



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201518985 A

(43)公開日：中華民國 104 (2015) 年 05 月 16 日

(21)申請案號：103126976

(22)申請日：中華民國 103 (2014) 年 08 月 06 日

(51)Int. Cl.：

G06F21/44 (2013.01)**H04L9/32 (2006.01)****H04L9/08 (2006.01)**

(30)優先權：2013/08/06

美國

61/862,798

(71)申請人：歐樂岡科技公司 (列支敦斯登) OLOGN TECHNOLOGIES AG (LI)

列支敦斯登

(72)發明人：伊納貞克 瑟吉 IGNATCHENKO, SERGEY (CA)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：28 項 圖式數：3 共 31 頁

(54)名稱

用於避免一器件之未經授權的仿製之系統、方法及裝置

SYSTEMS, METHODS AND APPARATUSES FOR PREVENTION OF UNAUTHORIZED CLONING OF A DEVICE

(57)摘要

本發明可提供一種自我鑑認器件及一種用於鑑認該自我鑑認器件之方法。在一態樣中，一器件可包括一感測電路，該感測電路可包括待量測之一電路。該感測電路可使用待量測之該電路來產生對於該器件之一或多個物理性質的量測資料。該器件可進一步包括一儲存器，以儲存含有自該量測資料導出之鑑認資料之一真偽憑證；及一通信埠，以經由耦合至該通信埠之一鏈路使該真偽憑證及該量測資料與一通信合作夥伴通信。

A self-authenticating device and a method for authenticating the self-authenticating device may be provided. In one aspect, a device may comprise a sensing circuit, which may comprise a circuit to be measured. The sensing circuit may generate measurement data for one or more physical properties of the device using the circuit to be measured. The device may further comprise a storage to store an authenticity certificate that contains authentication data derived from the measurement data and a communication port to communicate the authenticity certificate and measurement data with a communication partner via a link coupled to the communication port.

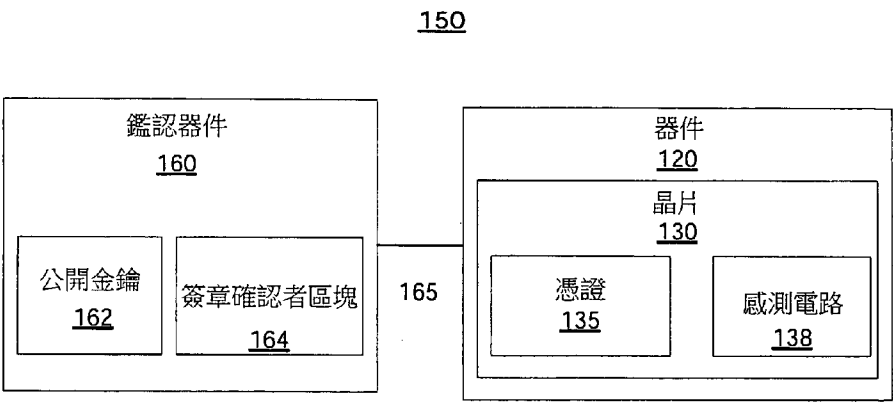


圖1B

- 120 . . . 器件/敏感器件
- 130 . . . 晶片/測試晶片
- 135 . . . 真偽憑證
- 138 . . . 感測電路
- 150 . . . 系統
- 160 . . . 鑑認器件
- 162 . . . 公開金鑰/金鑰
- 164 . . . 簽章確認者區塊
- 165 . . . 鏈路/連接

201518985

發明摘要

※ 申請案號：103126976

※ 申請日：103.8.6

※IPC 分類：G06F 21/44 (2013.01)
H04L 9/32 (2006.01)
H04L 9/68 (2006.01)

【發明名稱】

用於避免一器件之未經授權的仿製之系統、方法及裝置

SYSTEMS, METHODS AND APPARATUSES FOR PREVENTION
OF UNAUTHORIZED CLONING OF A DEVICE

● 【中文】

本發明可提供一種自我鑑認器件及一種用於鑑認該自我鑑認器件之方法。在一態樣中，一器件可包括一感測電路，該感測電路可包括待量測之一電路。該感測電路可使用待量測之該電路來產生對於該器件之一或多個物理性質的量測資料。該器件可進一步包括一儲存器，以儲存含有自該量測資料導出之鑑認資料之一真偽憑證；及一通信埠，以經由耦合至該通信埠之一鏈路使該真偽憑證及該量測資料與一通信合作夥伴通信。

● 【英文】

A self-authenticating device and a method for authenticating the self-authenticating device may be provided. In one aspect, a device may comprise a sensing circuit, which may comprise a circuit to be measured. The sensing circuit may generate measurement data for one or more physical properties of the device using the circuit to be measured. The device may further comprise a storage to store an authenticity certificate that contains authentication data derived from the measurement data and a communication port to communicate the authenticity certificate and measurement data with a communication partner via a link coupled to the communication port.

【代表圖】

【本案指定代表圖】：第（1B）圖。

【本代表圖之符號簡單說明】：

120	器件/敏感器件
130	晶片/測試晶片
135	真偽憑證
138	感測電路
150	系統
160	鑑認器件
162	公開金鑰/金鑰
164	簽章確認者區塊
165	鏈路/連接

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】

用於避免一器件之未經授權的仿製之系統、方法及裝置

SYSTEMS, METHODS AND APPARATUSES FOR PREVENTION
OF UNAUTHORIZED CLONING OF A DEVICE

相關申請案交叉參考

本申請案主張2013年8月06日申請之名為「Systems, Methods and Apparatuses for Prevention of Unauthorized Cloning of a Device」之美國臨時申請案第61/862,798號之優先權，該案之全文以引用的方式併入本文中。

【技術領域】

本文中所描述之系統、方法及裝置係關於一器件之鑑認。

【先前技術】

電子器件之仿製係一眾所周知的關注問題。例如，反向工程可應用於許多電子器件以判定該等器件之組件及組態。在該反向工程處理程序期間，封裝半導體晶片常常被除去封裝且其等電路布局經曝露。用於控制該等電子器件之軟體亦並未免受反向工程之害。因此，藉由反向工程獲得之資訊，全部電子器件經受仿製。

然而，對於許多電子器件而言易受仿製影響並非所要的。非法仿製不僅可使智慧財產處於被盜取之風險，亦可用於引起安全性的嚴重破壞。例如，一電子器件可用於傳遞財務資訊或可用於存取對一限制區之控制。在此等情境中，若非法仿製電子器件，則該非法複製品可用於在未經授權之情況下傳遞財務資訊或獲得對一限制區之存取。

因此，技術中需要對抗一電子器件之未經授權的仿製之保護。

【圖式簡單說明】

圖1A係根據本發明之一例示性系統之一方塊圖。

圖1B係根據本發明之另一例示性系統之一方塊圖。

圖1C、圖1D、圖1E、圖1F及圖1G係根據本發明之例示性感測電路之方塊圖。

圖2係繪示根據本發明之用於產生一電子晶片之一例示性處理程序之一流程圖。

圖3係繪示根據本發明之用於待鑑認之一器件之一例示性處理程序之一流程圖。

【實施方式】

本文中結合以下描述及附圖描述根據本發明之系統、裝置及方法之某些闡釋性態樣。然而，此等態樣係指示其中可採用本發明之原理之各種方式之僅一些且本發明意欲包含全部此等態樣及其等等效物。當結合圖式考量時可自以下詳細描述明白本發明之其他優點及新穎特徵。

