

捌、聲明事項

☐ 本業係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：_____

☒ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號 順序註記】

1. 美國；2002年03月18日；10/100,462

2. _____

3. _____

☒ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號 順序註記】

1. 美國；2002年03月18日；10/100,462

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號 順序註記】

1. _____

2. _____

3. _____

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

1. _____

2. _____

3. _____

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

1. _____

2. _____

3. _____

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

先前申請參考

本專利申請案已於2002年3月18日提出美國專利申請，專利申請案號為10/100,462。

技術領域

本發明係關於一種積體電路，具體而言，係關於積體電路之安全保護。

先前技術

隨著積體電路被運用在愈來愈重視安全保護的應用中，積體電路的安全保護也愈來愈重要。此類應用的部份包括智慧卡、行動電話、網際網路通訊裝置等等。具體而言，通常希望提供防止詐欺或未授權存取積體電路之一個或多個部份的安全保護。許多積體電路都包含輸入及/或輸出端子，用於輸入資訊至積體電路及/或自積體電路輸出資訊。此類輸入/輸出端子可以提供一未授權存取積體電路之一個或多個部份的路徑。此外，連接至一積體電路的某些輸入/輸出端子可用於偵錯、模擬及/或測試用途，並且也可以提供一未授權存取積體電路之一個或多個部份的路徑。

一種用於積體電路偵錯、模擬及/或測試用途的常用標準是已熟知的JTAG (Joint Test Action Group) IEEE (Institute of Electrical and Electronic Engineers；電機電子工程學會)1194.1測試存取連接埠及邊界掃描架構。除了標準JTAG介面以外，還有用於積體電路的各種其他偵錯、模擬及/或測試

介面。

在利用偵錯、模擬及/或測試介面的系統中，必須防止未授權存取內部IC資源，以便保護此類資源的安全。因此，需要一種為積體電路(IC)提供防止未授權存取之安全保護同時繼續提供偵錯、模擬及測試能力的方法。

發明內容

本發明係關於一種積體電路(IC)，具體而言，係關於防止未經授權存取積體電路(IC)之安全保護。在一項具體實施例中，會在積體電路(IC) 10外部提供一識別符。接著，將一相對應之輸入IC安全密鑰(52)提供給該積體電路(IC) 10，並且比對一所儲存之IC安全密鑰(30)。如果該輸入IC安全密鑰(52)不符合該所儲存之IC安全密鑰(30)，則禁止存取該受保護型功能電路(12)。本發明可使用任何偵錯介面，包括使用電氣和電子工程師協會(IEEE)所定義之JTAG 1149.1介面的標準偵錯介面。

實施方式

在本文中，術語"匯流排"係用來表示複數個信號或導線，其可用於傳遞一種或一種以上之各種資訊，如資料、位址、控制或狀態。當提及將信號、狀態位元或類似的裝置轉譯(rendering)成為邏輯真(true)或邏輯偽(false)狀態時，會分別使用術語"確立"(assert)及"否定"(negate)。如果邏輯真(true)狀態是邏輯位準壹時，則邏輯偽(false)狀態是邏輯位準零。並且，如果邏輯真(true)狀態是邏輯位準壹時，則邏輯偽(false)狀態是邏輯位準零。本文中使用的

術語 "偵錯" 表示其字面意義，並且還包含模擬和測試功能。

圖 1 顯示根據本發明具體實施例之積體電路 (IC) 10 的方塊圖。在一項具體實施例中，IC 10 包括一偵錯連接埠 20 及受保護型功能電路 12。在一項具體實施例中，受保護型功能電路 12 包含一處理器 14、其他電路 16 及一輸入/輸出 (I/O) 電路 18，這些組件以雙向通訊方式互相耦合，並且經由通訊信號 26 耦合至該偵錯連接埠 20。在一項具體實施例中，處理器 14 可能是用於執行指令的任何類處理器，例如，一中央處理單位、一數位信號處理器、一計時器處理單元等等。在一項具體實施例中，該其他電路 16 可能是用於執行該 IC 10 之一個或多個預定功能的電路，但是執行預定功能不需要執行指令，例如，MPEG 編碼器、解碼器、影像處理單元或硬接線型資料處理元件。在替代具體實施例中，受保護型功能電路 12 可只包含處理器 14、只包含其他電路 16，或包含處理器 14 和其他電路 16 兩者。在一項具體實施例中，I/O 電路 18 被耦合至一個或多個 IC 端子 24，以便與 IC 10 外部的電路 (圖中未顯示) 通訊。本發明的替代具體實施例中，I/O 電路 18 可包含任何類型的外部匯流排結構，包括資料/位址/控制匯流排結構。在其他具體實施例中，IC 10 可能甚至沒有 I/O 電路 18 及 IC 端子 24，例如，在沒有外部匯流排之單一晶片模式運用的 IC 10。在本發明一項具體實施例中，偵錯連接埠 20 係以雙向方式耦合至一個或多個 IC 端子 22，用於允許偵錯連接埠 20 與 IC 10

外部的裝置(圖中未顯示)通訊。

圖2顯示根據本發明具體實施例之圖1所示之偵錯連接埠20之一部份的方塊圖。在一項具體實施例中，偵錯連接埠20包含偵錯電路41，其經由信號58以雙向方式耦合至IC端子22，以便自IC 10外部的裝置(圖中未顯示)接收一個或多個偵錯信號及/或提供一個或多個偵錯信號給IC 10外部的裝置(圖中未顯示)。偵錯電路41包含其他偵錯電路42，其經由信號50以雙向方式耦合至存取保護電路40。該其他偵錯電路42將一個或多個信號48提供給識別符儲存電路32，用以指示該識別符儲存電路32何時經由一個或多個導線56或該等一個或多個端子22提供IC 10外部的所儲存之識別符值。或者，該偵錯電路41經由該等信號48從該識別符儲存電路32接收一所儲存的識別符值，並且經由該等一個或多個導線58或該等一個或多個端子22提供IC 10外部的所儲存之識別符。該存取保護電路40係經由導線60以雙向方式耦合至該受保護型功能電路12，以便傳送用於偵錯用途的資訊。

