膜２１１之被破壞之例子，惟爲了防止ＩＣ卡之被分解而被解讀鍵碼起見，使電極２１３、２１４間變爲等價之等電位就可達成，所以例如可以在電極２１３、２１４之間設置適當之電路等而在電極２１３、２１４之間形成短路等方法亦可以。

＜實施例８＞

圖１９表示本發明之其他實施例之平面配置之圖。在ＩＣ卡之半導體晶片２７１之內，形成有由上述實施例１所形成之容量２７２。具有僞造ＩＣ卡之意圖人乃以探針探索半導體晶片２７１，對於容量元件或周邊之積分電路類比・數值變換器開始侵犯以資欲讀出鍵碼。此時ＬＳＩ侵犯感測電路測到有探針之接觸時，對於高電壓發生電路送訊號使之動作，於是在容量元件２７２之兩端被施加耐電壓以上之高電壓，於形成容量之電極內部或其周邊發生短路，構成電極之金屬材料乃被轉移。於是容量值之再現成爲不可能無法讀出鍵碼，破壞了半導體晶片也不可能檢出容量值，由而ＩＣ卡乃不會有被僞造或變造之虞。

＜實施例９＞

本實施例乃隨機的改變容量之電介質膜之厚度，形成容量值之隨機的分散之容量之例子，使用圖２０來說明。第２０圖（ａ）係本實施例之平面圖，第２０（ｂ）乃共

五、發明說明（29）

Ａ－Ａ´剖面圖。第１之電極２８１與第２電極２８２乃分別與第３電極２２３對向地被配置。第１電極２８１與第３電極２２３之間介置有薄電介質膜２８３，而第２電極２８２與第３電極２２３之間即介置較上述電介質膜２８３爲厚之電介質膜２８４。

電介質膜２８３、２８４之電介率乃相等，而厚度互相不相同，因此第１電極２８１與第３電極２２３之容量值，及第２電極２８２與第３電極２２３間之容量值即互相不相同。

本實施例乃藉由雷射加工使各電介質膜之厚度隨機的分散狀的予以製造，其結果各容量地容量值均不相同，容量值乃隨機的分散。

再者，在本實施例中，各電極２８１、２８２、２２３乃只要在這之電極間可以形成容量之條件下，材質、形狀、以及尺寸等並不特別地予以限定。

（發明之利用可能性）

依本發明可以經濟的提供對於ＩＣ卡之僞造、變造有效的防禦之方法。於ＩＣ晶片及基板側分別具有表面備有不定形之凹凸之電極，將ＩＣ晶片以倒裝法使各電極與電極予以連接，將其連接阻抗（電阻）施予類比／數值變換做爲鍵碼。通常電極係備有複數個。而由於連接阻抗（電阻）將成爲隨機值，因無法實施複製。

再者，以對向地被配置之半導體晶片側之電極、與基

五、發明說明（30）

板側之電極間之電介質膜之材料、厚度或形狀等予以變更，將其容量值予以A／D（類比／數值）變換。而做爲鍵碼，由而容量值將成爲隨機的分散之值。再將它密碼化而做成鍵碼而使用，因此不可能僞造或變造。

再者，如對ＩＣ卡予以分解或實施電氣的測定即破壞該容量而不能再現，因此不可能僞造、變造也。

圖式之簡單說明

第１圖乃表示本發明之第１之實施例之剖面圖。

第２圖乃表示本發明之第１之實施例之平面圖。

第３圖乃表示本發明之第１之實施例之圖。

第４圖乃表示本發明之第１之實施例之立圖。

第５圖乃表示本發明之第１之實施例之剖面圖。

第６圖乃表示本發明之第１之實施例之平面圖及剖面圖。

第７圖乃表示本發明之第１之實施例之圖。

第８圖乃表示本發明之第１之實施例之圖。

第９圖乃表示本發明之第１之實施例之圖。

第１０圖乃表示本發明之第１之實施例之圖。

第１１圖乃表示本發明之第１之實施例之圖。

第１２圖乃表示本發明之實施例之圖。

第１３圖乃表示本發明之第２實施例之圖。

第１４圖乃表示本發明之第３實施例之平面及剖面構造之圖。

五、發明說明 (31)

第１５圖乃表示本發明之第４實施例之平面及剖面構造之圖。

第１６圖乃表示本發明之第５實施例之圖。

第１７圖乃表示本發明之第６實施例之圖。

第１８圖乃表示本發明之第７實施例之剖面圖。

第１９圖乃表示本發明之第８實施例之圖。

第２０圖乃表示本發明之第９實施例之平面及剖面造圖。

〔元件符號之說明〕

１１，１０３，１１１　ＩＣ晶片

１２，６５，２１３　晶片電極

１３，２１４　基板電極　１４，２１５　基板

２１，９１，９４，１０２，１１３，２５１　ＩＣ卡

２２　ＩＣ晶片載置部　２３　存儲區域

２４，６１，９２，９５　ＩＣ晶片

２５　電極載置部　２６　電極

２７　導電微粒子　３１　電流源

３２　電阻　３３，２４２　放大器

３４　變換器　３５　輸出端子

６２　薄片　６３　薄片電極

９３，９６，１０５　鍵碼產生部

１０１，２５２　讀取・寫入器

１０４　姓名碼或認識碼　１０６，１０９　鍵碼

五、發明說明 (32)

107，253　資料庫

212，271　半導體晶片

211　電介質膜

213，214　電極

223，224　粒子

241，272　容量元件

四、中文發明摘要（發明之名稱：半導體裝置）

本發明係提供一種防止處理重要之資料之ＩＣ卡等之僞造變造之有效手段爲目的者。

於ＩＣ晶片側及基板側分別備有表面具有不定形之凹凸之電極１２、１３，以倒裝法ＩＣ晶片１１以資連接各別之電極之間，而將其連接阻抗之値予以Ａ／Ｄ變換用做鍵碼，將連接阻抗成爲隨機値，而使用於密碼之鍵碼，即可以達成無法複製之目的。

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

1．一種半導體裝置，具備有：備有第1之電極之IC晶片，及，對向於上述第1之電極地設置，備有電氣的連接於上述第1電極之第2電極之基板，以及依據上述第1與第2電極之連接阻抗之類比／數值變換之資料所作成之鍵碼而構成爲其特徵者。

2．一種半導體裝置，具備有：備有第1之電極之IC晶片，以及對向於上述第1之電極地設置，備有使用導電性接著材而電氣的連接於上述第1電極之第2電極之基板，以及依據上述第1與第2電極之連接阻抗之類比／數值變換之資料所作成之碼而構成爲其特徵者。

3．一種半導體裝置，具備有：備有第1之電極之IC晶片，及對向於上述第1電極而設，備有使用含有導電微粒子之異方導電性接著材而電氣的連接於上述第1之電極之第2電極之基板，以及依據上述第1與第2電極之連接阻抗之類比／數值之值變換之資料而成之碼而構成爲其特徵者。