在以下詳細描述中，闡述許多特定細節以提供對本發明之透徹理解。在其他例項中，未詳細展示熟知結構、介面及處理程序以避免模糊本發明。然而，一般技術者將明白，本文中所揭示之該等特定細節並不需要用於實踐本發明且並不表示對本發明之範疇之一限制(惟如申請專利範圍中所敘述之除外)。預期本說明書之任一部分皆不解釋為實現本發明之完整範疇之任何部分之一否定。儘管描述本發明之某些實施例，然此等實施例同樣並不意欲限制本發明之完整範疇。

本發明提供用於判定一器件之真偽之系統、方法及裝置。在一非限制性實例中，根據本發明之一器件可包括一晶片。該晶片可包括用於儲存一真偽憑證之一儲存器及用於產生對於該晶片之一或多個物理性質之量測資料之一感測電路。該真偽憑證可含有藉由一鑑認器件

簽署之量測資料。

在另一非限制性實例中，根據本發明之一簽章者器件可包括用於儲存一私密金鑰及一簽署區塊之一儲存器。該簽章者器件可經組態以在一初始化處理程序期間建置至待鑑認之一器件(例如，一晶片)之一連接、自該器件收集量測資料、自該經收集量測資料產生一真偽憑證及發送該所產生之真偽憑證至該器件以用於儲存。在一些實施例中，簽章者器件可使用一電路(諸如一ASIC)實施且經組態於硬體中以執行以上功能。在一些其他實施例中，可使用藉由軟體指令組態之一通用電腦處理器實施簽章者器件。在又一些其他實施例中，可藉由硬體及/或軟體之任何組合來實施簽章者器件。

在另一非限制性實例中，根據本發明之一鑑認器件可包括用於儲存一公開金鑰及一簽章確認區塊之一儲存器。該鑑認器件可經組態以在一鑑認處理程序期間連接至待鑑認之一器件(例如，一晶片)、自該器件獲得一真偽憑證、確認該真偽憑證之簽章、自該器件收集量測資料、比較該所收集之量測資料與該真偽憑證中之鑑認資料及判定該器件是否真實。在一些實施例中，鑑認器件可使用一電路(諸如一ASIC)實施且經組態於硬體中以執行以上功能。在一些其他實施例中，可使用藉由軟體指令組態之一通用電腦處理器實施鑑認器件。在又一些其他實施例中，可藉由硬體及/或軟體之任何組合來實施鑑認器件。

圖1A展示根據本發明之一例示性系統100。該系統100可包括一簽章者器件110及一晶片130。該簽章者器件110可包括儲存一私密金鑰112及一簽署區塊114之一儲存器。該儲存器可為(例如)一可擦除可程式化唯讀記憶體(EPROM)、快閃記憶體、一硬碟機(HDD)等。在一些實施例中，可基於藉由可信平台模組提供之一「密封儲存」來實施該私密金鑰儲存器，該可信平台模組係定義於2007年8月由可信計算

聯盟 (TCG) 發表之「TCG Specification Architecture Overview Specification Revision 1.4」中，其之全文以引用的方式併入。可藉由簽署區塊114使用私密金鑰112以如本文中所描述般簽署資料。在一非限制性實例中，私密金鑰112可為一RSA金鑰、一橢圓曲線密碼編譯(ECC)金鑰或此項技術中已知或未來將開發之用於任何公開/私密密碼編譯演算法之任何其他私密金鑰。簽署區塊114可為能夠執行加密及/或簽署操作之硬體及/或軟體之任何組合。非限制性實例包含運行適當軟體之一或多個ASIC、FPGA、SoC或微處理器或微控制器。

晶片130可包括一感測電路138及用於儲存一真偽憑證135之一儲存器。在一些實施例中，真偽憑證135可儲存於一晶片上可程式化非揮發性記憶體(諸如一PROM、EPROM、EEPROM、快閃記憶體等)中。在一些其他實施例中，真偽憑證135可儲存於晶片130之外。例如，真偽憑證135可儲存於裝載(hosting)晶片130之一器件(諸如圖1B中所展示之器件120)上。在此等實施例之另一實例中，真偽憑證135可儲存於一外部資料庫(未展示)中且(例如)藉由一晶片序列號識別。該晶片序列號(例如)可儲存於晶片130上或器件120中。

感測電路138可用於量測晶片之一或多個物理性質，舉例而言，諸如特定MOSFET電晶體或若干特定MOSFET電晶體之洩漏電流、一特定路徑上之延遲、在特定操作期間藉由一特定電路消耗之電力等等。在一初始化處理程序期間可藉由簽章者器件110之簽署區塊114使用金鑰112來簽署量測資料。該簽署處理程序可產生基於該量測資料或自該量測資料導出之一結果且該結果可經保存作為真偽憑證135。

可藉由一鏈路115連接晶片130及簽章者器件110。該鏈路115可為任何合適類型之連接(諸如有線連接、無線連接等)。有線連接可為(例如)一IEEE 1194.1 (JTAG TAP)介面、系統管理匯流排(SMBus)、I²C匯流排，但任何其他連接亦合適。例如，基於當前可用技術之一串聯或

並聯連接(諸如USB、IEEE 1394、RJ-45等)或未來將開發之其他連接類型亦可用作有線連接。無線連接可為當前可用之任何無線通信(諸如NFC、藍芽、WiFi、無線電等)或未來將開發之任何無線通信。儘管未展示，然晶片130及簽章者器件110可分別包括用於鏈路115之適當通信埠。

圖1B展示根據本發明之一例示性系統150。該系統150可包括一鑑認器件160及待鑑認之一器件120。該鑑認器件160可包括儲存一公開金鑰162及一簽章確認者區塊164之一儲存器。該儲存器可為(例如)一可擦除可程式化唯讀記憶體(EPROM)、一快閃記憶體、硬碟機(HDD)等。金鑰162可為對應於一簽章者器件110之一私密金鑰112之一公開金鑰使得可使用該公開金鑰162驗證使用該私密金鑰112產生之任何簽章。可藉由簽章確認者區塊164執行簽章鑑認。該簽章確認者區塊164可為能夠執行解密及/或簽章確認操作之硬體及/或軟體之任何組合。非限制性實例包含運行適當軟體之一或多個ASIC、FPGA、SoC或微處理器或微控制器。

器件120可包括如圖1A中所展示之晶片之一晶片130。可藉由一鏈路165連接該器件120及鑑認器件160。該鏈路165可類似於鏈路115且可為任何合適類型之連接(諸如有線連接、無線連接等)。有線連接可為(例如)一IEEE 1194.1 (JTAG TAP)介面、SMBus、I²C匯流排，但任何其他連接亦合適。例如，基於當前可用技術之一串聯或並聯連接(諸如USB、IEEE 1394、RJ-45等)或未來將開發之其他連接類型亦可用作有線連接。無線連接可為當前可用之任何無線通信(諸如NFC、藍芽、WiFi、無線電等)或未來將開發之任何無線通信。儘管未展示，然器件120及鑑認器件160可分別包括用於鏈路165之適當通信埠。

在一些實施例中，鏈路115及165可為相同種類之連接。例如，器

件120可具有直接映射至晶片130之通信埠之用於外部連接之一通信埠。即，器件120可具有與晶片130之通信埠相同之一通信埠，其中各接針或插口連結至該晶片130之一對應接針或插口。在一些其他實施例中，鏈路115及165可為不同種類之連接。例如，器件120可具有在晶片130與其用於鏈路165之通信埠之間的電路，該等電路操縱或轉換處理中(on the way)的資料至晶片130，或操縱或轉換來自晶片130之處理中的資料。