在本發明的一項具體實施例中，該識別符儲存電路32中所儲存的識別符值是所製造之每個積體電路(IC) 10所特有的值。然而，在替代具體實施例中，可以使用介於識別符值與IC間之任何所想要的對應方式；例如，1:1對應，而某些其他具體實施例可能不要此對應方式。可以將識別符值儲存在可單次程式規劃非揮發性電路中，例如可被遮罩程式規劃的熔絲，或藉由該偵錯連接埠20外部的邏輯所

提供的熔絲。可以基於各種用途使用該識別符值來追蹤一 IC，以及在 IC 10 外部提供一識別符值。IC 10 的製造商可在 IC 10 外部保存一識別符值與對應之 IC 安全密鑰值的機密清單。同時，每個 IC 10 還儲存識別符(儲存在該識別符儲存電路 32 中)及該所儲存之 IC 安全密鑰(儲存在 IC 安全密鑰儲存電路 30 中)。

當 IC 10 外部的一被允許之偵錯裝置(圖中未顯示)經由該等端子 22 從 IC 10 接收該識別符值時，就會檢查識別符值與對應之 IC 安全密鑰值的機密清單，以便決定適當的輸入 IC 安全密鑰值，以經由該等 IC 端子 22 和一個或多個導線 52 輸入至 IC 10。請注意，可選擇任何適當長度的識別符長度，只要有足夠的位元數量可如所預期對應至個別 IC 即可。同樣地，可選擇任何適當長度的 IC 安全密鑰長度，只要有足夠的位元數量可防止以嘗試錯誤法未授權存取該受保護型功能電路 12 即可。在一項具體實施例中，識別符的長度為 16 位元及 IC 安全密鑰的長度為 48 位元。本發明的替代具體實施例可不需要提供識別符值，因此可不包含該識別符儲存電路 32。

在一項具體實施例中，該偵錯連接埠 20 包含該 IC 安全密鑰儲存電路 30，用於經由一個或多個信號 54 將一所儲存之 IC 安全密鑰(30)提供給比較電路 38。在一項具體實施例中，密鑰核對電路 34 以選用方式包括計數器電路 36 及該比較電路 38。在本發明替代具體實施例中，可以使用該計數器電路 36 防止保護啟用信號 46 失效。在本發明的一項具體

實施例中，如果在一預選擇事件之後經過了一段預先決定時間，該計數器電路36會防止保護啟用信號46失效。雖然該預選擇事件可能是任可所想要的事件，但是可能的事件是重置44之確立，或者是從該等IC端子22接收一第一輸入IC安全密鑰。在某些具體實施例中，如果在一預先決定時間視窗期間比較結果不是相符合，則不會啟用對該受保護型功能電路12的存取。在替代具體實施例中，該計數器電路36可計算該比較電路38所執行之未成功比較的次數，並且如果從上一次重置信號44確立之後已執行未成功比較達預先決定次數，就會防止該保護啟用信號46失效。在本發明的一項具體實施例中，在開機或重置該密鑰核對電路34之後，會將該保護啟用信號46初始化為已確立狀態，以便防止存取該受保護型功能電路12。在其他具體實施例中，可以藉由IC 10的內部或外部之其他事件來確立該保護啟用信號46。

在本發明的一項具體實施例中，該密鑰核對電路34接收一輸入IC安全密鑰，這是已藉由一個或多個IC端子22及一個或多個導線52從IC 10外部接收的輸入IC安全密鑰。接著，比較電路38比較從該等端子22所接收的該輸入IC安全密鑰與該IC安全密鑰儲存電路30中的該所儲存之IC安全密鑰。該比較電路38經由該等導線54從該IC安全密鑰儲存電路30接收該所儲存之IC安全密鑰。在本發明的一項具體實施例中，該比較電路38按照該比較電路38所接收之該所儲存之IC安全密鑰的每位位元來執行一逐一位元比較。在

本發明的替代具體實施例中，可暫時儲存該輸入IC安全密鑰，接著將所接收之該輸入IC安全密鑰的所有位元一次比較於該所儲存之IC安全密鑰。

如果該輸入IC安全密鑰符合該所儲存之IC安全密鑰，則該比較電路38否定(negate)該保護啟用信號46。否定該保護啟用信號46造成該存取保護電路40允許藉由該其他偵錯電路42來存取該受保護型功能電路12。在本發明的某些具體實施例中，確立該保護啟用信號46造成停用該其他偵錯電路42的一個或多個部份，而其他偵錯電路42的其他部份維持啟用狀態，而不受該保護啟用信號46之狀態影響。

在本發明的某些具體實施例中，強制啟用電路45可用來撤銷該比較電路38的功能，並且強制該保護啟用信號46被否定，而不管該輸入IC安全密鑰和該所儲存之IC安全密鑰的值。該強制啟用電路45的一項可能用途是，在製造商偵錯和測試IC 10期間啟用該偵錯電路41。一旦已確認IC 10上的電路設計，就可永久停用該強制啟用電路45，促使該IC端子24決不會再次被略過。實施此項做法的一種方式為，使用一個或多個可單次程式化非揮發性儲存電路，例如，熔絲。例如，在一項具體實施例中，燒斷該強制啟用電路45內的一個或多個熔絲可促使該強制啟用電路45再也無法撤銷該密鑰核對電路34。

