【發明說明書】

【中文發明名稱】　產生識別金鑰之裝置及方法

【英文發明名稱】　APPARATUS AND METHOD FOR GENERATING IDENTIFICATION KEY

【技術領域】

【0001】本發明有關一數位安全領域，更特別地係，關於一種為了電子裝置的安全、嵌入式系統安全、單晶片系統(System on Chip，SoC)安全、智慧卡安全、通用用戶識別模組(Universal Subscriber Identity Module，USIM)安全等所需，而產生用於編碼與解碼方法、數位簽章等的識別金鑰之裝置及方法。

【先前技術】

【0002】隨著資料導向社會持續前步，個人隱私的保護的需求已逐漸增加。因此，本質需要利用資訊加密與解密，以建構安全資訊傳輸的安全系統技術，而且是重要的技術。

【0003】在先進的資料導向社會中，隨著高效能電腦，使用嵌入式系統、或單晶片系統(SoC)形式的電腦裝置已快速增加。例如，諸如射頻識別(Radio-Frequency IDentification，RFID)、一智慧卡、一通用用戶識別模組(USIM)、一次性密碼(One-Time Password，OTP)等的電腦裝置已廣泛流行。

【0004】為了在電腦裝置建構安全系統，可使用供加密與解密演算法或獨特識別的加密金鑰。加密金鑰或獨特識別以下將稱為一識別金鑰。識別金鑰主要取決於可安全加密的外部產生虛擬隨機碼(Pseudo Random Number，PRN)的方法，且將虛擬隨機碼儲存在非揮發性記憶體，諸如快閃記憶體、電子抹除式可

編程唯讀記憶體(Electrically Erasable Erogrammable Read-Only Memory，EEPROM)等。

【0005】關於儲存在電腦裝置的識別金鑰，最近已發生諸如旁通道攻擊、逆向工程攻擊等的各種不同形態攻擊。要防止這類攻擊，物理不可複製函數(Physical Unclonable Function，PUF)技術已發展成為安全性產生及儲存識別金鑰之一方法。

【0006】PUF為供利用存在於電子系統的微妙實際特性差異以產生識別金鑰，及維持或儲存產生的識別金鑰之技術，識別金鑰在此亦稱為硬體指紋。

【0007】為了將PUF當作識別金鑰使用，首先，應有充份產生識別金鑰的隨機性；其次，產生的識別金鑰值應不受時間流或使用環境的變化而改變。

【0008】不過，傳統技術的問題係不容易獲得充份的隨機性，且由於根據時間流的實際特徵變化或由於使用環境變化，產生識別金鑰的改變，這些問題尚未解決。

【發明內容】

【0009】為了透過半導體製程產生一實際亂數值，然後發展一物理不可複製函數(PUF)技術，以提供一旦產生後不會隨時間變化的值，及將PUF技術當作識別金鑰使用，本發明之一態樣提供用於產生識別金鑰之裝置及方法。

【0010】本發明之一態樣亦提供用於產生識別金鑰之裝置與方法，其可概率保證數位值形式的識別金鑰的0數位值與1數位值間的平衡。

【0011】本發明之一態樣亦提供用於產生識別金鑰以組態PUF之一裝置與方法，識別金鑰能以相當低成本製造、簡單製造、實際無法複製的識別金鑰，因此不易受外部攻擊。

【0012】根據本發明之一態樣，提供一產生識別金鑰裝置，其藉由意欲違背在半導體製程期間提供的設計規則，概率性判斷在構成電路的節點間是否發生短路，以產生識別金鑰。

【0013】根據本發明之一態樣，提供用於產生識別金鑰之一裝置，其包括：一識別金鑰產生器，基於一接點或一穿孔(在半導體晶片中用來電連接傳導層)是否使傳導層短路，以產生一識別金鑰；及一識別金鑰讀取器，藉由讀取該接點或該穿孔是否使傳導層短路，以讀取該識別金鑰。

【0014】識別金鑰產生器可包括一電路，其包含一接點或一穿孔，其意欲設計上係等於或小於在半導體製程期間提供的設計規則所決定的尺寸。意欲設計上減少的接點或穿孔可概率性判斷在傳導層間是否短路。

【0015】在建立接點或穿孔是否使傳導層短路的判斷後，可產生具有根據時間流或根據使用環境不變特徵的判斷結果值。

【0016】識別產生器可設定接點尺寸或穿孔尺寸，以便接點或穿孔發生傳導層短路的機率、與接點或穿孔不發生傳導層短路的機率相等。在此，表示0的識別金鑰產生器所產生數位值的機率、與表示1的識別金鑰產生器所產生數位值的機率可同樣表示1/2，其中在以下，機率的1/2係相當於50%。

【0017】識別金鑰產生器可包括一電路，以利用單接點或單穿孔連接單獨一對傳導層以產生1位元數位值；且可利用N電路產生一N位元識別金鑰。

【0018】當構成由識別金鑰產生器所產生N位元識別金鑰的一數位值表示0的機率、與構成由識別金鑰產生器所產生N位元識別金鑰的一數位值表示1的機率不同，接近1/2時，可減少產生識別金鑰的隨機性。

【0019】根據本發明之一態樣，為了要確保產生識別金鑰的隨機性，可更包括用以處理識別金鑰之一識別金鑰處理單元。

【0020】一種用於產生識別金鑰之裝置可包括識別金鑰處理單元，以處理該識別金鑰，其係藉由：接收經由識別金鑰讀取器所讀取識別金鑰的輸入；基於k位元，將構成識別金鑰的數位值分群組、及產生複數個數位值群組；比較在複數個數位值群組中的第一群組與第二群組；及當第一群組中包括的一值(含有k數位位元)大於第二群組中包括的一值(含有k數位位元)，一數位值則決定為1，其中該數位值代表第一群組與第二群組。

【0021】理想地係，當產生0的機率與產生1的機率同樣表示1/2時，產生識別金鑰的隨機性可確保最大，不過，可能非常不容易實際達成。因此，當兩群組係以基於k 位元的分群組比較時，雖然產生0的機率與產生1的機率係不同同樣表示1/2，但是兩群組可在相等情況下，且因此第一群組具有比第二群組更大值的機率、與第一群組具有比第二群組更小值的機率可變成相等。

【0022】第一群組與第二群組可具有相等值，且在此範例中，代表第一群組與(或)第二群組的數位值可認為是1或0的任一者、或不決定。如此，在用於產生識別金鑰的裝置中，即使當產生0的機率與產生1的機率不同，同樣表示1/2，產生0的機率與產生1的機率最終可透過識別處理單元而相等，藉此可確保隨機性。

【0023】為了要在產生識別金鑰的裝置(包括識別金鑰處理單元)上產生一M位元識別金鑰，當基於k位元執行一群組時，可能需要產生M x k位元。不過，當第一群組與第二群組的值相等時，一代表值可不決定t次，如此一電路可組態成產生比M x k位元更足夠的位元數。