在一些實施例中，器件120可用於敏感性任務(例如，財務交易、存取控制、醫學測試設備等)中，且在使用期間可能需要經鑑認。一鑑認器件160及一敏感器件120之實例分別包含：一終端及一存取卡；一關鍵任務系統(舉例而言，諸如一飛機)及用於此一系統之一控制區塊；一醫學器件及該醫學器件之一可替代組件等。

簽章者器件110可為藉由一授權方使用以初始化晶片130之一器件。在一些實施例中，可在製造晶片130之處理程序期間執行初始化處理程序。例如，簽章者器件110可為晶片製程期間使用之自動測試設備(ATE)的一部分。在一些其他實施例中，可在將晶片130放於器件120中之後執行初始化處理程序。無論作為一獨立器件或作為一ATE之部分，簽章者器件110皆可實施於硬體、軟體或硬體及軟體之一組合中。

儘管未展示，然器件120、簽章者器件110及鑑認器件160之各者可進一步包含經組態以執行一些或全部功能性之硬體及/或軟體元件。該等硬體元件可包含電子電路，諸如中央處理單元、微處理器、微控制器、場可程式化閘極陣列(FPGA)、特定應用積體電路(ASIC)、晶片上系統(SoC)或其等之任何組合。在一些實施例中，本文中所描述之功能性可實施於硬體組態中。在一些其他實施例中，該等電路可經組態以執行實施本文中所描述之功能性的軟體模組。在又

一些其他實施例中，可藉由硬體及軟體之一組合來實施本文中所描述之功能性。

如圖1C中所展示，感測電路138可包括待量測之一電路181及一量測電路182。可藉由待量測之該電路181產生「原始資料」。該量測電路182可為經組態以量測及視需要處理該原始資料以產生量測資料之一電路。該量測資料可表示為電信號(例如，表示為數位電信號)。在一些實施例中，原始資料亦可表示及解譯為電信號。在一些其他實施例中，可藉由一些其他構件表示原始資料。例如，在一例示性實施例中，原始資料可為在待量測之電路181執行一預定義操作時藉由該電路產生之熱量或藉由該電路達到之溫度，且可藉由一溫度感測器(該溫度感測器可為量測電路182之一部分)量測此原始資料以產生量測資料。

在一些實施例中，待量測之電路181可為出於一些其他目的而已存在於晶片130上之一電子電路。在一些其他實施例中，電路181可出於量測目的而特殊構造於晶片130上。在一些實施例中，待量測之電路181可如晶片130之預定部位處之一電路點般簡單。在一些實施例中，若藉由電信號表示原始資料，則量測電路182可如自該原始資料產生一輸出信號之一或多個導線般簡單。

存在實施感測電路138之各種方式。在本文中描述用於實施感測電路138之一些實例但其等僅為例示性而非詳盡的。此外，儘管術語感測電路138係用作一單數術語，然晶片130可包括用於該晶片130之不同部位處之不同物理性質及/或相同物理性質之複數個感測電路。

亦應注意，在圖1A及圖1B上感測電路138係經展示為晶片130之部分。然而，在一些實施例中，如量測電路182之一量測電路可實施於簽章者器件110及/或鑑認器件160上。在該等實施例中，可藉由該簽章者器件110及/或該鑑認器件160上之該量測電路產生量測資料。

在一些實施例中，若藉由電信號表示原始資料，則晶片130及器件120可包括一額外連接器介面，該連接器介面將該原始資料自待量測之電路181提供至其他器件(諸如鑑認器件160或簽章者器件110)。因此，一簽章者器件110或鑑認器件160可使用經由鏈路115或165獲得之量測資料或可使用直接來自此額外連接器介面之資料。在此等實施例之一些實施例中，鑑認器件160可執行待量測之電路181之兩個量測之間之一比較。可藉由晶片上量測電路182進行一量測且經由鏈路165獲得量測資料。可藉由鑑認器件160中之一量測電路進行另一量測，該量測電路可經由額外連接器介面自待量測之電路181獲得原始資料。若來自此兩個量測之資料不合理地不同於彼此，則鑑認器件160可判定晶片130且因此器件120並不真實。在一些實施例中，該兩個量測可近似同時進行。此外，在一些實施例中，量測電路182及/或鑑認器件160中之量測電路可經校準以補償該等量測電路中之系統誤差。

在一非限制性實例中，晶片130可包括複數個感測電路138。在具有複數個感測電路138之實施例中，對於該等感測電路之一些，待量測之電路181及量測電路182兩者皆可實施於晶片130上，而對於該等感測電路之其他者，待量測之電路181可實施於晶片130上且量測電路182可實施於簽章者器件110及/或鑑認器件160上。

圖1D展示感測電路138之一例示性實施方案。此例示性實施方案可稱為感測電路138A，該感測電路138A可包括待量測之一電路181A及一量測電路182A。在一非限制性實例中，待量測之物理性質可為一輸入時脈之一邊緣與待量測之電路181A之輸出之一者之一邊緣之間之一延遲。該輸入時脈在圖1D中標記為「CLK」且可饋送至待量測之電路181A及量測電路182A兩者。在一些實施例中，在當前時脈週期中變化之至待量測之電路181A之任何輸入可用作圖1D上之輸入「CLK」。

在一實施例中，可(例如)藉由比較待量測之電路181A之延遲與一變流器(或中繼器)鏈之一延遲來量測延遲。例如，量測電路182A可包括預定數目個變流器或中繼器之一鏈186、一比較器188及一正反器190。該比較器188可具有兩個輸入端：一者連接至變流器或中繼器之該鏈186之一輸出，且另一者連接至待量測之電路181A之一輸出。待量測之電路181A之此輸出可沿著與當前時脈週期內之輸入時脈相同之方向改變。比較器188可產生指示待量測之電路181A中之延遲長度之一輸出。在一非限制性實施例中，比較器188可為一XOR邏輯閘。該XOR邏輯閘可對變流器(或中繼器)之鏈之輸出與待量測之電路181A之輸出執行xor運算。該經xor之結果可連接至正反器190之時脈輸入以看看是否已發生足夠長以引起該正反器190觸發之一靜態冒險。是否觸發正反器190可指示透過電路181A之延遲是否在透過變流器之鏈186之延遲之一時段 d_T 內，其中 d_T 係足以觸發正反器190之時間。在一些實施例中，可針對變流器或中繼器鏈之不同長度重複相同量測以獲得更多資訊。應注意，在一些實施例中，可以一類似方式利用動態冒險。

如本文中所使用，一冒險可係指其中輸入變量之變化歸因於一些延遲形式而引起輸出之一臨時變化之一現象。例如，一靜態冒險可發生，此係因為兩個信號路徑具有不同延遲且該冒險之長度可大致等於沿著該兩個路徑之延遲之差。在一非限制性實施例中，第一路徑可為經由電路181A之路徑且第二路徑可為經由變流器/中繼器之鏈之路徑。正反器是否已觸發可指示冒險是否足夠長以觸發該正反器，且因此可用於有效地判定兩個路徑之間之延遲之差是否大於或小於一常數(即，觸發正反器之臨限值差)。