4．如申請專利範圍第3項所述之半導體裝置，其中上述第1及第2電極之材料與上述導電微粒子之材料之主成份係相同者。

5．一種半導體裝置，具備有：備有在表面備有不定形之凹凸之第1之電極之IC晶片，及對向於上述第1電極而設，備有電氣的連接於第1電極之第2電極之片片狀基板，以及依據上述第1、第2電極之連接阻抗之值所作成之鍵碼而構成者。

六、申請專利範圍

6．如申請專利範圍第1項所述之半導體裝置，其中上述鍵碼乃將上述經類比／數值變換之資料而予以密碼處理、寫入於上述ＩＣ晶片之存儲區者。

7．如申請專利範圍第1項所述之半導體裝置，其中上述鍵碼乃將上述經類比／數值變換之資料而經ＩＣ晶片內之第1密碼處理及在上述ＩＣ卡外之第2之密碼處理，而後寫入於上述ＩＣ晶片之存儲區者。

8．如申請專利範圍第1項所述之半導體裝置，其中上述鍵碼乃由上述ＩＣ卡用之讀取寫入器所讀取，而與上述ＩＣ卡之登錄碼一齊，保存於設於連接於上述讀取寫入器之服務程序內之資料庫內者。

9．如申請專利範圍第1項所述之半導體裝置，其中上述鍵碼乃使用於防止上述ＩＣ卡之僞造及變造者。

10．如申請專利範圍第1項所述之半導體裝置，其中

上述鍵碼乃使用於上述ＩＣ卡與上述ＩＣ卡實施資料之互相變換之讀取寫入器之間之互相校對之用者。

11．如申請專利範圍第1項所述之半導體裝置，其中

上述鍵碼係，與密碼或生物的特徵碼併用之後，使用於校對是否本人之用。

12．如申請專利範圍第11項所述之半導體裝置，其中

上述生物的特徵碼係由，掌紋碼、指紋碼、嗅感碼、

六、申請專利範圍

臉碼、聲音碼、靜脈碼、瞳孔碼、ＤＮＡ碼中所選擇之至少其中之一所成者。

１３．如申請專利範圍第6項所述之半導體裝置，其中

以控制讀取寫入器之上位之系統來實施，使用於上述鍵碼之讀出之公開鍵密碼之解讀或使用於上述鍵碼之存儲寫入之共同鍵密碼之解讀者。

１４．如申請專利範圍第１項所述之半導體裝置，其中

上述鍵碼乃使用於，當上述ＩＣ卡之使用於電子貨幣時之校對是否本人或僞造之校驗，上述ＩＣ卡與讀取寫入之互相校對者。

１５．如申請專利範圍第１項所述之半導體裝置，其中

上述類比／數值變換之分解能係２～４階段者。

１６．如申請專利範圍第１項所述之半導體裝置，其中

上述第１與第２之電極之連接部份之尺寸爲１５微米（micron）以下。

１７．如申請專利範圍第１項所述之半導體裝置，其中

上述ＩＣ晶片內矩陣狀地排列有複數之電極狀。

１８．如申請專利範圍第１項所述之半導體裝置，其中

六、申請專利範圍

上述鍵碼乃使用於爲鑑別同時地回應之其他複數之ＩＣ卡者。

１９．如申請專利範圍第１項所述之半導體裝置，其中

上述第１或第２之電極之至少一方乃該表面具有不定形之凹凸者。

２０．如申請專利範圍第１項所述之半導體裝置，其中

上述第１及第２之電極乃分別由複數之小墊之陣列所成者。

２１．如申請專利範圍第１項所述之半導體裝置，其中

當上述類比／數值之變換時，上述連接阻抗之類比值乃備有迴避據位於該位切換部份之境界領域者之手段者。

２２．一種碼製成方法，具備有：求出設於ＩＣ晶片之第１電極與設於與上述ＩＣ晶片不同之基板上之第２電極之連接阻抗之過程，及

依據上述連接阻抗之值來製作資料碼之過程，及

將上述資料碼予以密碼處理之過程，及

將上述被密碼處理之上述資料碼存儲於上述ＩＣ晶片之過程而構成爲其特徵者。

２３．如申請專利範圍第２２項所述之碼製成方法，其中

上述密碼處理係在ＩＣ晶片之外部來實施者。

六、申請專利範圍

２４．如申請專利範圍第２２項所述之碼製成方法，其中

上述密碼處理乃包含在上述ＩＣ晶片之內部實施之第１密碼處理及在上述ＩＣ晶片之外部實施之第２密碼處理者。

２５．一種校對方法，具備有：讀取，依據連接設於ＩＣ晶片之電極與設於基板上之連接於上述電極之電極之連接阻抗之資料之過程，及

讀取存儲於上述ＩＣ晶片之碼之過程，及

校對上述資料與上述碼之過程，爲其特徵者。

２６．如申請專利範圍第２５項所述之校對方法，其中

上述資料乃上述連接阻抗乃被類比／數値變換，公開鍵密碼處理之後，再以共同鍵密碼方式而予以密碼化者。

２７．如申請專利範圍第２６項所述之校對方法，其中

上述公開鍵密碼處理係在上述ＩＣ晶片內而實施者。

２８．如申請專利範圍第２６項所述之校對方法，其中

上述共同密碼方式中之密碼化乃在上述ＩＣ卡用之讀取寫入器內實施者。

２９．如申請專利範圍第２５項或２６、２７、２８項所述之校對方法，其中

上述校對乃以確認上述ＩＣ卡是否僞造爲目的者。

六、申請專利範圍

３０．一種校對方法，具備有：

求出依據設於半導體裝置之第１之電極與第２之電極之連接阻抗之第１資料之過程，及

由資料庫獲得爲特定之上述半導體裝置而存儲之第２資料之過程，及

校對上述第１資料與上述第２資料之過程而構成爲其特徵者。

３１．如申請專利範圍第３０項所述之校對方法，其中

上述第１資料乃上述連接阻抗之被類比／數值變換公開鍵密碼處理之後予以解讀者。

３２．如申請專利範圍第３０項或第３１項所述之校對方法，其中

上述校對乃爲了實施上述半導體裝置之認證之用者。

３３．一種校對方法，具備有：

求出設於半導體裝置之第１之電極與第２電極之連接阻抗之過程，及以上述連接阻抗予以類比／數值變換之資料而將隨機數予以密碼處理求出第１之資料之過程，及

由資料庫讀取爲特定上述半導體裝置而儲存之資料之過程，及以存儲於上述資料庫之資料而對上述隨機數相同之隨機數予以密碼處理而獲得第２資料之過程，以及校對上述第１資料與上述第２資料之過程而構成爲其特徵者。