在本發明的某些具體實施例中，會將重置信號44提供給該密鑰核對電路34及IC 10的其他部份。接著，藉由該其他電路16（請參閱圖1）中的重置確立電路或IC 10的內部

或外部電路來確立該重置信號44，以便重置IC 10的整個部份或一部份。在某些具體實施例中，該比較電路38被停用，並且在該計數器電路36(視需要使用)已判斷一預先決定時間已逾時或已嘗試預先決定次數後，就再也不允許比較。該密鑰核對電路可視需要使用該重置信號44，以重置該計數器電路36及/或啟用該比較電路38，以開始或重新繼續執行比較。

該其他偵錯電路42可包含用於實施一個或多個標準偵錯、模擬或測試介面與協定的電路，例如，JTAG介面與協定。在一項具體實施例中，IC端子22可包含包括JTAG TDO(測試資料輸出)和TDI(測試資料輸入)信號。在本發明的某些具體實施例中，該保護啟用信號46不會影響該其他偵錯電路42所執行的選用JTAG功能。這允許該其他偵錯電路42以JTAG相容方式執行，甚至當該保護啟用信號46被確立且因此防止該偵錯電路41存取該受保護型功能電路12時。

請注意，在本發明的某些具體實施例中，可使用該等IC端子22之一當做偵錯IC端子，用以經由信號52將該輸入IC安全密鑰提供給該比較電路38，並且還當做一當做偵錯IC端子，用以經由該偵錯電路41與該受保護型功能電路12通訊。在本發明的某些具體實施例中，信號52及信號58和60中的一個或多個信號可能是JTAG TDI信號。

同樣地，在本發明的某些具體實施例中，可使用該等IC端子22之一當做偵錯IC端子，用以經由信號56將該識別符

值從該識別符儲存電路 32 提供給 IC 10 的外部電路 (圖中未顯示)。還可使用該等 IC 端子 22 之同一端子當做偵錯 IC 端子，用以經由該存取保護電路 40 提供從該受保護型功能電路 12 至 IC 10 之外部電路 (圖中未顯示) 間的通訊。在一項具體實施例中，信號 56 及信號 58 和 60 中的一個或多個信號可能是 JTAG TDO 信號。

圖 3 顯示根據本發明具體實施例，用於提供積體電路之安全保護的方法流程圖。在一項具體實施例中，可使用圖 3 所示的流程為圖 1 所示的 IC 10 提供安全保護。從橢圓形之開始步驟 100，圖 3 所示的流程進行到步驟 102，用以在 IC 外部提供一識別符。步驟 102 經由圓形步驟 A 104 進行到步驟 106。在步驟 106，從該 IC 之外部接收一輸入 IC 安全密鑰。從步驟 106，流程進行到步驟 108，用以比較該輸入 IC 安全密鑰與所儲存之 IC 安全密鑰。從步驟 108，流程進行到菱形之判斷步驟 110，用以判斷該輸入 IC 安全密鑰與該所儲存之 IC 安全密鑰是否相符合。

如果相符合，流程進行到選用型步驟 112，用以啟用對該受保護型功能電路 12 之存取。從步驟 112，流程進行到選用型步驟 114，用以啟用對該其他偵錯電路 42 之至少一部份之存取。請注意，在本發明的替代具體實施例中，可略過選用型步驟 114，並且不使用符合結果來影響該其他偵錯電路 42 中的任何電路。從步驟 114，流程進行到之橢圓形步驟 124 而流程結果。

菱形之判斷步驟 110 之結果為不符合，則流程進行到步

驟 116，用以拒絕對該受保護型功能電路 12 之存取。在步驟 116，流程進行到選用型步驟 118，用以拒絕對該其他偵錯電路 42 之至少一部份之存取。請注意，在本發明的替代具體實施例中，可略過選用型步驟 118，並且不使用符合結果來影響該其他偵錯電路 42 中的任何電路。或者，該其他偵錯電路 42 之一個或多個部份可繼續維持啟用狀態，因此不受該保護啟用信號 46 所影響。在步驟 118，流程進行到菱形之判斷步驟 120，用以檢查是否允許接收及評估其他 IC 安全密鑰。如果不允許接收及評估其他 IC 安全密鑰，則流程進行到橢圓形步驟 124 而流程結果。然而，如果允許接收及評估其他 IC 安全密鑰，則流程進行到步驟 122，可選擇性插入一選用型延遲。提供一選用型延遲可能有助於限制嘗試次數，用以阻撓本發明所提供的安全保護機制，同時允許校正一錯誤輸入項的合法機會。可用任何適當的方法來決定該選用型延遲的長度。某些具體實施例可省略該選用型延遲步驟 122。從步驟 122，流程進行到圓形步驟 A 104，以便接收其他之輸入 IC 安全密鑰。在替代具體實施例中，可藉由修改菱形之判斷步驟 120，以限制鍵入一輸入 IC 安全密鑰的嘗試次數。菱形之判斷步驟 120 的基礎可能是，計數鍵入嘗試次數，並且比較該嘗試次數與一預先決定臨限值，並一如果該嘗試次數等於或大於該臨限值，則拒絕回到圓形步驟 A 104。在其他具體實施例中，菱形之判斷步驟 120 的基礎可能是任何其他值、演算法或 IC 10 的內部或外部的狀態。