圖1E繪示用於量測延遲之另一實施例。在此實施例中，一感測電路138B可包括待量測之一電路181B及一量測電路182B。該量測電

路182B可包括一電流源183、一電容器C、一取樣保持電路184及一電壓量測電路185。可藉由使用待量測之電路181B之輸入時脈來量測延遲以控制電流源183使得該電流源可僅在一CLK信號到達之後產生電流。藉由電流源183產生之該電流可用於給電容器C充電。待量測之電路181B之一輸出可用於控制取樣保持電路184，該取樣保持電路184可在待量測之該電路181B之該輸出改變時之時間取樣電容器C上之電壓。在此實施例中，電壓量測電路185可耦合至取樣保持電路184之一輸出。可量測該取樣保持電路184之該輸出處之電壓以判定待量測之電路181B之延遲。

在一些實施例中，用於量測電路181A或181B中之延遲之一量測電路可實施於一簽章者器件110上或於一鑑認器件160上。在此等實施例中，可(例如)在一輸入時脈之一邊緣與晶片130之輸出接針之一者之一邊緣之間執行量測。

對於感測電路138之另一非限制性實施方案係繪示於圖1F中。如圖1F中所展示，一感測電路138C可包括待量測之一電路181C及一量測電路182C。當執行一量測時，量測電路182C可使待量測之電路181C之輸入與一規則輸入I切斷連接，且接著量測待量測之該電路181C之輸入上之洩漏電流。例如，量測電路182C可量測來自待量測之電路181C之輸入之一MOSFET洩漏電流。可(例如)藉由切換器S實現該切斷連接。在一些實施例中，可對待量測之電路181C之一個以上輸入執行量測。在一些實施例中，用於量測洩漏電流之一量測電路可實施於簽章者器件110或鑑認器件160上。在此等實施例中，可(例如)對晶片130之輸入之一或多者執行洩漏電流之量測。

在一非限制性實例中，可如2012年《IEEE International Conference on Microelectronic Test Structures (ICMTS)》，Kumagai, Y. 等人之「Test Circuit for Extremely Low Gate Leakage Current

Measurement of 10 aA for 80,000 MOSFETs in 80s」(其全文以引用的方式併入本文中)中所描述般量測洩漏電流。亦可使用此項技術中已知或未來將開發之量測洩漏電流的其他方法。

用於感測電路138之另一例示性實施方案係繪示於圖1G中。如圖1G中所展示，一感測電路138D可包括一電阻器R、待量測之一電路181D及一量測電路182D。一電壓供應源Vcc可施加至該電阻器R。該量測電路182D可量測待量測之該電路181D的電力消耗。在一非限制性實例中，可藉由量測跨電阻器R之電壓差來量測電力消耗。在一些實施例中，電阻器R可置於電路181D與接地(GND)連接器之間。亦可使用此項技術中已知或未來將開發之電力消耗量測的其他實施方案。

在一些實施例中，可在待量測之電路181D閒置時，量測電力消耗。在一些其他實施例中，可在藉由待量測之電路181D執行一預定義任務時，量測電力消耗。

在一些實施例中，用於量測電力消耗之一量測電路可實施於簽章者器件110上或於鑑認器件160上。在此等實施例中，可(例如)對晶片130之電力供應接針之一或多者執行量測。

在一些實施例中，待藉由感測電路138量測之一物理性質可為由一晶片上振盪器產生之頻率。例如，待量測之電路181可包括一振盪器(舉例而言，諸如多諧振盪器或環式振盪器)。在一些實施例中，該振盪器可為熱穩定及/或電壓穩定。量測電路可量測由該振盪器產生之頻率。例如，若藉由晶片130上之量測電路182來量測振盪器頻率，則該晶片130可使用一外部或內部時脈作為一參考基礎以執行該頻率量測。

在一些實施例中，待量測之物理性質可為在待量測之電路181執行可為(例如)一預定義複雜計算之一預定義任務之後在一特定實體點處之一溫度變化。在此等實施例中，量測電路182可包括量測在執行

任務之前及之後在一特定點(該特定點可定位於待量測之電路181附近)處之溫度之一溫度感測器。在一些實施例中，該溫度感測器可(例如)作為一晶片上單元而定位於晶片130內。在一些其他實施例中，一量測電路可定位於一簽章者器件110及/或鑑認器件160內以接收及處理來自此一溫度感測器之原始資料。

在一些實施例中，可考量環境資訊作為影響一經量測之物理性質之因素。例示性環境資訊可包含溫度及/或電壓資訊。該電壓資訊可包括各種電壓，諸如電力供應電壓 V_{cc} 、反向偏壓電壓等。在一非限制性實例中，若經量測之物理性質係振盪器頻率，則在初始化處理程序期間，一簽章者器件110可收集對於振盪器頻率、溫度及/或電壓資料之量測，簽署該所收集之量測資料及將該經簽署之資料儲存作為真偽憑證135之部分。當一鑑認器件160執行鑑認時，其可自晶片130收集當前溫度及/或電壓資料及自真偽憑證135獲得所儲存之溫度及/或電壓資料，且使用一預定振盪器頻率-溫度曲線及/或頻率-電壓曲線以在比較當前量測之頻率及所儲存之頻率之前將其等正規化。

如本文中所使用之正規化可係指根據一或多個已知因素處理一經量測之資料點之技術。例如，振盪器頻率可取決於溫度及電壓。該相依關係可在一預定振盪器頻率-溫度曲線及/或頻率-電壓曲線中提供。此等曲線可(例如)藉由在複數個測試晶片130上之量測而獲得或基於振盪器頻率對溫度或電壓之已知相依性而計算，且可儲存於(例如)鑑認器件160內。替代性地，此等曲線可儲存於一些其他部位處但在需要時可用於鑑認器件160。

在一些實施例中，簽章者器件110可儲存針對某預定義溫度及/或電壓正規化之振盪器頻率，而非在初始化處理程序期間儲存所收集之溫度及/或電壓作為真偽憑證之一部分。因此，在鑑認處理程序期間，鑑認器件160可比較一正規化之當前收集之振盪器頻率資料與儲

存於真偽憑證135內之振盪頻率資料。

在一些實施例中，一正規化技術亦可應用於藉由感測電路138量測之其他物理性質以降低環境因素(諸如溫度、電壓及/或操作頻率)之效應。此外，在一些實施例中，可在施加至晶片130上之相關電路之不同環境參數(諸如電壓、操作頻率或溫度)之情況下若干次收集如本文中所描述之任何量測資料。在一些實施例中，此等環境參數(諸如操作頻率或電壓)之一些可在外部供應或可根據來自簽章者器件110及/或鑑認器件160之指令而在晶片130內產生。

應注意，在一些實施例中，感測電路138可組合上文所描述之用於相同或不同物理性質之一個以上感測電路。例如，可存在針對溫度及電壓之不同感測電路及/或針對晶片130上之不同位置處之電壓之不同感測電路。

圖2係繪示根據本發明之一實施例之一例示性方法200之一流程圖。該方法200展示一晶片130之一初始化處理程序。應注意，如本文中所描述之該初始化處理程序可藉由一簽章者器件110執行。在一些實施例中，可在將晶片130放於器件120中之前執行初始化處理程序。

在方塊210處，製造一晶片。舉一非限制性實例，一晶片130可製造為一ASIC或一VLSI。在另一非限制性實例中，可藉由程式化一FPGA來產生一晶片130。

在方塊220處，該晶片可(例如)經由鏈路115連接至一簽章者器件110。可(例如)就在製造該晶片之後執行此方塊。在一些實施例中，該方塊220可結合一ASIC/VLSI測試作為製程之一部分。