３４．如申請專利範圍第３３項所述之校對方法，其中

六、申請專利範圍

上述校對乃爲了實施上述半導體裝置之認證之用者。

３５．一種ＩＣ卡，具有：互相對向地配置之基板及半導體晶片，及分別互相對向且離開的配置於該基板及半導體晶片之互相對向之側之表面上之電極，

將形成於上述電極間之容量之容量值之予以數值化者使用於ＩＣ卡之鍵碼爲其特徵者。

３６．如申請專利範圍第３５項所述之ＩＣ卡，其中於上述半導體晶片上形成上放大器，以分別連接於該放大器之上述容量及規定之電阻而形成了積分電路，上述容量值之數值乃將由上述積分電路而出現之電壓值之被類比・數值變換來實施者。

３７．如申請專利範圍第３５項或３６項所述之ＩＣ卡，其中

於上述基板及半導體晶片之上分別形成有複數之上述電極，形成於互相對向且離開地被配置於上述電極之間之容量乃該容量值係隨機的不同者。

３８．如申請專利範圍第３７項所述之ＩＣ卡，其中於上述互相對向且離開而配置之電極之間，介置有由不同之種類之電介質所成之電介質膜者。

３９．如申請專利範圍第３７項所述之ＩＣ卡，其中於上述互相對向且離開而配置之電極之間，介置有由相同種類之電介質所成厚度互相不同之電介質膜者。

４０．如申請專利範圍第３７項所述之ＩＣ卡，其中上述互相對向且離開而配置之電極之間之距離乃互相

六、申請專利範圍

不同者。

41．如申請專利範圍第40項所述之ＩＣ卡，其中上述互相對向且離開地被配置之電極之厚度乃至互相不同者。

42．如申請專利範圍第37項所述之ＩＣ卡，其中於上述互相對向且離開的予以配置之上述電極之間，介置有直徑之互相不同，且同一種類之粒子狀之電介質者。

43．如申請專利範圍第35或36～42項其中之一項所述之ＩＣ卡，其中上述電介質膜乃由，$BaSrTiO_3$膜、ＰＳＴ膜、$CaTiO_3$膜及KH_2PO_4膜所成之群中所選用者。

44．一種ＩＣ卡之正否鑑別方法，對於具有形成姓名區域及鍵碼之半導體晶片之ＩＣ卡，詢問該ＩＣ卡之所有者之姓名，依據來自上述ＩＣ卡之回答而對資料庫送上述姓名而詢問該鍵碼，再對上述ＩＣ卡送出使用隨機數所發生之公開鍵碼，解讀由上述ＩＣ卡之密碼化之回答，對比上述資料庫之鍵碼，由而鑑定上述ＩＣ卡之正否爲其特徵者。

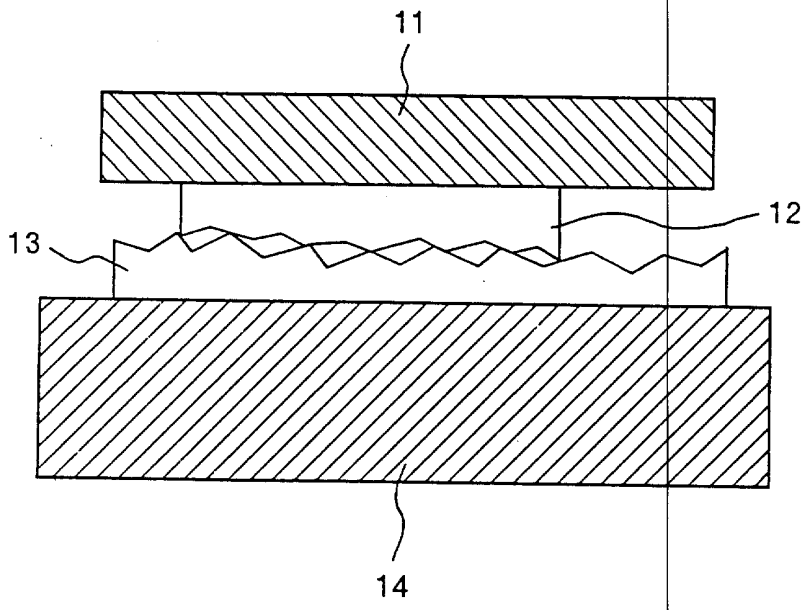
45．如申請專利範圍第44項所述之ＩＣ卡之正否鑑別方法，其中上述資料庫中預先登錄有上述ＩＣ卡之鍵碼者。