【0024】根據本發明之一態樣，提供用於產生一識別金鑰的裝置，該裝置包括：一識別金鑰產生器，其在半導體傳導層間具有一間隔，該識別金鑰產生器係基於半導體傳導層間是否發生短路，以產生一識別金鑰；及一識別金鑰讀

取器，其藉由讀取在傳導層間是否發生短路，以讀取識別金鑰，其中在半導體傳導層間的間隔可設定成一尺寸，其違背在半導體製程期間提供的設計規則。

【0025】識別金鑰產生器在半導體傳導層間可具有間隔，以在半導體傳導層間發生短路的機率、與在半導體傳導層間不會發生短路的機率之間具有差異，且在一預定誤差範圍內。

【0026】根據本發明之一態樣，亦提供產生一識別金鑰的方法，該方法包括：藉由意欲違背半導體製程期間提供的設計規則，概率性判斷在構成電路的節點間是否發生短路，以產生一識別金鑰；及藉 由讀取在構成電路的節點間是否發生短路，以讀取該識別金鑰。

【0027】根據本發明之一態樣，亦提供產生識別金鑰的方法，該方法包括：產生識別金鑰，其在半導體傳導層間具有一間隔，且基於在半導體傳導層間是否發生短路；及藉由讀取在傳導層間是否發生短路，以讀取識別金鑰，其中在半導體傳導層間的間隔係設定成一尺寸，其違背在半導體製程期間提供的設計規則。

【0028】發明效益

根據本發明的具體實施例，提供一裝置及一方法供產生高度可靠的識別金鑰，由於識別金鑰係透過半導體製程任意產生，且一旦產生識別金鑰值，就不會變化。

【0029】根據本發明的具體實施例，提供一裝置及一方法，供產生識別金鑰，其可概率保證數位值形式的識別金鑰中的數位值0與數位值1間的平衡，藉此可確保隨機性。

【0030】根據本發明的具體實施例，提供產生一裝置與一方法，以供產生能以相當低成本製造、簡單製造、實際無法複製的識別金鑰，因此不易受外部攻擊。

【圖式簡單說明】

【0031】本發明的這些及/或其他態樣、特徵與效益可從下列連同附圖的描述示範性具體實施例而變得更明白：

圖1為示例性說明供產生根據本發明之一具體實施例的識別金鑰裝置圖；

圖2為描述根據本發明之一具體實施例的識別金鑰產生器組態圖；

圖3為描述根據本發明之一具體實施例的識別金鑰產生器組態之曲線圖；

圖4為描述根據本發明之一具體實施例的識別金鑰產生器組態圖；

圖5為示例性說明藉由根據本發明之一具體實施例的識別金鑰產生器，以產生識別金鑰之接點陣列或穿孔陣列圖；

圖6為示例性說明利用本發明之一具體實施例的圖5之接點陣列與穿孔陣列，以產生識別金鑰的識別金鑰產生器組態圖；

圖7為描述藉由根據本發明之一具體實施例的識別金鑰處理單元，以處理該識別金鑰的製程圖；及

圖8為示例性說明根據本發明之一具體實施例的產生識別金鑰之方法圖。

【實施方式】

【0032】以下將參考本發明的示範性具體實施例，連同附圖的範例，其中相同參考數字表示類似元件。下面描述的示範性具體實施例將參考附圖解釋本發明。

【0033】圖1為示例性說明供根據本發明之一具體實施例以產生識別金鑰裝置(100)圖。

【0034】一識別金鑰產生器(110)可透過半導體製程產生一識別金鑰，其不會隨時間流變化，且該識別金鑰可任意產生，不過，不會隨時間流變化。

【0035】識別金鑰產生器(110)產生的識別金鑰可對應例如一N位元數位值，其中N是自然數。

【0036】產生可靠識別金鑰的最重要因素可為產生識別金鑰的隨機性、與不會隨時間流變化的識別金鑰不變性。

【0037】識別金鑰產生器(110)可組態成具有在半導體製程產生的節點間是否發生短路的隨機性，且在節點間是否發生短路不會隨時間流或使用環境而變化，因此一旦，產生識別金鑰不會變化。

【0038】識別金鑰產生器(110)可基於傳導層(例如金屬層)是否由在半導體製程期間產生的傳導層間形成的一接點或一穿孔發生短路，以產生識別金鑰。

【0039】接點或穿孔可設計成連接傳導層，且接點尺寸或穿孔尺寸可普遍決定傳導層間是否短路。一普通的設計規則可決定最小的接點或穿孔的尺寸，以保證在傳導層間的短路。

【0040】不過，在根據本發明之一具體實施例的識別金鑰產生器(110)組態中，接點的尺寸或穿孔的尺寸可決定為小於設計規則決定的尺寸，藉使接點的部份或穿孔的部份可使傳導層短路，且接點的另一部份或穿孔的另一部份可不使傳導層短路。在此，可概率性判斷是否發生短路。

【0041】在一傳統半導體製程中，當一接點或一穿孔未使傳導層短路，該製程便認為失敗，不過，可用於產生具有亂數的識別金鑰。

【0042】設定根據上述具體實施例的接點尺寸或穿孔尺寸將參考圖2與圖3深入描述。

【0043】根據本發明的另一具體實施例，在半導體製程期間，藉由概率性判斷是否在傳導線路間發生短路、藉由意欲決定在傳導線路間的間隔是否小於設計規則所決定的尺寸，識別金鑰產生器(110)可產生具有隨機性的一識別金鑰。

【0044】上述具體實施例可用來在傳統半導體製程期間，藉由意欲違背設計規則以產生一任意識別金鑰，其可保證傳導線路間的空隙，即是大於一預定程度的間隔。

【0045】在傳導線路間的間隔設定係參可圖4深入描述。

【0046】識別金鑰產生器(110)可電產生根據上述本發明具體實施例的產生識別金鑰。一接點或一穿孔是否在傳導層發生短路、或在傳導線路間是否發生短路可利用一讀取電晶體加以識別，其組態將參考圖6深入描述。

【0047】在使用接點或穿孔尺寸調整的具體實施例中，即使當藉由調整接點或穿孔的尺寸，使傳導層短路的接點或穿孔之比率、與不使傳導層短路的接點或穿孔之比率可調整成具有同樣機率等於1/2，在短路發生情況(例如，0數位值)與在相對情況(例如，1數位值)的整個相等比率可能概率式地不容易保證。

【0048】即是，當接點或穿孔的尺寸變成接近設計規則的決定值時，短路發生的機率會變成較高，相反地係，當接點或穿孔的尺寸變成小於設計規則的決定值時，短路不會發生的機率會變成較高。當短路發生的機率、與短路不發生的機率之任一者變成較高時，可減少產生識別金鑰的隨機性。