在方塊230處，可自晶片收集量測資料。例如，晶片130之感測電路138可產生對於一或多個物理性質之量測資料。如本文中所描述，該量測可取決於感測電路138中之感測組件之類型。

在方塊240處，可從自晶片收集之量測資料製備鑑認資料。在一

些實施例中，鑑認資料可包含從自晶片130之感測電路138收集之量測資料導出之資訊。例如，在一非限制性實施例中，一預期範圍之值(而非一絕對值)可用作一鑑認資料之一部分。此一範圍可考量歸因於在真偽驗證期間觀察之環境參數對在晶片初始化期間觀察之環境參數之所允許之變化之預期變動。在另一非限制性實施例中，全部可能值之範圍可分成一組子範圍，且可將一經量測值所屬於之一子範圍指定為鑑認資料之一部分。

在方塊245處，可藉由簽章者器件110簽署經製備之鑑認資料以形成一真偽憑證135。簽章者器件110可使用金鑰112及簽署區塊114以用於簽署經製備之鑑認資料。在一些實施例中，真偽憑證135亦可包含除經製備之鑑認資料之外之資訊(舉例而言，諸如製造者id、晶片類型、晶片所允許之用途等)。

在方塊250處，可將簽章者器件110中產生之真偽憑證發送至晶片以用於儲存。因此，根據本發明之各晶片130可具有基於來自該晶片之感測電路138之量測資料及藉由一簽章者器件110之一私密金鑰112簽署之其自身之真偽憑證135。可將晶片130放於一器件120中以鑑認該器件120。應注意，在一些實施例中，可在執行此初始化處理程序200之前首先將一晶片130放於一器件120中。在該等實施例中，至晶片130之連接可透過器件120之一連接器(諸如圖2之鏈路165)。

圖3係繪示用於使用一鑑認器件160驗證一晶片130之真偽之一例示性方法300之一流程圖。因為在鑑認期間藉由器件120裝載晶片130，所以當該晶片130真實時可判定該器件120為真實的。在方塊310處，鑑認器件160可連接至器件120。該連接可為(例如)圖1B中所展示之連接165。在方塊320處，鑑認器件165可自器件120之晶片130獲得真偽憑證135。可(例如)透過連接165獲得該真偽憑證135。

在方塊325處，可驗證真偽憑證135。例如，可使用公開金鑰162

驗證真偽憑證135，該公開金鑰162對應於簽章者器件110之私密金鑰112。可將該公開金鑰162儲存於鑑認器件160處或透過一可信第三方使該公開金鑰162可用於該鑑認器件160。在一些實施例中，鑑認器件160可儲存一根憑證及使用PKI簽章驗證程序以驗證真偽憑證135。該根憑證可為(例如)來自一憑證授權中心(CA)之一憑證。若真偽憑證135並不有效，則鑑認器件160可判定晶片130及/或器件120並不真實。若真偽憑證有效，則該方法可繼續進行至方塊330。

在方塊330處，鑑認器件160可自晶片130之感測電路138收集當前量測資料。

在方塊340處，鑑認器件160可比較當前量測資料與自真偽憑證135獲得之鑑認資料。如本文中所描述，在一些實施例中，此一比較可考量來自當前量測之結果與自真偽憑證獲得之結果之間之潛在差異。在一些實施例中，量測值之一「預期範圍」可經預定義，且在此等實施例之一些實施例中，此一預期範圍可為真偽憑證之一部分。

在一些實施例中，鑑認器件160是否認為該比較為成功的可取決於全部感測電路是否產生在其等各自預期範圍內之資料。在一些實施例中，可在真偽憑證135中之資料中指定範圍或自真偽憑證135中之該資料導出該等範圍。在一些其他實施例中，鑑認器件160是否認為一比較為成功的可取決於預定數目個感測電路是否產生預期範圍內之量測資料。

在一些其他實施例中，一比較是否成功之決定可基於指派至各感測電路或各類型之感測電路之權重。例如，可將用於產生其等各自預期範圍內之量測資料之感測電路之權重加在一起，且該總和可與一預定義之總權重臨限值比較。若該總和通過了該總權重臨限值，則可判定比較為成功的。應注意，在一些實施例中，對於相同感測電路可存在兩個不同權重：用於產生範圍內之量測資料之一權重及用於產生

該範圍外之量測資料之另一權重。例如，若一電壓量測係在一預期範圍內，則一正權重(例如，10)可增加至總和，但若該電壓量測係在該預期範圍外，則大於該正權重達一數量級之一負權重(例如，100)可增加至該總和以減小該總和。在一些進一步實施例中，權重可取決於經量測值與一預期值差多少而不同。例如，若在上文實例中電壓量測係在預期範圍之界限處，則沒有權重(例如，零)可增加至總和。

在一些其他實施例中，可基於測試當前量測資料對應於自真偽憑證135獲得之鑑認資料之一統計假設而判定一比較是否為成功的。例如，藉由一特定感測電路產生之量測資料可具有一誤差分佈。可(例如)藉由多次測試感測電路、藉由理論推理或藉由任何其他合適方法來獲得此一誤差分佈。應注意，一般而言藉由不同感測電路產生之資料可具有不同誤差分佈。在一些實施例中，可使關於此誤差分佈之資訊可用於鑑認器件160。例如，誤差分佈資訊可為儲存於真偽憑證135內部之資訊之一部分，或可預載入至鑑認器件160，或可在比較處理程序期間藉由該鑑認器件160獲取(例如，自一外部源(諸如網際網路)載入等)。藉由該誤差分佈資訊，可基於來自真偽憑證135之量測資料之值與來自當前量測之一結果之間之差異來計算晶片130真實之概率。在一些實施例中，可使用一預定義臨限值使得若一經計算之概率小於該臨限值則鑑認器件160可認為一晶片不真實。該預定義臨限值可為0.8、0.9、0.95、0.98、0.99等且可基於概率計算中所涉及之物理性質而予以定義。

應注意，存在測試一假設之許多方式。例如，在一實施例中，可使用一卡方方法。在此實施例中，可使用N個感測電路(其中N係一或更大)且真偽憑證135可含有N個值。在方塊320處，可藉由鑑認器件160收集N個當前量測結果。在方塊340處，可執行一假設評估，其中鑑認器件160可將真偽憑證135中之N個值之各者視為一預期值，及將

一各自當前量測結果視為一觀察值。接著，可針對N個量測結果計算一卡方值(舉例而言，諸如皮爾森(Pearson)之累積測試統計值)。接著，該卡方統計值可用於計算一概率，該概率可稱為如此項技術中已知之一「p值」。

在方塊350處，可藉由鑑認器件160判定晶片130及/或器件120是否真實。例如，若在方塊340中之比較係成功的，則可認為晶片130及/或器件120真實。否則，可認為不真實。亦應注意，上文所描述之方法可一起使用。例如，在一實施例中，為判定一晶片是否真實，鑑認器件160可應用一「預期範圍」方法至與一些數目個感測電路有關之資料，且應用一卡方方法至與其他剩餘感測電路有關之資料。若兩個測試之任一者失效，則可認為晶片不真實。