（請先閱讀背面之注意事項再填寫本頁）

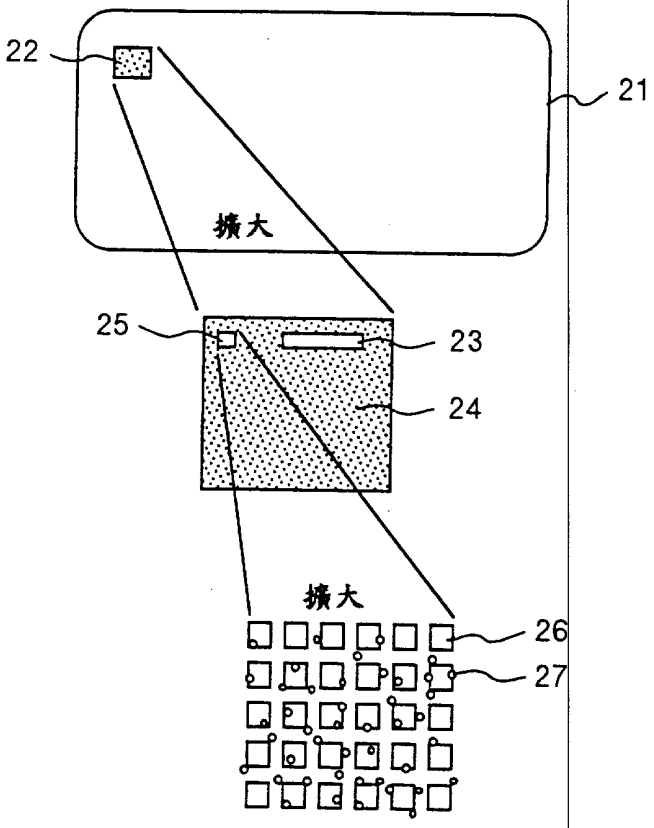
訂

衣

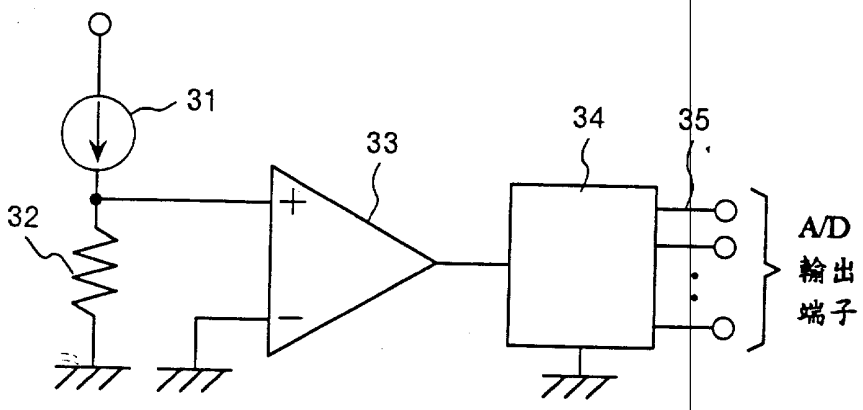
731919



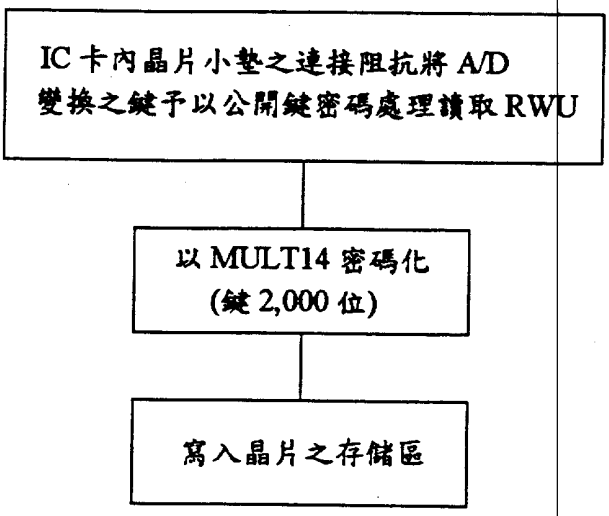
第1圖



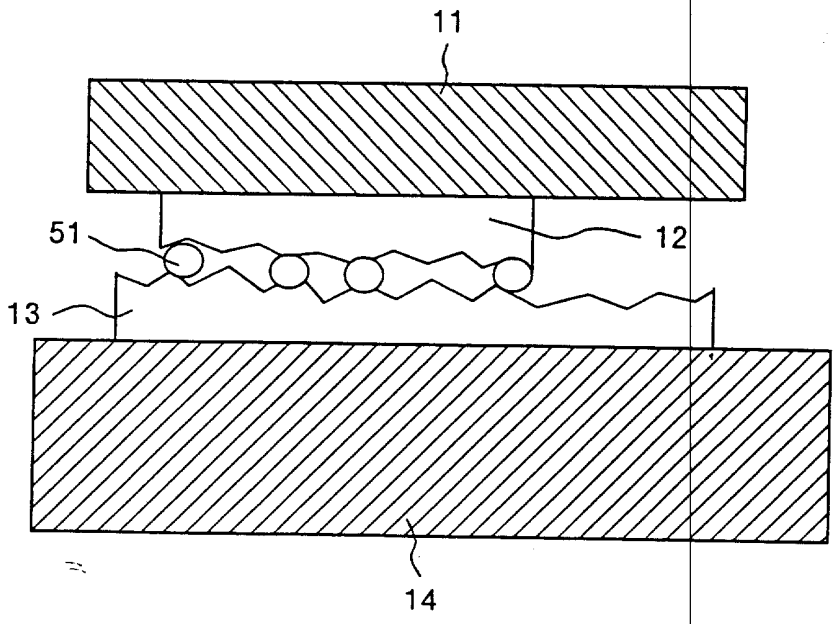
第 2 圖



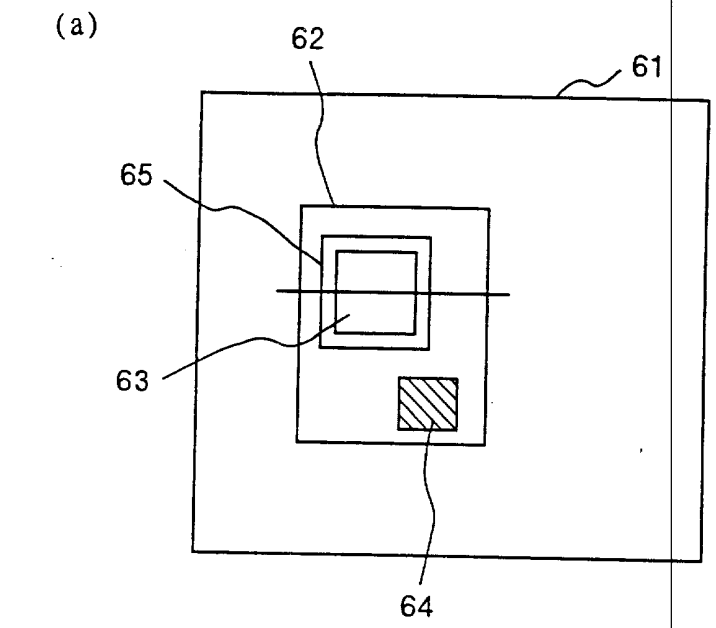
第 3 圖

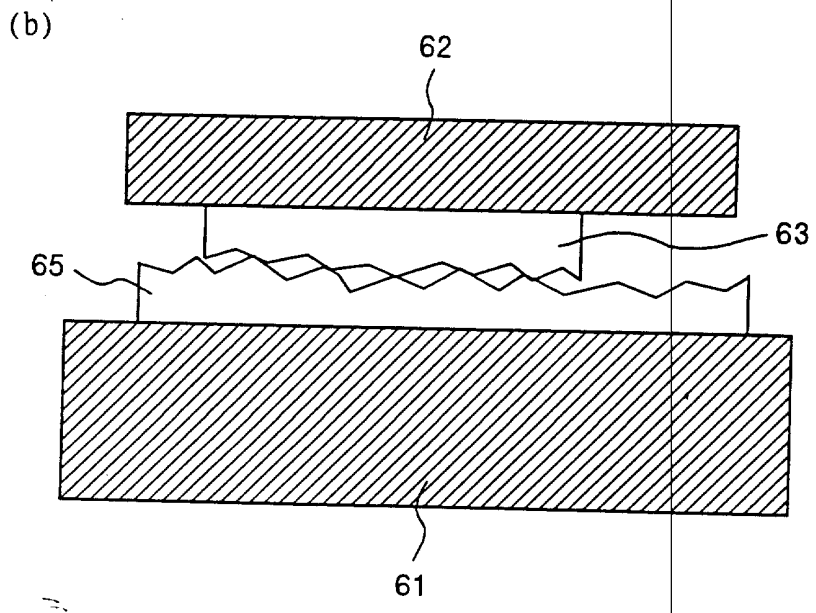

IC卡內晶片小墊之連接阻抗將A/D
變換之鍵予以公開鍵密碼處理讀取RWU
以MULT14密碼化
(鍵2,000位)
寫入晶片之存儲區

第4圖

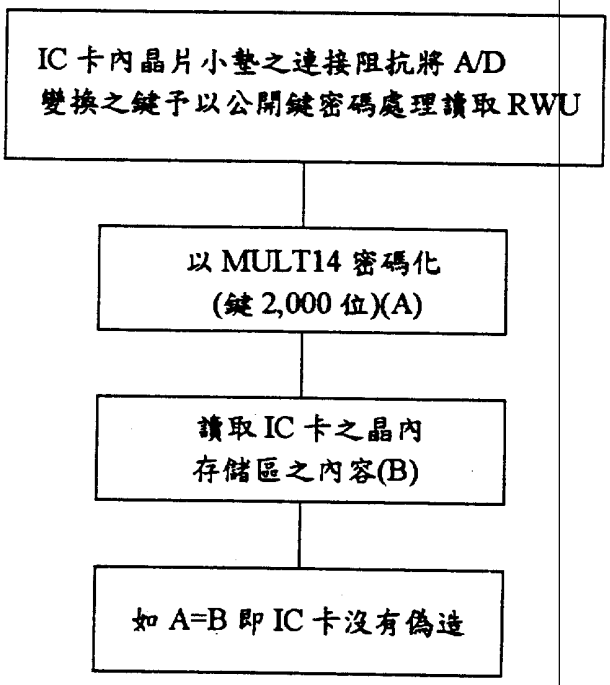