圖 4 顯示根據本發明替代具體實施例，用於提供積體電路之安全保護的方法流程圖。在一項具體實施例中，可使用圖 4 所示的流程為圖 1 所示的 IC 10 提供安全保護，其中 IC 10 使用一 JTAG 測試存取連接埠來接收一輸入 IC 安全密鑰。當圖 4 中所執行之步驟的功能相同於圖 3 中相對應之步驟的功能時，圖 4 會使用和圖 3 相同的參考號碼。與圖 3 所示的流程相比，圖 4 所示的流程提供本發明一項具體實施例的更詳細細節，其中會利用一 JTAG 測試存取連接埠及邊界掃描架構。

從橢圓形之開始步驟 100，圖 4 所示的流程進行到步驟 102，用以使 JTAG 狀態機器進入 SHIFT_IR 狀態，並且在維持此狀態時，在後續時脈循環期間在 TDO 信號輸出一識別符 (PART_ID)。在一項具體實施例中，於 SHIFT_IR 狀態期間，該 TDO 信號同時提供該識別符 (PART_ID) 與一二進位 01。該 TDO 信號係在 IC 外部所提供。步驟 102 經由圓形步驟 A 104 進行到步驟 201。在步驟 201，當該 JTAG 狀態機器維持或再次進入該 SHIFT_IR 狀態時，會在 TDI 信號上輸入一使用者定義型指令 (例如，ENABLE_DEBUG 指令) 的二進位表示。從步驟 201，流程進行到步驟 202，用以使該 JTAG 狀態機器進入 UPDATE_IR 狀態，並且將該 ENABLE_DEBUG 指令之二進位表示載入 JTAG_IR (指令暫存器)。從步驟 202，流程進行到步驟 106、108，用以執行 ENABLE_DEBUG 指令。在步驟 106、108，從該 IC 之外部接收一輸入 IC 安全密鑰。按照所接收之該輸入 IC 安全密鑰的位元，以逐位元方

式比較該所儲存之IC安全密鑰。在本發明的替代具體實施例中，可暫時儲存該輸入IC安全密鑰，直接已接收到所有位元，以便以平行方式執行比較。從步驟106、108，在比較該完整輸入IC安全密鑰與該所儲存之IC安全密鑰之後，流程進行到菱形之判斷步驟110，其方式類似於圖3所示的流程。

於前面的說明書中，已參考特定具體實施例來說明本發明。然而，熟知技藝人士應明白本發明的各種修改並且容易修改，而不會脫離如下文中申請專利範例所提供之本發明的範疇與精神。因此，說明書暨附圖應視為解說，而不應視為限制，並且所有此類的修改皆屬本發明範疇內。例如，雖然已就安全防止從IC 10之外部來源存取IC 10而論來說明本發明，然而在本發明的替代具體實施例中，可防止IC 10上的其他未授權部份存取同一IC 10上之電路的一個或多個部份。

已說明關於特定具體實施例的優勢、其他優點及問題解決方案。但是，可導致任何優勢、優點及解決方案發生或更顯著的優勢、優點、問題解決方案及任何元件不應被理解為任何或所有申請專利範例的關鍵、必要項或基本功能或元件。本文中所使用的術語"包括"、"包含"或其任何其他變化都是用來涵蓋非專有內含項，使得包括元件清單的方法、物品或裝置不僅包括這些元件，而且還包括未明確列出或此類方法、物品或裝置原有的其他元件。

圖式簡單說明

本發明將藉由實例及附圖來進行解說，但本發明未限定在這些實例及附圖內，其中相似的參照代表相似的元件，並且其中：

圖 1 顯示根據本發明具體實施例之積體電路 (IC) 10 的方塊圖；

圖 2 顯示根據本發明具體實施例之圖 1 所示之偵錯連接埠 20 之一部份的方塊圖；

圖 3 顯示根據本發明一項具體實施例，用於提供積體電路之安全保護的方法流程圖；以及

圖 4 顯示根據本發明替代具體實施例，用於提供積體電路之安全保護的方法流程圖。

熟知技藝人士應明白，圖中的元件是簡化的圖解，並且不需要按比例繪製。例如，相對於其他元件，圖中部份元件的尺寸可能過度放大，以利於更容易瞭解本發明的具體實施例。

圖式代表符號說明

10	積體電路 (IC)
12	受保護型功能電路
14	處理器
16	其他電路
18	輸入/輸出 (I/O) 電路
20	偵錯連接埠
22, 24	IC 端子
26	通訊信號

30	IC 安全密鑰儲存電路
32	識別符儲存電路
34	密鑰核對電路
36	計數器電路
38	比較電路
40	存取保護電路
41	偵錯電路
42	其他偵錯電路
44	重置信號
45	強制啟用電路
46	保護啟用信號
50, 54, 58, 48	信號
52	輸入 IC 安全密鑰
58, 60, 52	導線

肆、中文發明摘要

本發明係關於一種積體電路(IC)，具體而言，係關於防止未經授權存取積體電路(IC)之安全保護。在一項具體實施例中，會在積體電路(IC) 10外部提供一識別符。接著，將一相對應之輸入IC安全密鑰(52)提供給該積體電路(IC) 10，並且比對一所儲存之IC安全密鑰(30)。如果該輸入IC安全密鑰(52)不符合該所儲存之IC安全密鑰(30)，則禁止存取該受保護型功能電路(12)。本發明可使用任何偵錯介面，包括使用電氣和電子工程師協會(IEEE)所定義之JTAG 1149.1介面的標準偵錯介面。

伍、英文發明摘要

The invention relates to an integrated circuit (IC), and more particularly to security to protect an IC (10) against unauthorized accesses. In one embodiment, an identifier is provided external to IC 10. A corresponding input IC security key (52) is then provided to IC 10 and compared to a stored IC security key (30). If the input IC security key (52) and the stored IC security key (30) do not match, access to protected functional circuitry (12) is prohibited. The present invention may use any debug interface, including standard debug interfaces using the JTAG 1149.1 interface defined by the IEEE.