雖然已繪示及描述本發明之特定實施例及應用，但應理解，本發明並不限於本文中所揭示之精確組態及組件。本文中所使用之術語、描述及圖式係僅藉由圖解闡述且並不意謂限制。可在不脫離本發明之精神及範疇之情況下在本文中所揭示之本發明之裝置之配置、操作及細節、方法及系統中作出熟習此項技術者將明白之各種修改、改變及變動。藉由非限制性實例，將理解，本文中所包含之方塊圖意欲展示各裝置及系統之組件之一選定子集且各成像裝置及系統可包含圖上並未展示之其他組件。因此，一般技術者將認知，可在不減損本文中所描述之實施例之範疇及效能之情況下省略或重新排序本文中所描述之特定步驟及功能性。

結合本文中所揭示之實施例而描述之各種闡釋性邏輯區塊、模組、電路及演算法步驟可實施為電子硬體、電腦軟體或兩者之組合。為繪示硬體及軟體之此可互換性，上文已大體上在其等功能性方面描述各種闡釋性組件、區塊，模組、電路及步驟。此功能性是否實施為硬體或是軟體取決於施加於整體系統上之特定應用及設計約束。對於

各特定應用可以變化方式(諸如藉由使用微處理器、微控制器、場可程式化閘極陣列(FPGA)、特定應用積體電路(ASIC)及/或晶片上系統(SoC)之任何組合)實施所描述之功能性，但此等實施方案決策不應解釋為引起脫離本發明之範疇。

結合本文中所揭示之實施例所描述之一方法或演算法之步驟可直接體現於硬體中，於藉由一處理器執行之一軟體模組中，或於該兩者之一組合中。一軟體模組可駐留於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、一可移除碟片、一CD-ROM、一DVD或此項技術中已知之任何其他形式之儲存媒體中。

本文中所揭示之方法包括用於達成所描述之方法之一或多個步驟或動作。該等方法步驟及/或動作可在不脫離本發明之範疇之情況下彼此交換。換言之，除非對於實施例之適當操作要求步驟或動作之一特定順序，否則可在不脫離本發明之範疇之情況下修改特定步驟及/或動作之順序及/或使用。

【符號說明】

100	系統
110	簽章者器件
112	私密金鑰/金鑰
114	簽署區塊
115	鏈路
120	器件/敏感器件
130	晶片/測試晶片
135	真偽憑證
138	感測電路
138A	感測電路

138B	感測電路
138C	感測電路
138D	感測電路
150	系統
160	鑑認器件
162	公開金鑰/金鑰
164	簽章確認者區塊
165	鏈路/連接
181	待量測之電路/電路
181A	待量測之電路/電路
181B	待量測之電路/電路
181C	待量測之電路
181D	待量測之電路/電路
182	量測電路/晶片上量測電路
182A	量測電路
182B	量測電路
182C	量測電路
182D	量測電路
183	電流源
184	取樣保持電路
185	電壓量測電路
186	鏈
188	比較器
190	正反器
200	方法/初始化處理程序
210	方塊

220	方塊
230	方塊
240	方塊
245	方塊
250	方塊
300	方法
310	方塊
320	方塊
325	方塊
330	方塊
340	方塊
350	方塊
C	電容器流
CLK	輸入時脈/輸入/信號
d _T	時段
I	規則輸入
R	電阻器
S	切換器
V _{cc}	電壓供應源/電力供應電壓

申請專利範圍

1. 一種器件，其包括：

一感測電路，其包括待量測之一電路，該感測電路可使用待量測之該電路來產生對於該器件之一或多個物理性質的量測資料；

一儲存器，其儲存含有自該量測資料導出之鑑認資料之一真偽憑證；及

一通信埠，其經由耦合至該通信埠之一鏈路使該真偽憑證及該量測資料與一通信合作夥伴通信。

2. 如請求項1之器件，其中該真偽憑證係經由該通信埠接收且儲存於該儲存器中。

3. 如請求項1之器件，其中該一或多個物理性質包含以下之一或多者：由該器件上之待量測之該電路產生之熱量或達到之一溫度、一特定MOSFET電晶體或若干特定MOSFET電晶體之一洩漏電流、一特定路徑上之一延遲、在特定操作期間由一特定電路消耗之電力，及由一晶片上振盪器產生之一頻率。

4. 如請求項1之器件，其中該感測電路經組態以在進行該一或多個物理性質之量測時，量測環境資訊。

5. 如請求項4之器件，其中該環境資訊包含以下之一或多者：電力供應電壓、反向偏壓電壓及溫度。

6. 如請求項5之器件，其中該鑑認資料包含該環境資訊之經簽署的資料。

7. 如請求項5之器件，其中儲存於該真偽憑證中之該鑑認資料係針對某預定義溫度及/或電壓而正規化。

8. 一種用於鑑認一器件以保護免受一未經授權之仿製的方法，其

包括：

自該器件獲得一真偽憑證；

判定該真偽憑證是否真實；

自該器件收集對於該器件之一或多個物理性質的量測資料，

比較該經收集之量測資料與包含於該真偽憑證中之鑑認資料；及

基於該比較結果來判定該器件是否真實。

9. 如請求項8之方法，其中該一或多個物理性質包含以下之一或多者：在該器件上之待量測之該電路執行一預定義操作時，由該電路產生之熱量或達到之一溫度、一特定MOSFET電晶體或若干特定MOSFET電晶體之一洩漏電流、一特定路徑上之一延遲、在特定操作期間由一特定電路消耗之電力及由一晶片上振盪器產生之一頻率。
10. 如請求項8之方法，其中該鑑認資料包含環境資訊之經簽署資料。
11. 如請求項10之方法，其中該環境資訊包含以下之一或多者：電力供應電壓、反向偏壓電壓及溫度。
12. 如請求項10之方法，其中儲存於該真偽憑證中之該鑑認資料係針對某預定義溫度及/或電壓而正規化。
13. 如請求項8之方法，其中判定該器件是否真實取決於該經收集之量測資料是否在一預期範圍內。
14. 如請求項13之方法，其中該預期範圍經預定義。
15. 如請求項13之方法，其中該預期範圍係自該所獲得之真偽憑證中的資料導出。
16. 如請求項8之方法，其中比較該經收集之量測資料與該真偽憑證中之該鑑認資料包括指派權重至量測資料中的至少一些。

17. 如請求項8之方法，其中比較該經收集之量測資料與該真偽憑證中之該鑑認資料包括計算該器件真實之一概率。
18. 如請求項17之方法，其中計算該器件真實之該概率包括確認該經收集之量測資料對應於自該真偽憑證獲得之該鑑認資料之一統計假設。
19. 如請求項18之方法，其中確認該統計假設包括對多個量測結果使用一卡方方法及判定一 p 值大於一預定義臨限值。
20. 一種用於鑑認一器件之鑑認裝置，其包括：
 - 用於儲存一公開金鑰之一儲存器；
 - 經組態以使用該公開金鑰來鑑認真偽憑證之一簽章確認區塊；
 - 一通信埠；及
 - 一處理器，其經組態以：
 - 建置至待透過該通信埠鑑認之該器件之一連接；
 - 透過該通信埠，自該器件獲得一真偽憑證；
 - 自該器件收集對於該器件之一或多個物理性質的量測資料；
 - 比較該經收集之量測資料與該真偽憑證中的鑑認資料；及
 - 基於該比較結果來判定該器件是否真實。
21. 如請求項20之鑑認裝置，其中該一或多個物理性質包含以下之一或多者：在該器件上之待量測之一電路執行一預定義操作時，由該電路產生之熱量或達到之一溫度、一特定MOSFET電晶體或若干特定MOSFET電晶體之一洩漏電流、一特定路徑上之一延遲、在特定操作期間由一特定電路消耗之電力及由一晶片上振盪器產生之一頻率。
22. 如請求項20之鑑認裝置，其中比較該經收集之量測資料與該真