11
51
12
13
14

第5圖



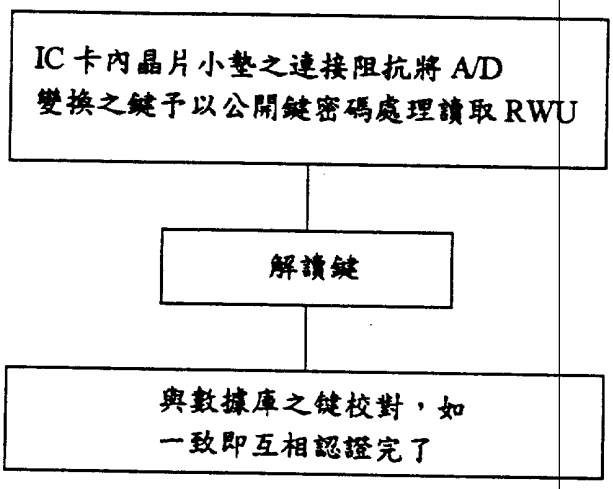


第 6 圖

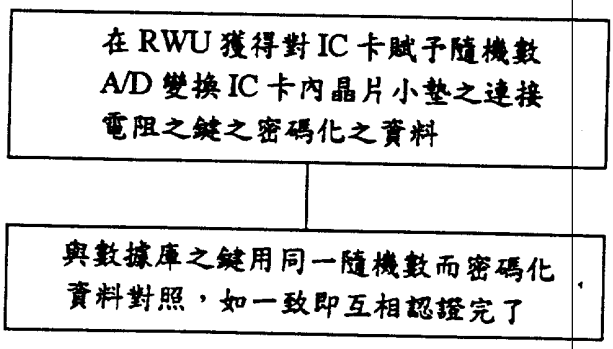

IC 卡內晶片小墊之連接阻抗將 A/D
變換之鍵予以公開鍵密碼處理讀取 RWU
以 MULT14 密碼化
(鍵 2,000 位)(A)
讀取 IC 卡之晶內
存儲區之內容(B)
如 A=B 即 IC 卡沒有偽造

第 7 圖

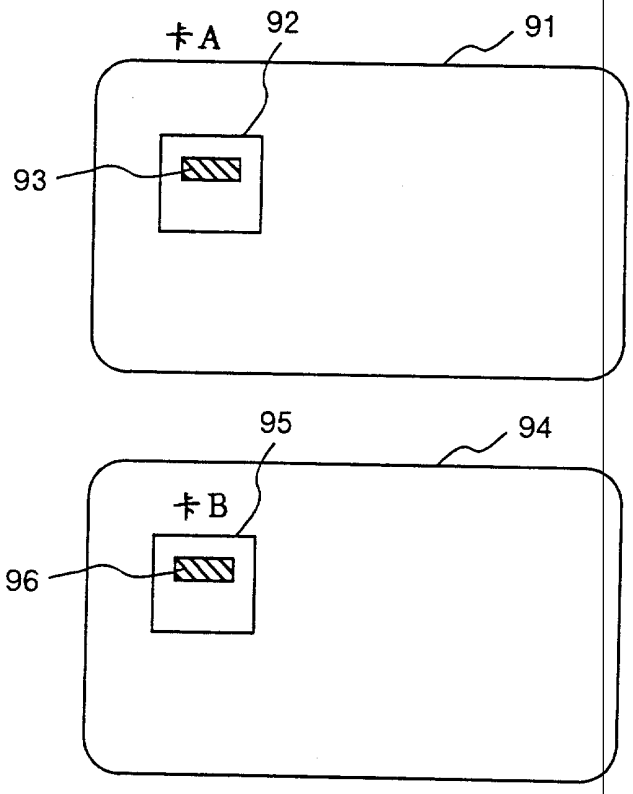
(a)


IC卡內晶片小墊之連接阻抗將A/D
變換之鍵予以公開鍵密碼處理讀取RWU
解讀鍵
與數據庫之鍵校對，如
一致即互相認證完了

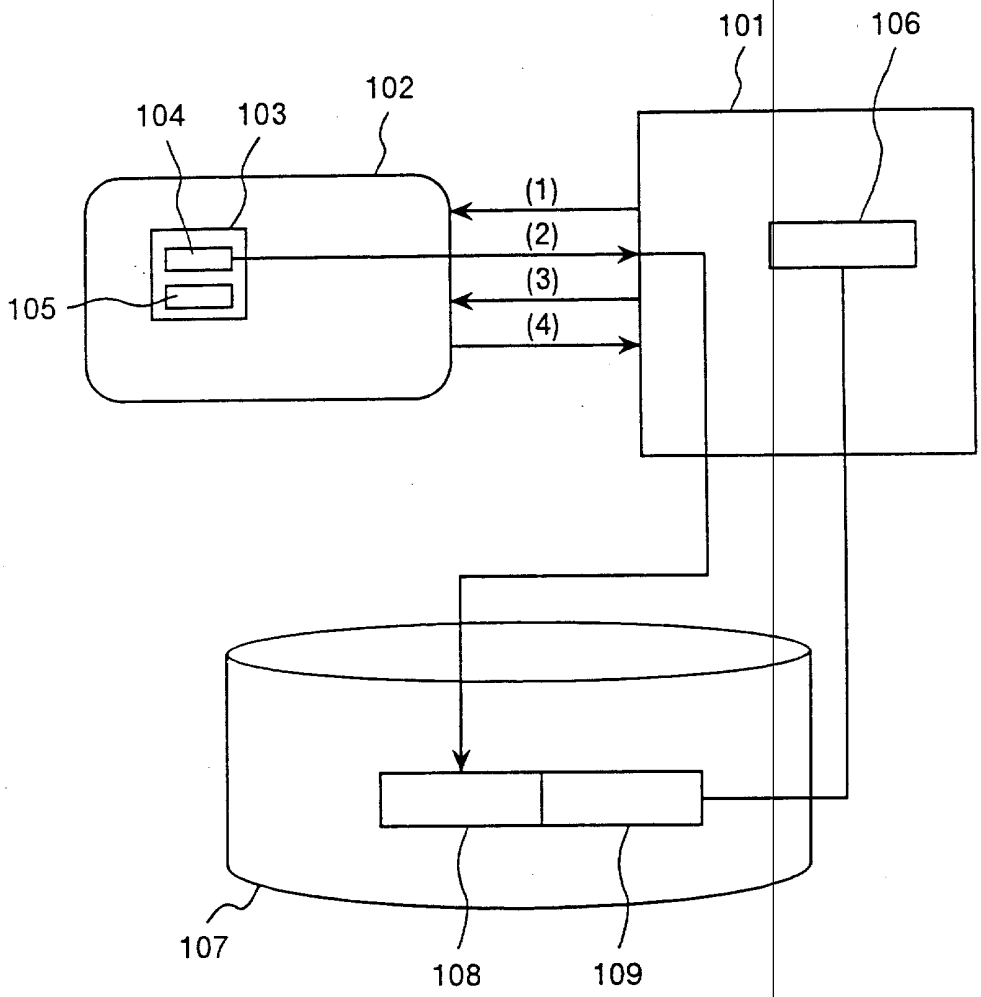
(b)