【0049】相同的問題可能發生在調整如上述傳導線路間的間隔的具體實施例中。

【0050】因此，用於產生識別金鑰的裝置(100)可更包括識別金鑰處理單元(130)，以處理該識別金鑰產生器(110)產生的識別金鑰，藉此增加亂數。

【0051】識別金鑰處理單元(130)的操作將參考圖7深入描述。

【0052】圖2為描述根據本發明之一具體實施例的識別金鑰組態圖。

【0053】在圖2，其示例性說明在半導體製程期間，在金屬(1)層(202)與金屬(2)層(201)間形成的穿孔組態。

【0054】在穿孔設定成如設計規則決定的足夠大尺寸的一群組(210)中，所有穿孔可使金屬(1)層(202)與金屬(2)層(201)短路，且是否發生短路可如0數位值所示。

【0055】在穿孔設定成小尺寸的一群組(230)中，所有穿孔不會使金屬(1)層(202)與金屬(2)層(201)短路。在此，是否發生短路能以1數位值表示。

【0056】在穿孔設定成在群組(210)尺寸與群組(230)尺寸之間的中間尺寸的一群組(220)中，穿孔的一部分可使金屬(1)層(202)與金屬(2)層(201)短路，且穿孔的另一部份不會使金屬(1)層(202)與金屬(2)層(201)短路。

【0057】類似群組(220)，識別金鑰產生器(110)可藉由設定穿孔的尺寸加以組態，以便穿孔的部份可使金屬(1)層(202)與金屬(2)層(201)短路，且穿孔的另一部份不會使金屬(1)層(202)與金屬(2)層(201)短路。

【0058】有關穿孔尺寸的設計規則可能不同，此取決於半導體製程。例如，當在0.18μ m(微米)的互補金屬氧化半導體(Complementary Metal-Oxide-Semiconductor，CMOS)製程期間，穿孔的設計規則設定成0.25μ m(微米)，識別金鑰產生器(110)可將穿孔的尺寸設定為0.19μ m(微米)，藉此促使概率性判斷金屬層間是否發生短路。

【0059】有關是否發生短路機率分佈的短路發生之理想機率可表示50%機率。識別金鑰產生器(110)可藉由將穿孔的尺寸設定成儘可能接近50%的機率分佈而加以組態。在設定穿孔的尺寸中，穿孔的尺寸可藉由基於製程的實驗加以決定。

【0060】圖3為描述根據本發明之一具體實施例的識別金鑰產生器組態之曲線圖。

【0061】如曲線圖所示，當穿孔的尺寸變得愈大，在金屬層間發生短路機率可能接近1。設計規則決定的穿孔尺寸可能符合Sd，其為足以在金屬層間產生短路的值。

【0062】Sm可為是否在金屬層間發生短路機率理論上符合0.5的穿孔尺寸。基於製程，Sm可具有不同值，且一類似值可經由實驗發現，不過，正確的Sm可能不容易發現。

【0063】在識別金鑰產生器(110)中，基於一特定的實驗，在金屬層間是否發生短路可設定成0.5，在具有預定允許誤差的Sx1(未在圖顯示)與Sx2(未在圖顯示)的範圍內。在此，Sx1與 Sx2可能接近顯示的Sx，且可符合具有預定邊際的大小。

【0064】圖4為描述根據本發明之一具體實施例的識別金鑰產生器組態圖。

【0065】根據本發明的另一具體實施例，藉由調整在金屬線路間的間隔，可概率性判斷是否在金屬線路間發生短路。

【0066】在金屬線路間的間隔設定太窄無法避免金屬線路間短路的一群組(410)中，短路可能發生在所有情況的金屬線路間。

【0067】在金屬線路間的間隔設定成非常大的一群組(430)中，短路不可能發生在所有情況的金屬線路間。

【0068】類似一群組(420)，識別金鑰產生器(110)可設定在金屬線路間概率性發生短路的間隔，以便金屬線路的部份可短路，且金屬線的另一部份不會短路。

【0069】圖5為示例性說明可在半導體層上形成的接點陣列或穿孔陣列，以藉由根據本發明之一具體實施例的識別金鑰產生器(110)產生識別金鑰的圖。

【0070】在圖5，其示例性說明在半導體基體上分層的金屬層間所形成的穿孔組態，該穿孔包括寬度M穿孔(或水平排列)與長度N穿孔(或垂直排列)，即是，整個N x M穿孔，其中M與N是自然數。

【0071】識別金鑰產生器(110)可基於 N x M穿孔之每一者是否使金屬層短路(0數位值)、或不使金屬層短路(1數位值)，以產生一N x M位元識別金鑰。

【0072】識別金鑰讀取器(120)可讀取產生的N x M位元識別金鑰。

【0073】圖6為示例性說明根據本發明之一具體實施例的識別金鑰產生器(120)的電路組態圖。

【0074】識別金鑰產生器(120)可利用在參考電壓 VDD與接電間的一讀取電晶體加以識別。

【0075】在包括一下拉電路的圖6範例中，當識別金鑰產生器(110)中的分開穿孔使金屬層短路時，一輸出值可表示0，且當一分開的穿孔不使金屬層短路時，一輸出值表示1，藉使識別金鑰產生器(110)可產生一識別金鑰。有關下拉電路的描述顯然延伸到包括一上拉電路的組態範例，如此在此省略其詳細描述。

【0076】一識別金鑰可利用金屬線路間的短路，在具體實施例中同樣產生。

【0077】雖然圖6的識別金鑰產生器(120)組態的一示範性具體實施例已顯示及描述，但是本發明不應侷限於部分示範性具體實施例。

【0078】因此，在藉由決定識別金鑰產生器(110)的金屬層間或金屬線路間是否發生短路以產生一數位值的組態情況中，可進行各種不同修改與變化，不致悖離本發明的精神或範疇。

【0079】識別金鑰產生器(110)產生的識別金鑰可傳送及儲存在識別金鑰讀取器(120)。識別金鑰讀取器(120)相當於一暫存器或一正反器(未在圖顯示)，其可接收產生的識別金鑰的輸入，及可儲存產生的識別金鑰。

【0080】可讀取及儲存產生的識別金鑰之暫存器或正反器、以及類似暫存器或正反器的其他組態在以下係構成識別金鑰讀取器(120)，而不需任何進一步描述。

【0081】圖7為藉由根據本發明之一具體實施例的一識別金鑰處理單元以處理識別金鑰的程序圖。

【0082】識別金鑰處理單元(130)可基於一預定數目，將識別金鑰產生器(110)產生的N x M位元數位值分組。

【0083】雖然數位值的概念分群組已參考圖7描述，但是本發明並未侷限於描述的示範性具體實施例。包括暫存器或正反器的識別金鑰讀取器(120)可將暫存器或正反器分群組。所屬技術領域專業人士可容易應用這些示範性具體實施例；如此，示範性具體實施例不應認為悖離本發明的範疇。