偽憑證中之該鑑認資料係確認該經接收之量測資料係在一預期範圍內。

23. 如請求項22之鑑認裝置，其中該預期範圍經預定義。
24. 如請求項22之鑑認裝置，其中該預期範圍係自真偽憑證中之該資料導出。
25. 如請求項20之鑑認裝置，其中比較該經收集之量測資料與該真偽憑證中之該鑑認資料包括指派權重至量測資料中的至少一些。
26. 如請求項20之鑑認裝置，其中比較該經收集之量測資料與該真偽憑證中之該鑑認資料包括計算該器件真實之一概率。
27. 如請求項26之鑑認裝置，其中計算該器件真實之該概率包括確認該經收集之量測資料對應於自該真偽憑證獲得之該鑑認資料之一統計假設。
28. 如請求項27之鑑認裝置，其中確認該統計假設包括對多個量測結果使用一卡方方法及判定一 p 值大於一預定義臨限值。

圖式

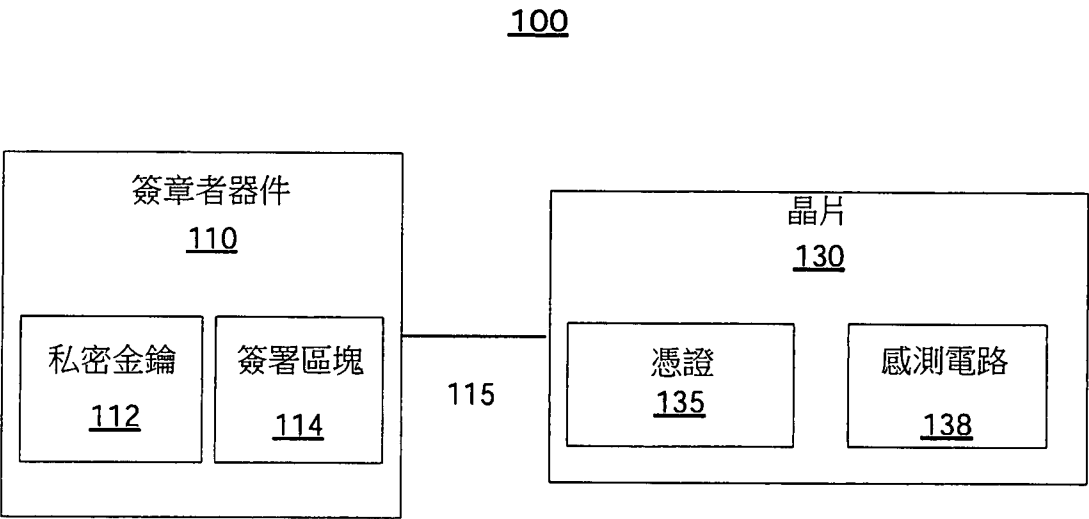