在RWU獲得對IC卡賦予隨機數
A/D變換IC卡內晶片小墊之連接
電阻之鍵之密碼化之資料
與數據庫之鍵用同一隨機數而密碼化
資料對照，如一致即互相認證完了

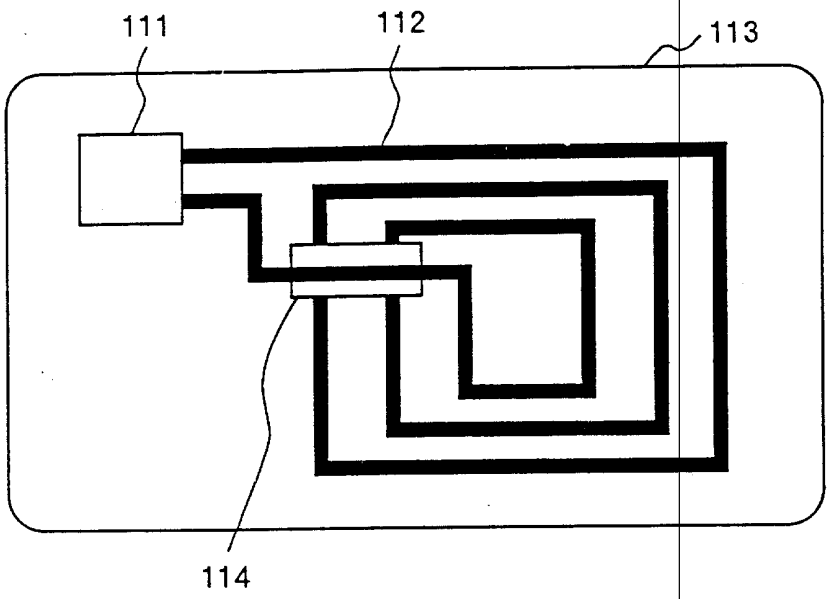
第8圖



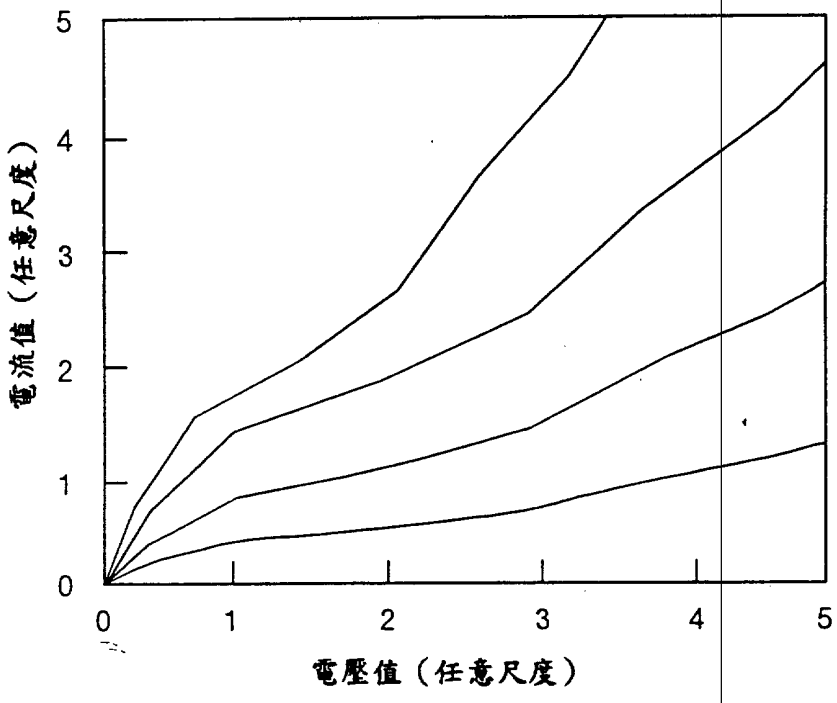
第 9 圖



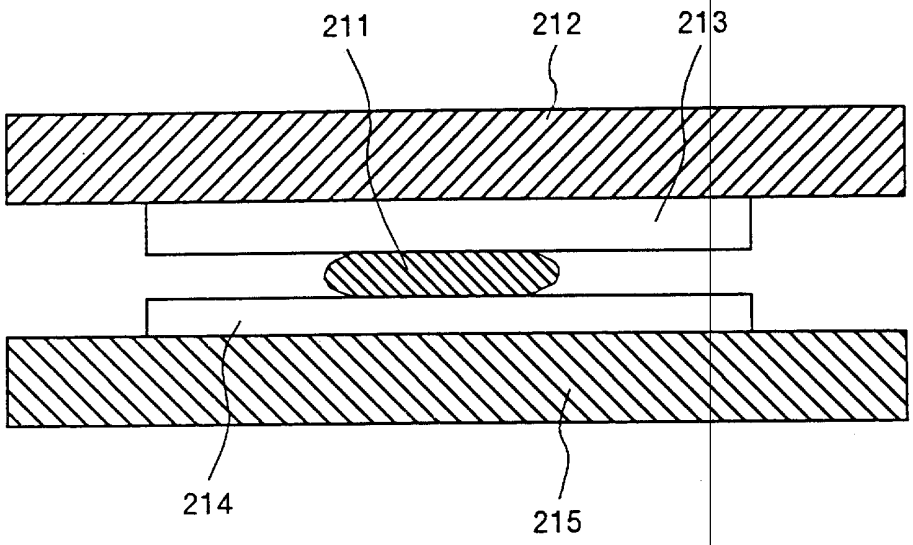