拾壹、圖式

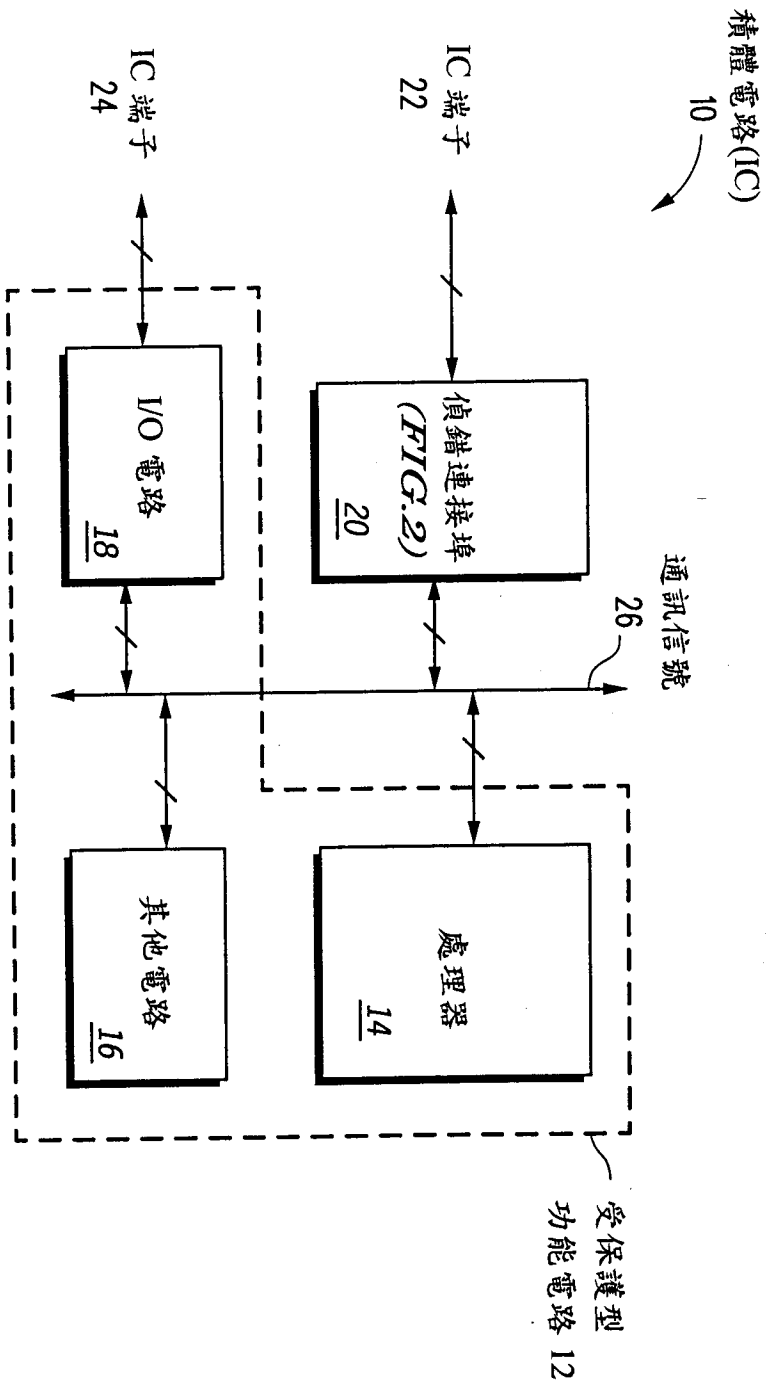


圖 1

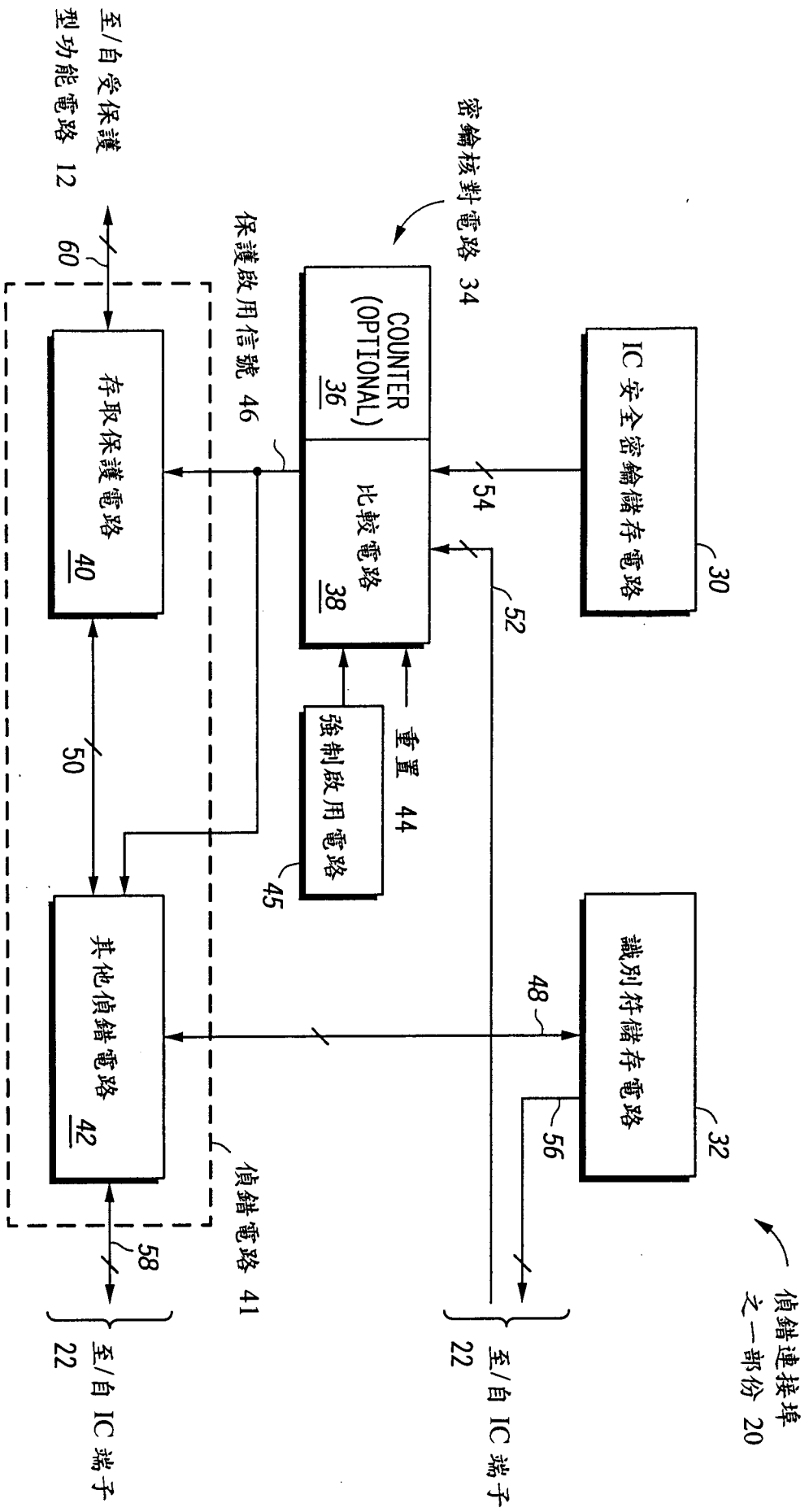


圖 2

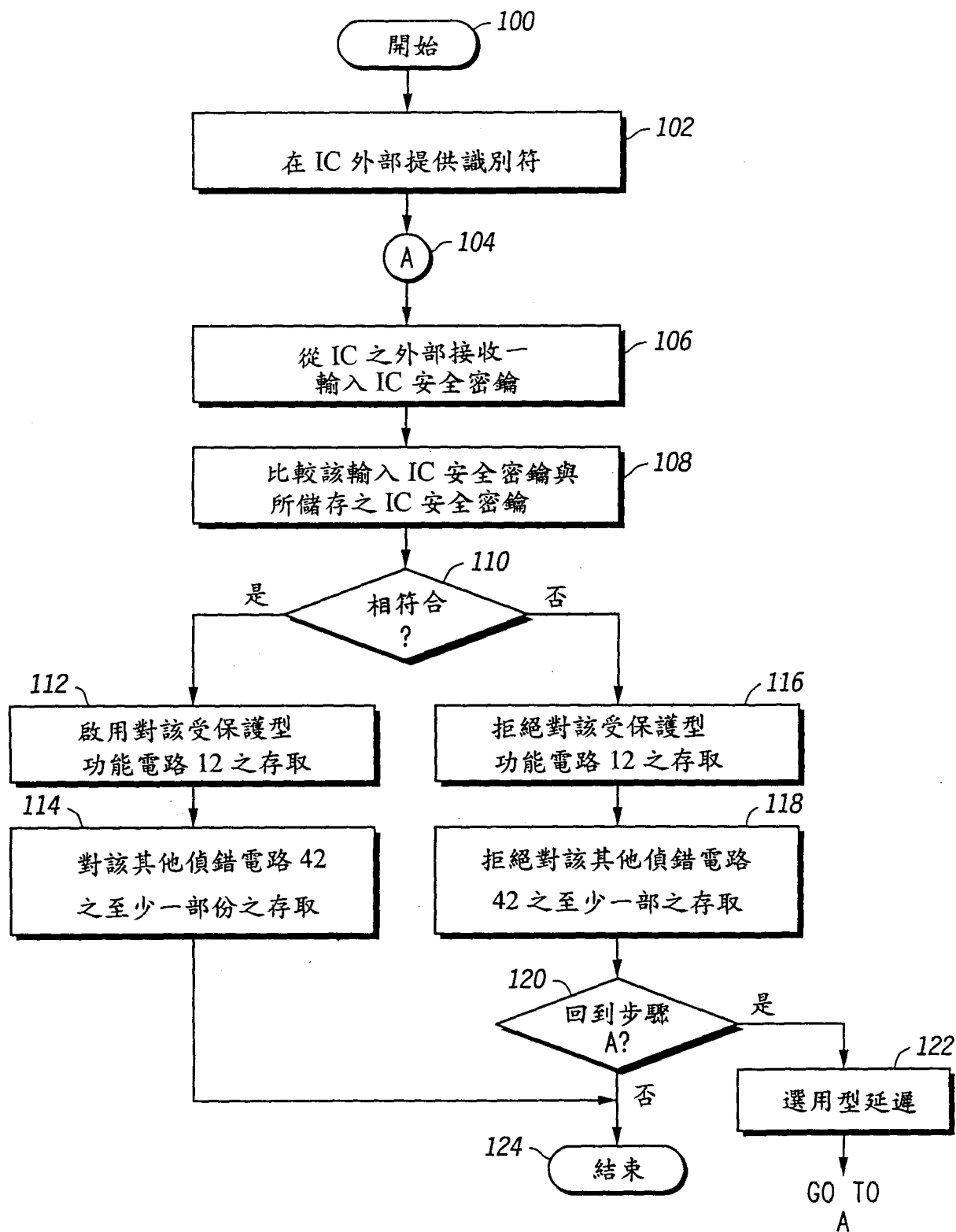


圖 3

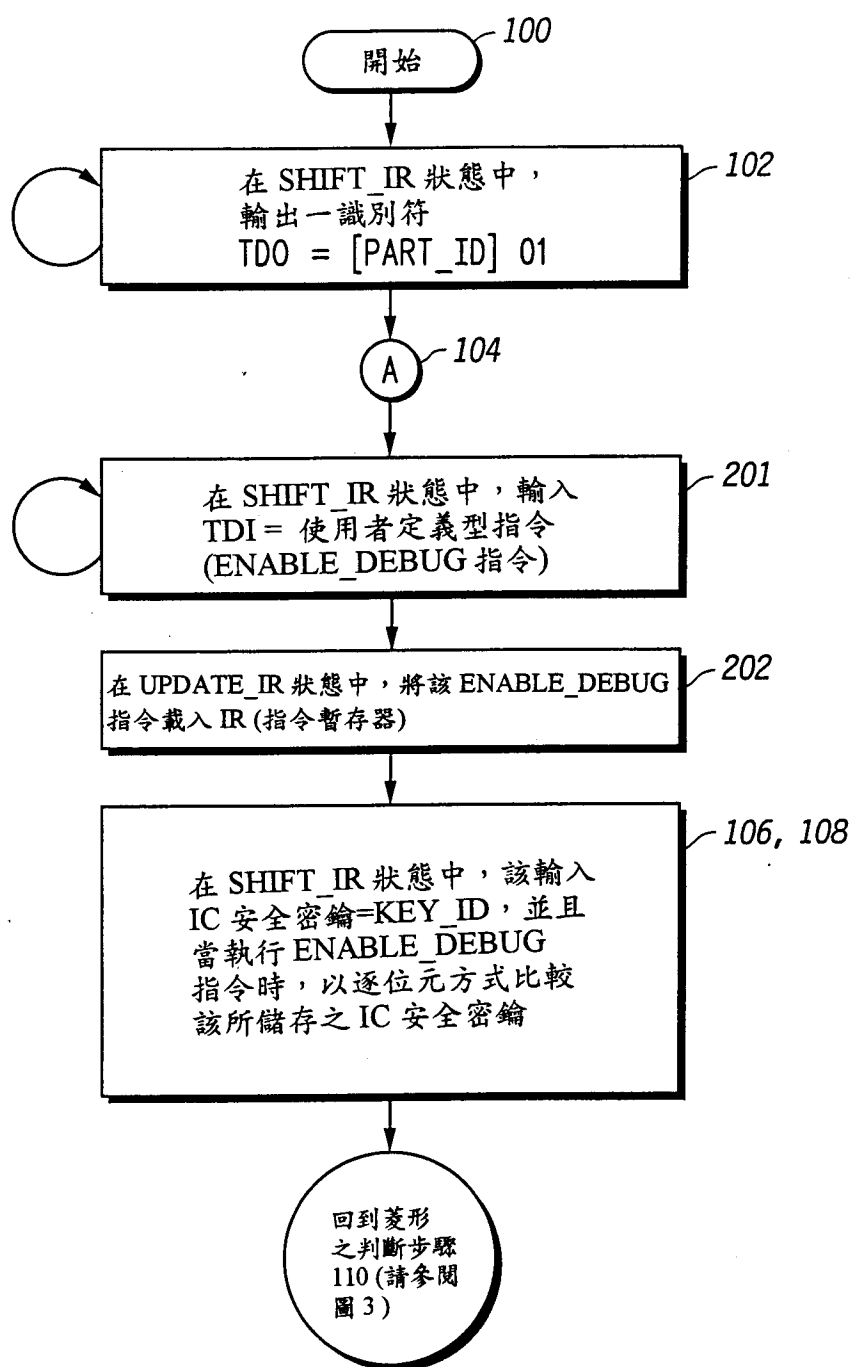


圖 4

陸、(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：

- | | |
|--------|--------------|
| 10 | 積體電路(IC) |
| 12 | 受保護型功能電路 |
| 20 | 偵錯連接埠 |
| 14 | 處理器 |
| 16 | 其他電路 |
| 18 | 輸入/輸出(I/O)電路 |
| 26 | 通訊信號 |
| 22, 24 | IC端子 |