圖1A

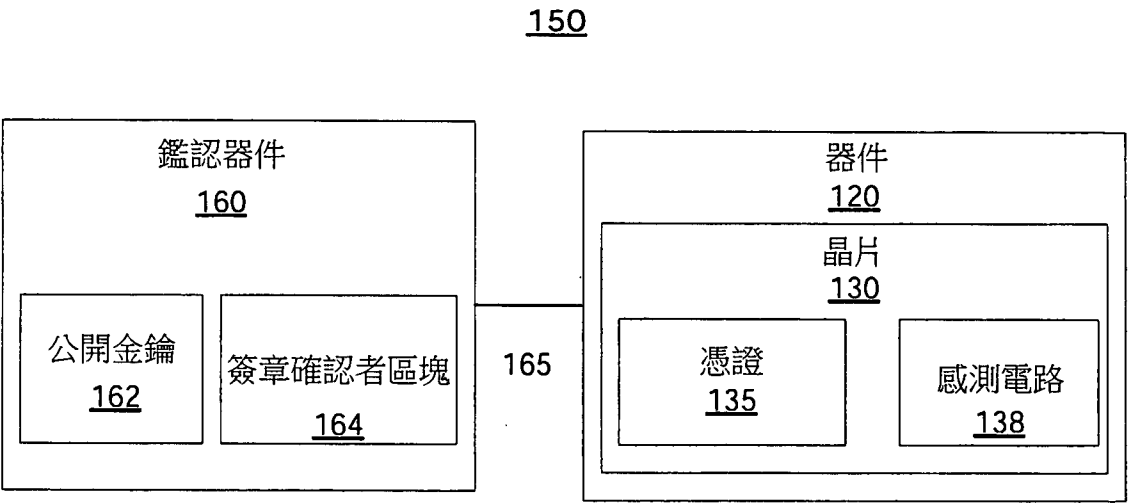


圖1B

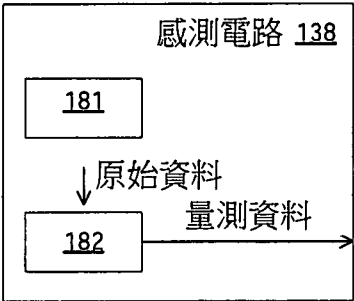


圖1C

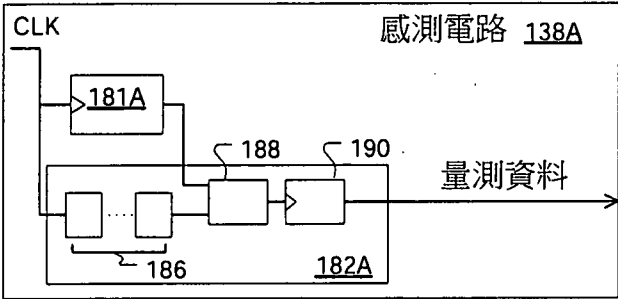


圖1D

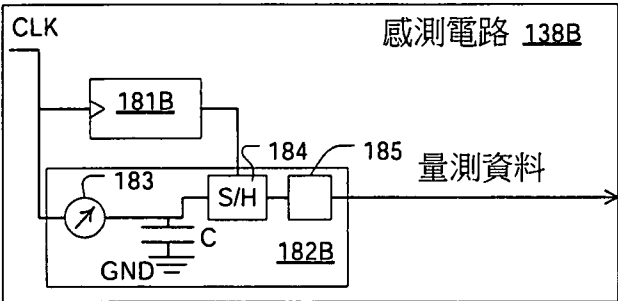


圖1E

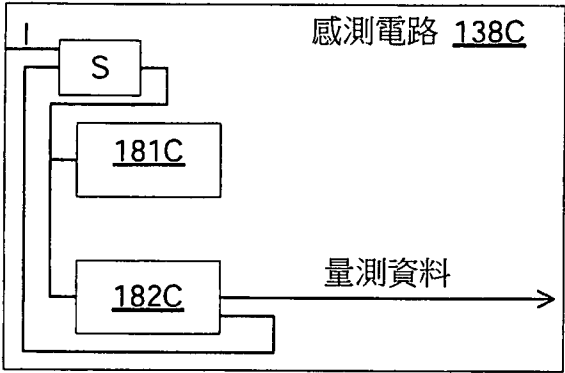


圖1F

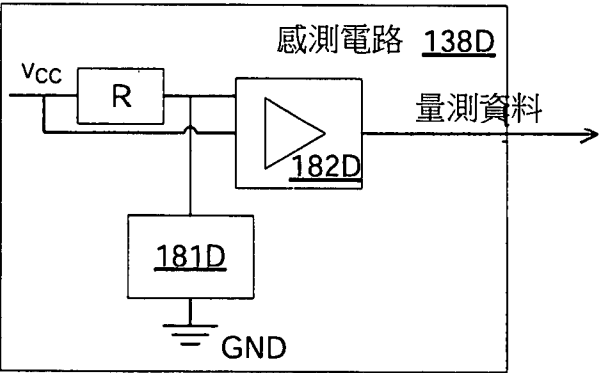


圖1G

200

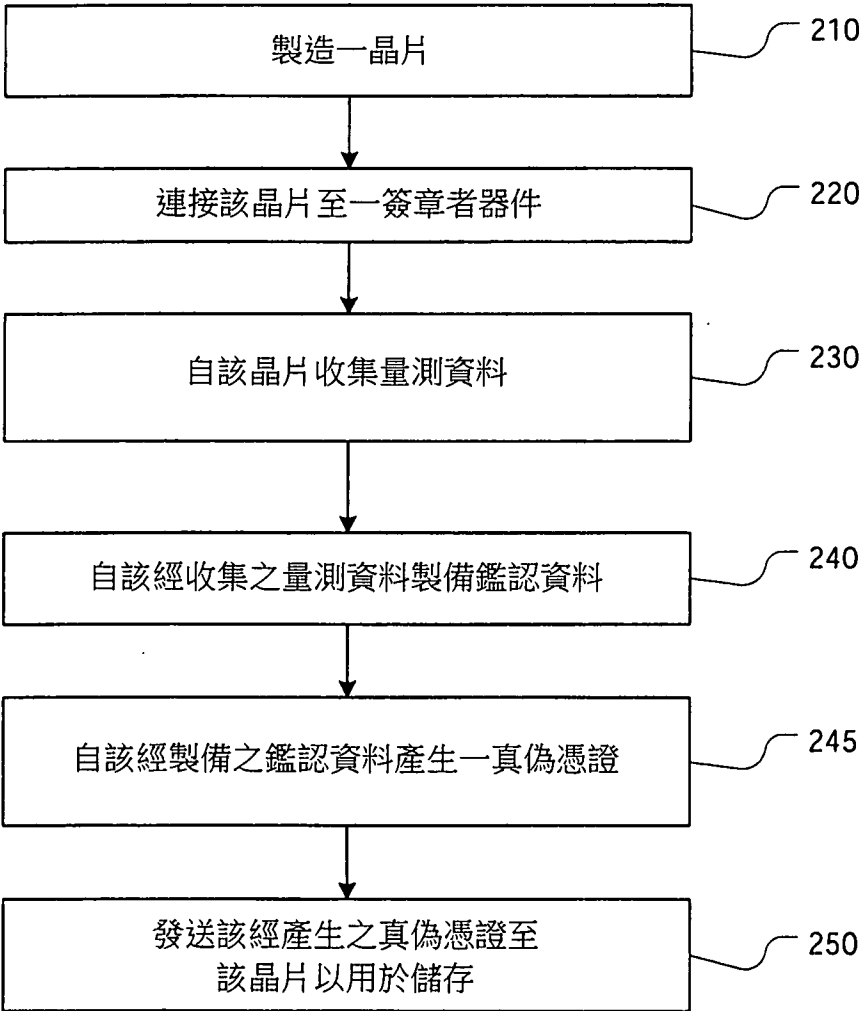


圖2

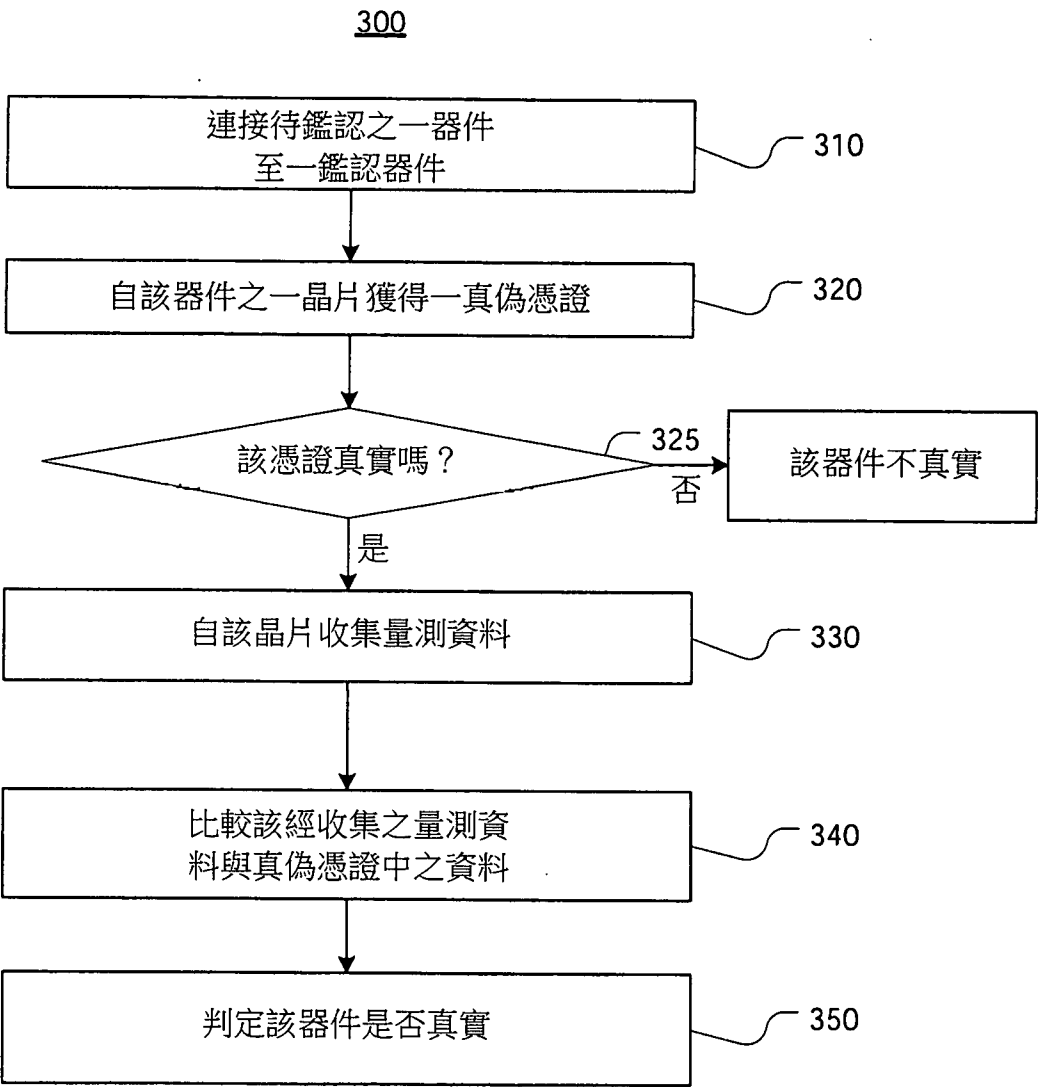


圖3