【0084】在圖7，四個數位值組成一群組。

【0085】識別金鑰處理單元(130)可比較一群組(710)與一群組(720)之每一者產生的4位元數位值。當群組(710)的4位元數位值大於群組(720)的4位元數位值時，代表群組(710)與群組(720)的數位值可決定為1。

【0086】相反地，當群組(710)的4位元數位值小於群組(720)的4位元數位值時，代表群組(710)與群組(720)的數位值可決定為0。

【0087】同時，當群組(720)的4位元數位值大於群組(710)的4位元數位值時，代表性的數位值可決定為1。

【0088】當群組(710)的4位元數位值等於群組(720)的4位元數位值時，代表性的數位值可決定為1與0之一者、或不決定。

【0089】利用此方案，利用一群組(730)與一群組(740)等的比較，藉由產生代表性數位值，最終可利用產生的識別金鑰決定一識別金鑰。

【0090】上述可構成處理識別金鑰以增加識別金鑰隨機性之程序。

【0091】在識別金鑰產生器(110)中，當發生短路的比率(0數位值)、與不發生短路的比率(1數位值)不同時，在0與1間的平衡不可能有時執行。在此，有關每一位元的產生1的機率、與產生0的機率可不同於50%。不過，由於兩群組相等，所以兩群組之一者可具有數位值大於兩群組之另一者的機率可符合50%。因此，在0與1間的概率性平衡可透過上述程序加以執行。

【0092】當最初產生的識別金鑰符合N x M位元時，由於新的1位元數位值可利用8位元數位值決定，所以最終可由識別金鑰處理單元(130)決定的識別金鑰可符合N x M / 8位元。

【0093】上述有關分群組的程序、或藉由識別金鑰處理單元(130)處理識別金鑰的程序未侷限於示範性具體實施例，且可達成用於維持0數位值與1數位值間平衡之處理識別金鑰程序的各種修改與變化，不致悖離本發明的精神或範疇。

【0094】識別金鑰產生器(110)產生、及識別金鑰處理單元(130)決定的新識別金鑰可據有隨機性，且可變成可靠值，一旦產生，理論上會持續沒有變化。

【0095】根據本發明的具體實施例，根據時間流不會變化之具有亂數特徵的可靠識別金鑰能夠以相當低的製造成本容易製造。

【0096】在半導體製程期間，可產生任意識別金鑰，且在完成製程後，識別金鑰不會變化，如此在傳統方案中，可不需要外部輸入識別金鑰至非揮發性記憶體的程序。因此，不存在外部輸入與輸出識別金鑰的程序，且當半導體晶片的設計圖洩漏時，識別金鑰可基於製程期間的實際特徵差異而產生，且不可複製，具有非常優良的安全性。而且，由於不需要非揮發性記憶體的製程，所以可減少製造成本。

【0097】圖8為示例性說明根據本發明之一具體實施例產生識別金鑰的方法圖。

【0098】在步驟(810)，識別金鑰產生器(110)可產生一識別金鑰。

【0099】識別金鑰產生器(110)可組態成具有在半導體製程期間產生的節點間是否發生短路的隨機性，而且在節點間是否發生短路的特徵可實際無變化，因此一旦產生識別金鑰，就不會變化。

【0100】識別金鑰產生器(110)可基於在半導體製程期間產生的傳導層間形成的接點或穿孔間是否發生短路，以產生識別金鑰。設定接點的尺寸或穿孔的尺寸係如上面參考圖2與圖3描述。

【0101】識別金鑰產生器(110)可在半導體製程期間調整在傳導線路間的間隔，以便傳導線路的一部份短路，且傳導性線路的另一部份不會短路，藉此產生具有隨機性的一識別金鑰。具體實施例係如上面參考圖4至6描述。

【0102】在步驟(820)，識別金鑰讀取器(120)可利用一暫存器或一正反器儲存產生的識別金鑰。在產生識別金鑰及讀取識別金鑰中，接點或穿孔是否使傳導層或傳導線路短路可利用一讀取電晶體加以識別，如參考圖6的描述。

【0103】在步驟(830)，識別金鑰處理單元(130)可處理由識別金鑰產生器(110)產生的識別金鑰，藉此保證隨機性。

【0104】處理識別金鑰的程序係如上述圖7所示。

【0105】本發明的上述示範性具體實施例可記錄在非暫時電腦可讀媒體，包括實施電腦具體實施的各種不同操作。媒體亦可包括(單獨或結合)程式指令、資料檔案、資料結構等。非暫時電腦可讀媒體的範例包括磁性媒體，諸如硬碟、磁片與磁帶；光學媒體，諸如CD ROM光碟與DVD；磁性光碟媒體，諸如光碟；及特別組態成儲存及執行程式指令的硬體裝置，諸如唯讀記憶體(Read-Only Memory，ROM)、隨意存取記憶體(Random Access Memory，RAM)、快閃記憶體等。程式指令的範例包括機器碼(諸如由編譯器產生)與檔案(包含高階程式碼)二者，其可由利用直譯器的電腦能執行。描述的硬體裝置可配置成擔任一或多個軟體模組，以執行上述本發明示範性具體實施例的操作，或反之亦然。

【0106】雖然本發明的一些示範性具體實施例已顯示及描述，但是本發明並未侷限於描述的示範性具體實施例。相反的，所屬技術領域專業人士應瞭解，這些示模範具體實施例可修改，不致悖離本發明的精神與原理，且是在文後申請專利範圍及其等效的範疇內。

【符號說明】

【0107】

100	識別金鑰裝置
110	識別金鑰產生器
120	識別金鑰讀取器
130	識別金鑰處理單元
201	金屬層
202	金屬層
210、220、230	群組
410、420、430	群組
710、720、730、740	群組
810	產生識別金鑰
820	讀取識別金鑰
830	處理識別金鑰

專利案號：105116551（由103115670分割）

公告本

申請日：100/03/01

I652930

IPC分類：*H04L 9/14* (2006.01)
H01L 23/52 (2006.01)

【發明摘要】

【中文發明名稱】　產生識別金鑰之裝置及方法

【英文發明名稱】　APPARATUS AND METHOD FOR GENERATING IDENTIFICATION KEY

【中文】

一種用於產生一識別金鑰之裝置，其係藉由意欲違背在半導體製程期間提供的設計規則，概率性判斷在構成電路的節點間是否發生短路，以產生一識別金鑰。該識別金鑰產生裝置可包括：一識別金鑰產生器，以基於用來電連接半導體晶片傳導層之一接點或一穿孔是否使傳導層短路，以產生一識別金鑰；及一識別金鑰讀取器，其藉由讀取接點或一穿孔是否使傳導層短路，以讀取該識別金鑰。

【英文】

Provided is an apparatus for generating an identification key by a probabilistic determination of whether a short occurs between nodes constituting a circuit, by intentionally contradicting a design rule provided during a semiconductor manufacturing process. The identification key generating apparatus may include an identification key generator to generate an identification key based on whether a contact or a via used to electrically connect conductive layers in a semiconductor chip shorts the conductive layers, and an identification key reader to read the identification key by reading whether the contact or the via shorts the conductive layers.