第10圖



第11圖

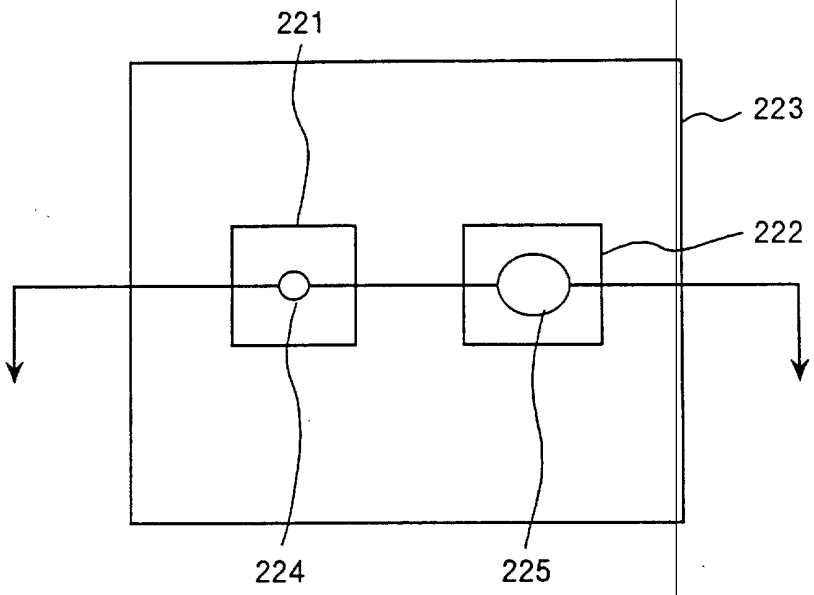


第12圖

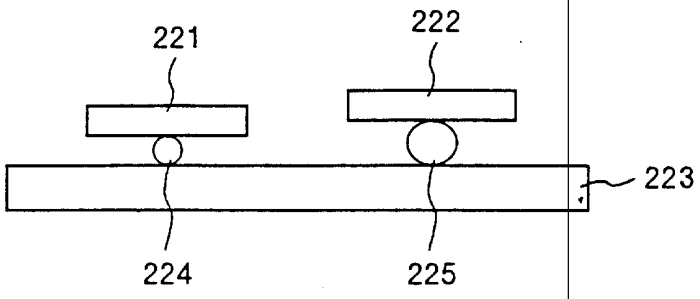


第13圖

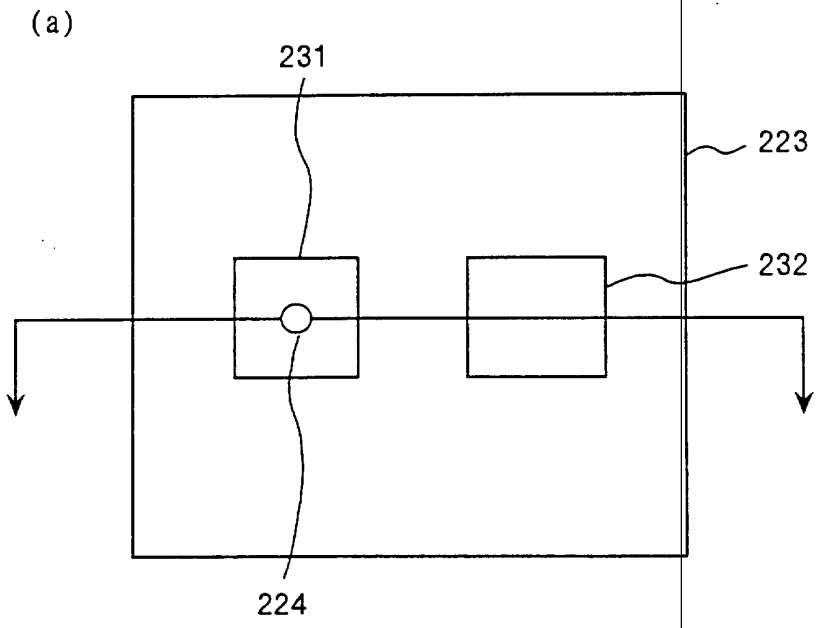
(a)



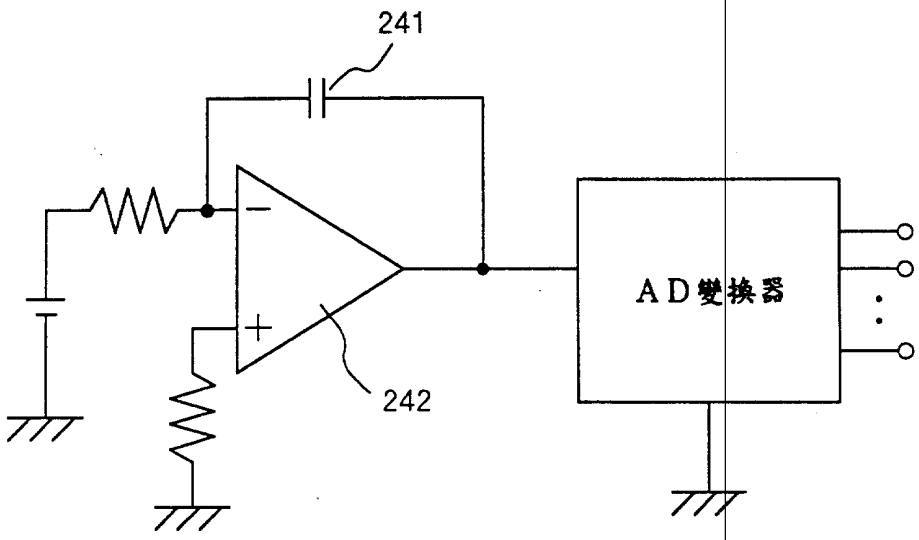
(b)