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

發明專利說明書

中文說明書替換頁(93年10月)

(填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫)

※申請案號：092105788 ※IPC分類：H04L 9/00 (2006.01)※申請日期：92.3.17

壹、發明名稱

(中文)積體電路之安全保護及其方法(英文)INTEGRATED CIRCUIT SECURITY AND METHOD THEREFOR貳、發明人(共2人)發明人 1 (如發明人超過一人，請填說明書發明人續頁)姓名：(中文) 威廉 C. 莫爾(英文) WILLIAM C. MOYER住居所地址：(中文) 美國德州滴泉市碼頭支路1005號(英文) 1005 PIER BRANCH ROAD, DRIPPING SPRINGS,
TX 78620, U.S.A.國籍：(中文) 美國 (英文) U.S.A.參、申請人(共1人)申請人 1 (如申請人超過一人，請填說明書申請人續頁)姓名或名稱：(中文) 美商飛思卡爾半導體公司(英文) FREESCALE SEMICONDUCTOR, INC.住居所或營業所地址：(中文) 美國德州奧斯丁市威廉坎嫩道西6501號(英文) 6501 WILLIAM CANNON DRIVE WEST,
AUSTIN, TEXAS 78735, U.S.A.國籍：(中文) 美國 (英文) U.S.A.代表人：(中文) 珍妮佛 B 伍艾梅特(英文) WUAMETT, JENNIFER B

發明人 2

姓名：(中文) 麥可 D. 費茲西蒙

(英文) MICHAEL D. FITZSIMMONS

住居所地址：(中文) 美國德州奧斯汀市德州北首都公路7700號723室

(英文) 7700 NORTH CAPITAL OF TEXAS #723, AUSTIN,

TX 78731, U.S.A.