【指定代表圖】　　圖1

【代表圖之符號簡單說明】

100	識別金鑰裝置
110	識別金鑰產生器
120	識別金鑰讀取器
130	識別金鑰處理單元

【發明圖式】

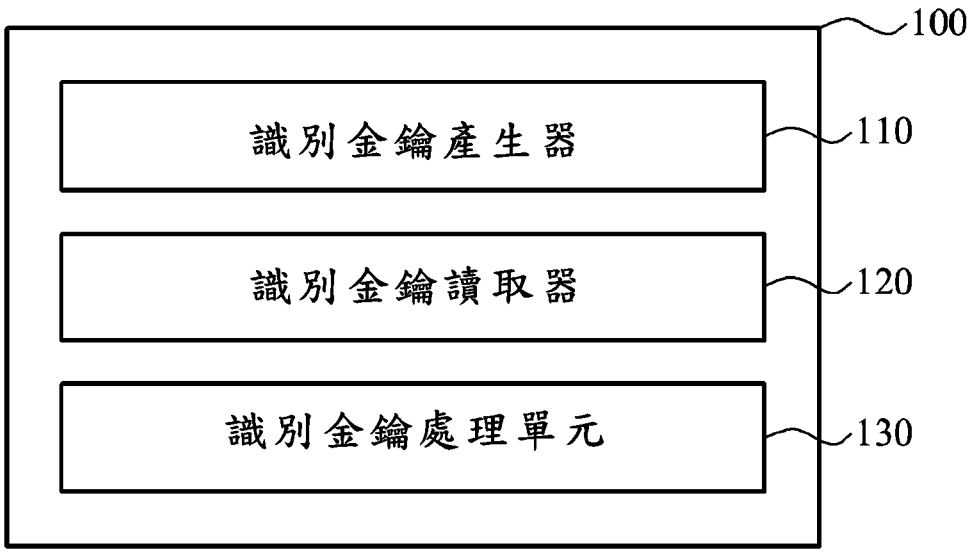

圖 1

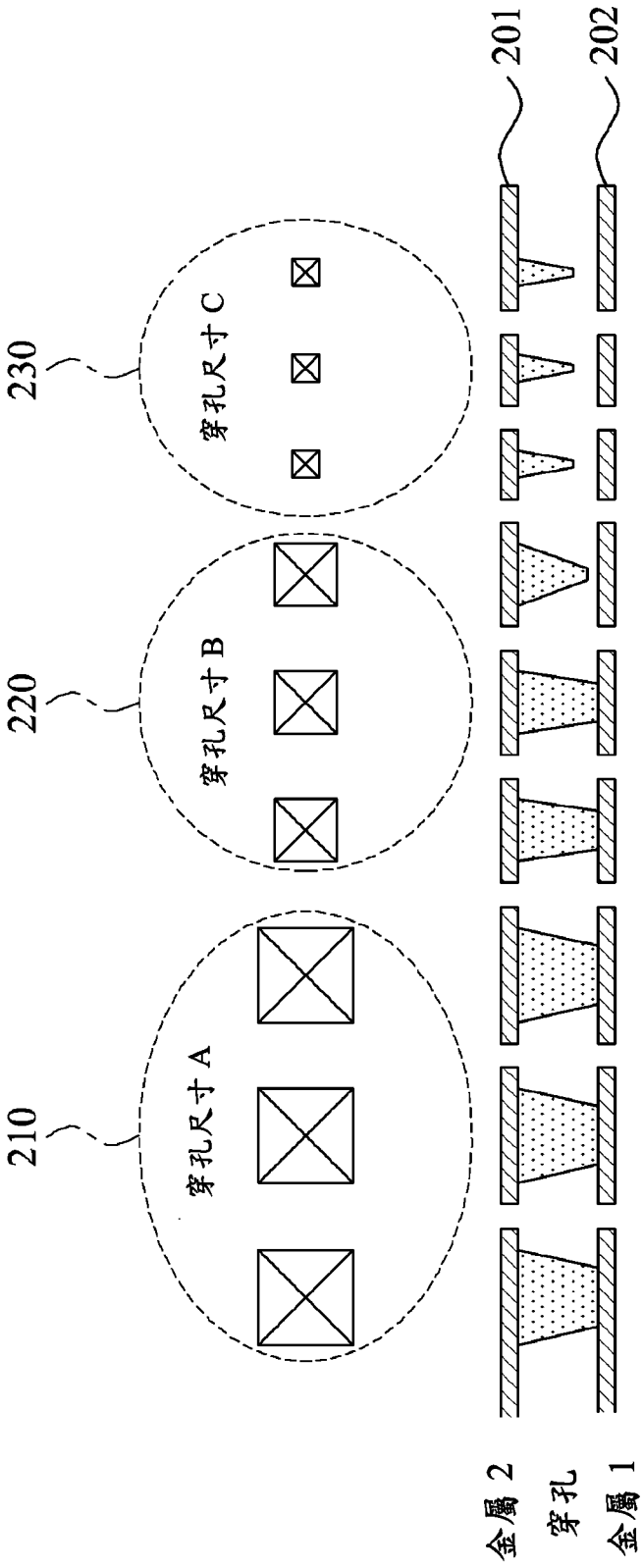

圖 2

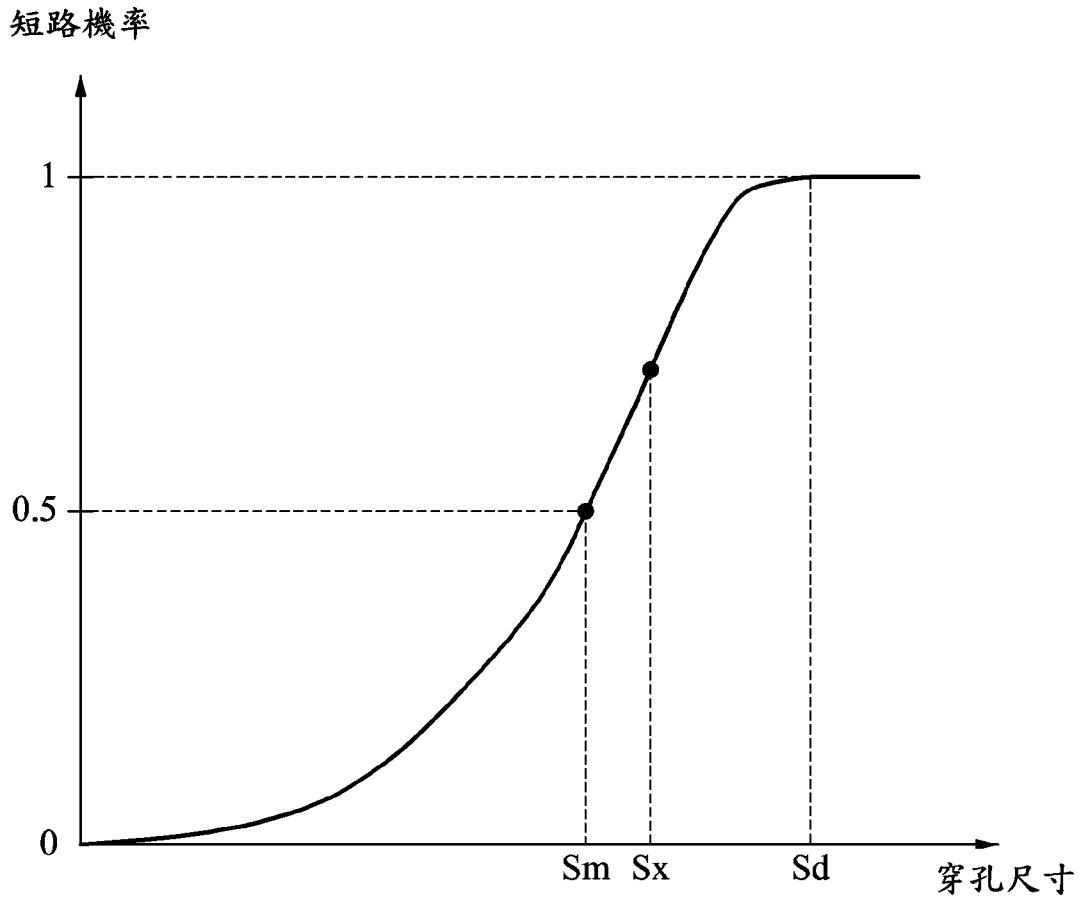

圖 3

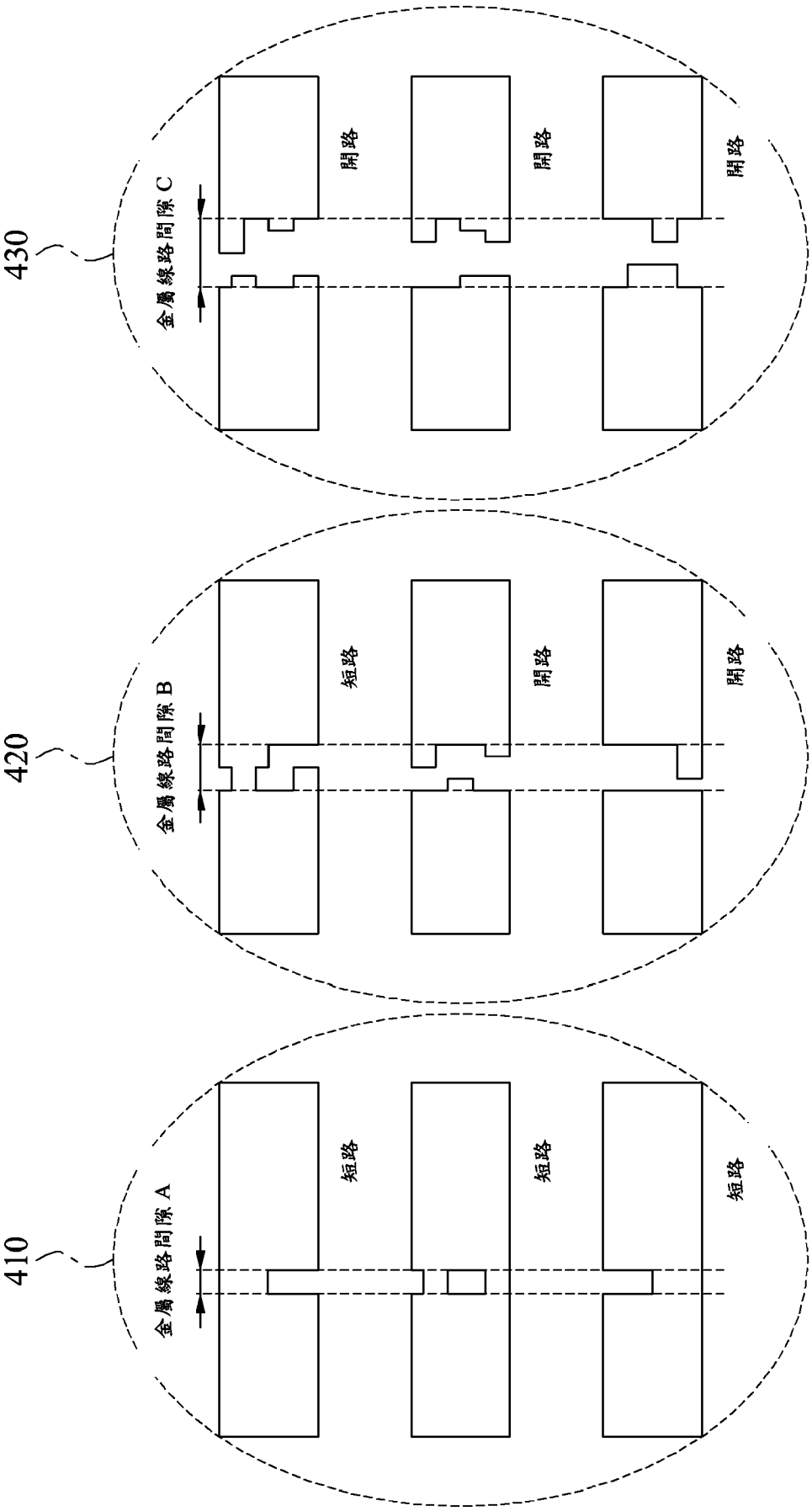

圖 4

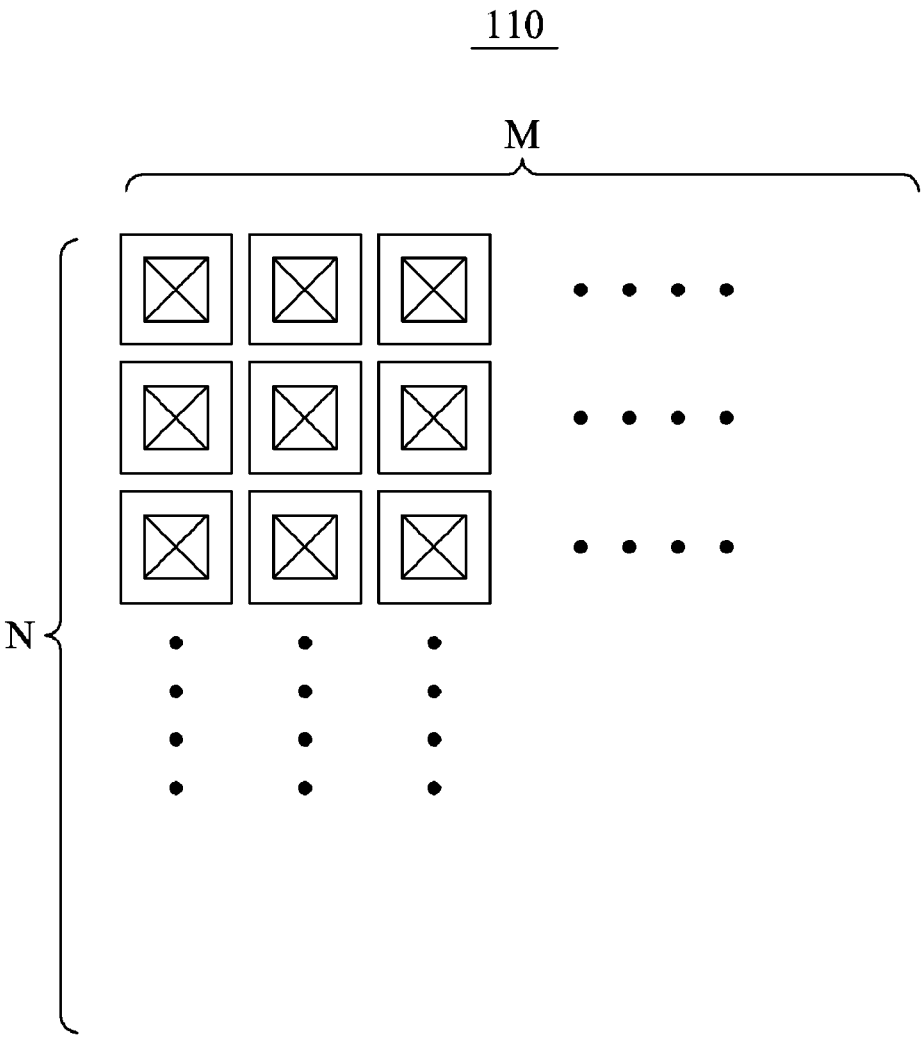

圖 5

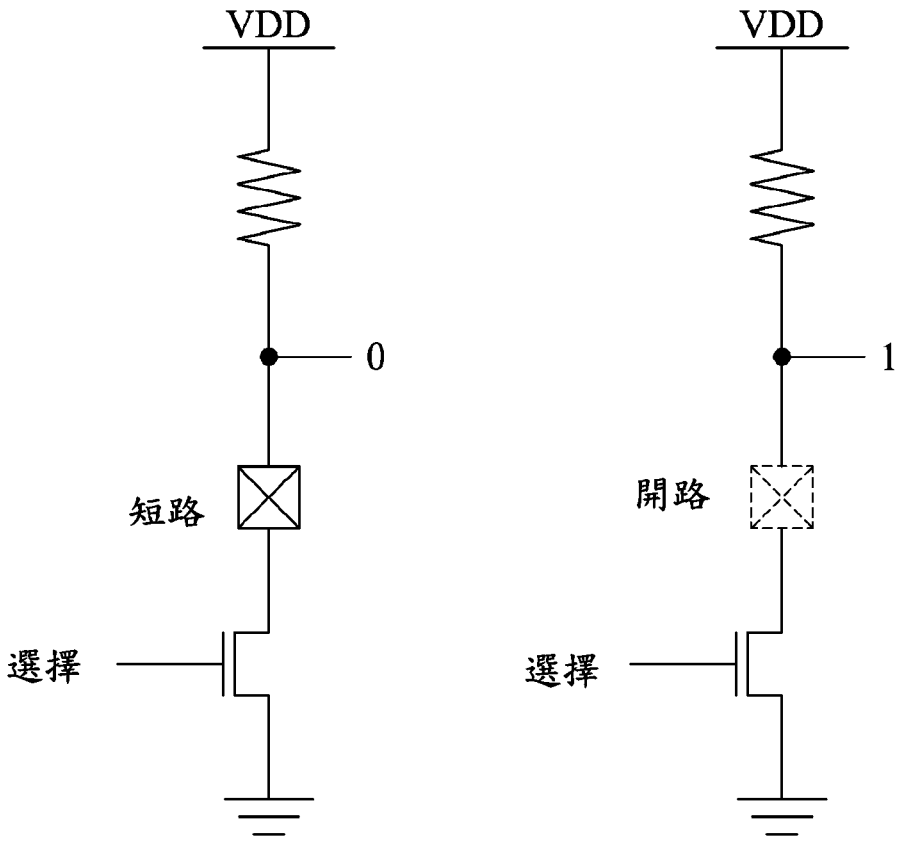