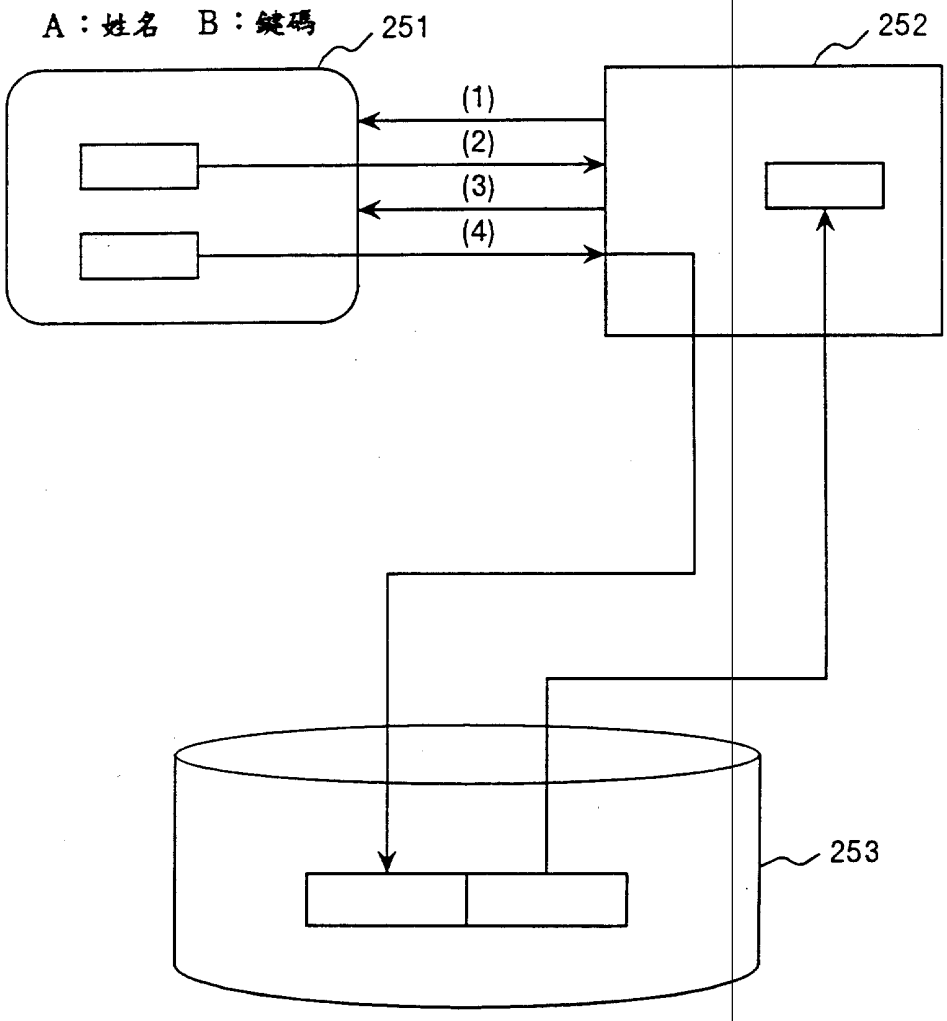
第14圖



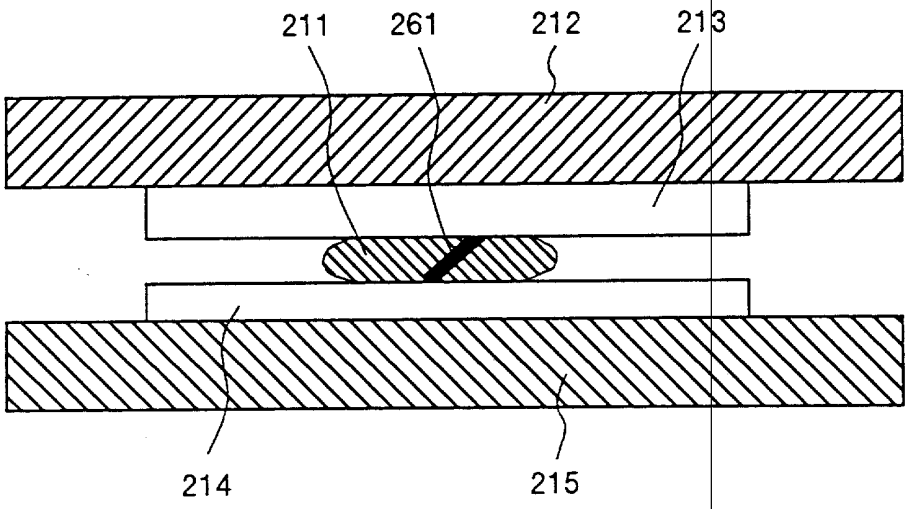
第15圖



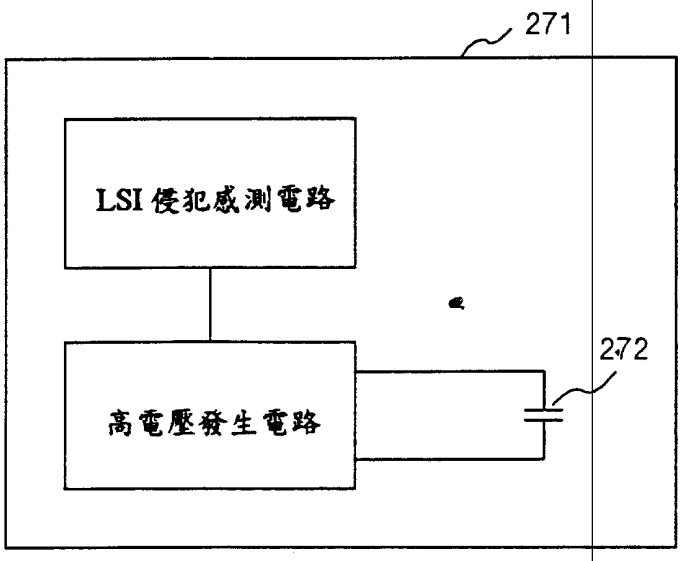
第16圖



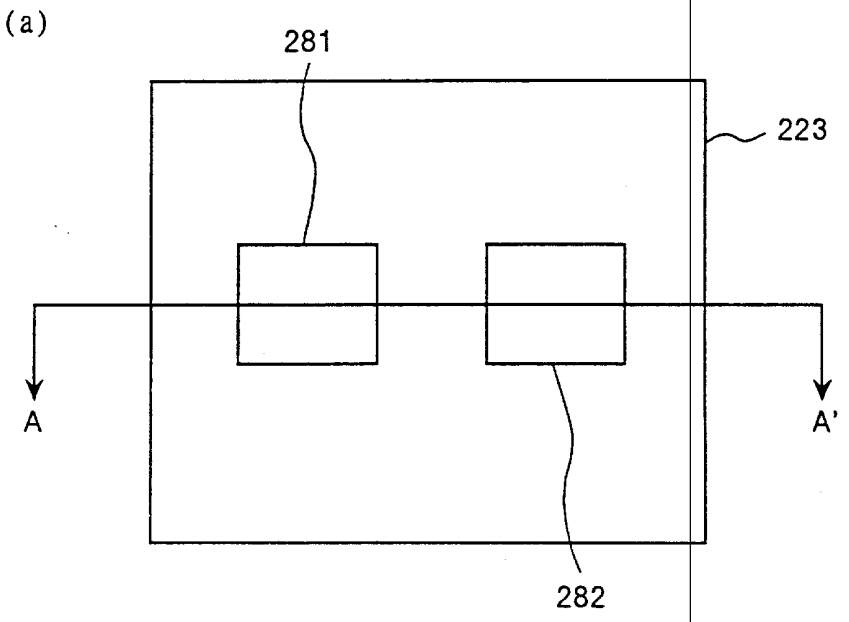
第17圖

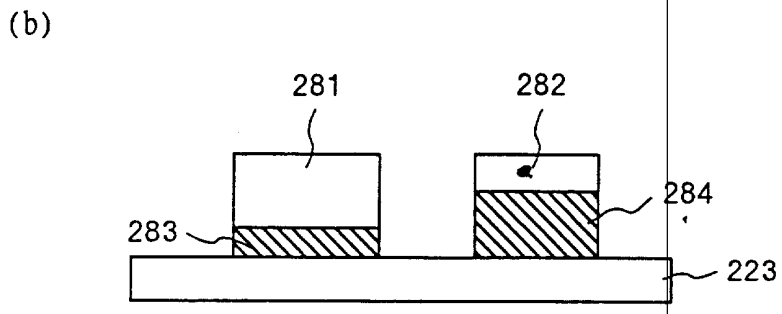


第18圖



第19圖





第20圖