國籍：(中文) 美國

(英文) U.S.A.

拾、申請專利範圍

1. 一種積體電路(IC) (10)，包括：

包括一處理器(14)之受保護型功能電路(12)；

一偵錯連接埠，允許一外部裝置對受保護型電路之外部存取，該偵錯連接埠具有儲存電路(30)，用於儲存一所儲存之IC安全密鑰；

一IC偵錯介面(52 & 58)以從該積體電路(IC)外部之一裝置接收一輸入安全密鑰；

比較電路(38)，該比較電路的一第一輸入端係耦合至該儲存電路(30)，一第二輸入端係耦合至該IC偵錯介面(52)，及一輸出端係用於提供基於該輸入安全密鑰及該所儲存之IC安全密鑰之一保護啟用信號(46)；以及

存取保護電路(40)，其耦合至該受保護型功能電路(12)，並且該存取保護電路的一輸入端係用於接收該保護啟用信號，當該保護啟用信號為無效時，該存取保護電路允許該偵錯連接埠對該受保護型功能電路(12)之存取。

2. 如申請專利範圍第1項之積體電路(IC)，其中該比較電路(38)提供該保護啟用信號，以響應比較該所儲存之IC安全密鑰與透過該IC偵錯介面所接收的該輸入IC安全密鑰。

3. 如申請專利範圍第1項之積體電路(IC)，其中該IC偵錯

介面及該存取保護電路依據該保護啟用信號，以選擇性允許介於複數個IC偵錯端子與該受保護型功能電路之間的通訊。

4. 如申請專利範圍第1項之積體電路(IC)，其中該偵錯連接埠進一步包括一識別符儲存電路(32)，其耦合至該IC偵錯介面以儲存一IC識別符。
5. 如申請專利範圍第4項之積體電路(IC)，其中該偵錯連接埠係在該IC偵錯介面處接收該輸入安全密鑰之前，經由該IC偵錯介面提供該IC外部之該IC識別符。
6. 如申請專利範圍第1項之積體電路(IC)，進一步包括用於儲存一強制啟用值之強制啟用電路(45)，該強制啟用電路係耦合至該比較電路，其中如果該強制啟用值具有一第一狀態，則該存取保護電路允許介於該IC偵錯介面與該受保護型功能電路之間的通訊，並且如果該強制啟用值具有一第二狀態，則該存取保護電路依據該保護啟用信號，以選擇性允許介於該IC偵錯介面與該受保護型功能電路之間的通訊。
7. 一種用於在一積體電路(IC) (10)提供安全保護之方法，該積體電路(IC)具有受保護型功能電路(12)，該方法包括：

從該積體電路(IC)提供一IC識別符；

回應提供該IC識別符，在該積體電路(IC)處接收一輸入IC安全密鑰，其中該輸入IC安全密鑰係藉由該積體電路(IC)外部之一偵錯裝置而提供，且其中在提供

該輸入 IC 安全密鑰之前，該偵錯裝置評估一組 IC 識別符及相對應之 IC 安全密鑰值以決定該輸入 IC 安全密鑰；

在該積體電路 (IC) 中，比較該輸入 IC 安全密鑰與一儲存之 IC 安全密鑰；以及

回應該比較步驟，在該積體電路 (IC) 中選擇性地致能對受保護型功能電路之存取。

8. 一種用於在一積體電路 (IC) 提供安全保護之方法，該積體電路 (IC) 具有受保護型功能電路及一 JTAG 介面，該方法包括：

在一第一 JTAG 狀態中，經由該 JTAG 介面接收一使用者定義之指令 (201)；

在一第二 JTAG 狀態中，經由該 JTAG 介面接收一輸入 IC 安全密鑰，其中該輸入 IC 安全密鑰係藉由該積體電路 (IC) 外部之一偵錯裝置而提供，並且其中在提供該輸入 IC 安全密鑰之前，該偵錯裝置評估一組 IC 識別符及相對應之 IC 安全密鑰值以決定該輸入 IC 安全密鑰，及在該積體電路 (IC) 中比較該輸入 IC 安全密鑰與一所儲存之 IC 安全密鑰 (106, 108)；以及

選擇性致能經由該 JTAG 介面存取該受保護型功能電路 (112, 116)。

9. 如申請專利範圍第 8 項之方法，其中該第一 JTAG 狀態 (201) 相當於一 SHIFT_IR 狀態。

10. 一種用於在一積體電路 (IC) 提供安全保護之方法，該積

體電路(IC)具有受保護型功能電路，比較電路及耦合至該受保護型功能電路之至少一IC端子，該方法包括：

從該積體電路(IC)提供一IC識別符；

回應提供該IC識別符，在該積體電路(IC)處接收一輸入IC安全密鑰，其中該輸入安全密鑰係藉由該積體電路(IC)外部之一偵錯裝置而提供，且其中在提供該輸入安全密鑰之前，該偵錯裝置評估一組IC識別符及相對應之IC安全密鑰值以決定該輸入IC安全密鑰；

經由該至少一IC端子存取該受保護型功能電路；

程式規劃一強制啟用指示符以啟用比較電路，其中該比較電路比較一輸入IC安全密鑰與一所儲存之IC安全密鑰，並且回應該比較，選擇性啟用經由該至少一IC端子存取該受保護型功能電路。