圖 6

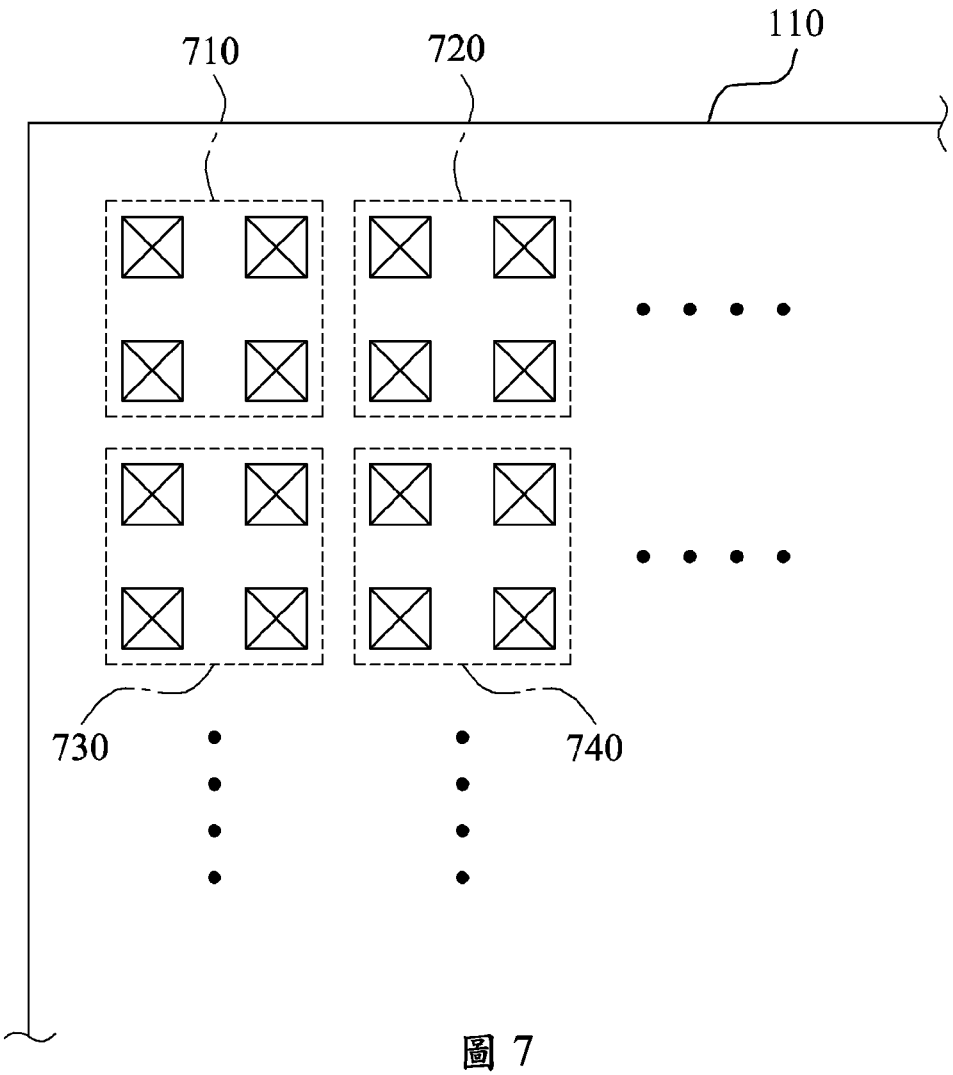

圖 7

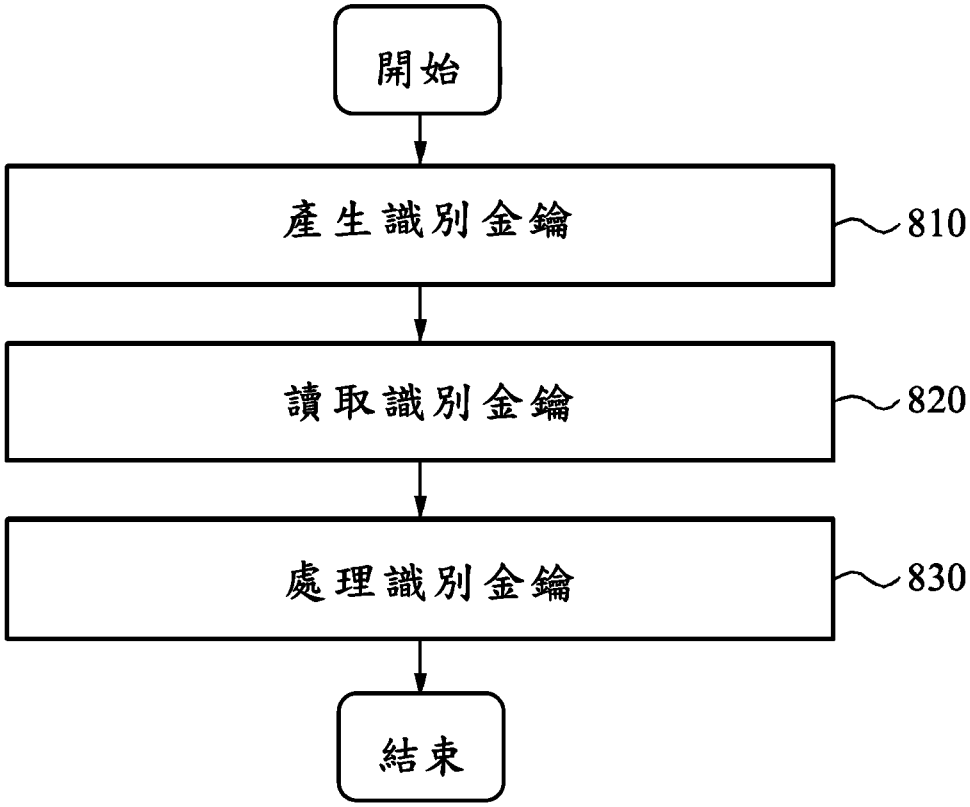

圖 8

修正日期：2018 年 02 月 14 日

【發明申請專利範圍】

【第1項】 一種用於產生一識別金鑰之裝置，該裝置包括：

一金鑰產生器，其藉由概率性決定構成電路的節點間是否發生短路，以產生一識別金鑰；及

一金鑰讀取器，其藉由讀取在構成電路的節點間是否發生短路，以讀取該識別金鑰；

其中，電路是否發生短路或開路是基於電路製作時的製程變異。

【第2項】 如請求項1所述裝置，其中，電路是否發生短路或開路包含半導體內傳導層間是否發生短路或開路。

【第3項】 如請求項2所述裝置，其中，半導體內傳導層間是否發生短路或開路包含該半導體內傳導層間的一接點或一穿孔是否與該傳導層短路。

【第4項】 如請求項3所述裝置，其中，該接點或該穿孔是否與該傳導層短路是與該接點或該穿孔的尺寸有關。

【第5項】 如請求項4所述裝置，其中，該接點或該穿孔的尺寸是與半導體製程期間的設計規則相互違背。

【第6項】 如請求項1所述裝置，其中，更包含：

一處理單元，該處理單元用以將該識別金鑰中的數位值分為含有k數位位元的第一群組以及含有k數位位元的第二群組，其中k是自然數，並經由比較該第一群組與該第二群組以提供處理後的識別金鑰。

【第7項】 一種用於產生一識別金鑰之方法，該方法包括：

藉由概率性決定構成電路的節點間是否發生短路，以產生一金鑰；及

藉由讀取在構成電路的節點間是否發生短路，以讀取該金鑰；

其中，電路是否發生短路或開路是基於電路製作時的製程變異。

【第8項】 如請求項7所述方法，其中，電路是否發生短路或開路包含半導體內傳導層間是否發生短路或開路。

【第9項】 如請求項8所述方法，其中，半導體內傳導層間是否發生短路或開路包含該半導體內傳導層間的一接點或一穿孔是否與該傳導層短路。

【第10項】如請求項9所述方法，其中，該接點或該穿孔是否與該傳導層短路是與該接點或該穿孔的尺寸有關。

【第11項】如請求項10所述方法，其中，該接點或該穿孔的尺寸是與半導體製程期間的設計規則相互違背。

【第12項】如請求項7所述方法，其中，更包含：

處理該識別金鑰，其中該處理過程包含將該識別金鑰中的數位值分為含有k數位位元的第一群組以及含有k數位位元的第二群組，其中k是自然數，並經由比較該第一群組與該第二群組以提供處理後的識別金鑰。