I723632

(19)中華民國智慧財產局

(12)發明說明書公告本　**(11)證書號數：TW I723632 B**

(45)公告日： 中華民國 110 (2021) 年 04 月 01 日

(21)申請案號：108141447　(22)申請日： 中華民國 108 (2019) 年 11 月 14 日

(51)Int. Cl.：　*G06F21/75　(2013.01)*

(30)優先權：2018/12/06　歐洲專利局　18210773.0

(71)申請人：美商萬事達卡國際公司 (美國) MASTERCARD INTERNATIONAL INCORPORATED (US)

美國

(72)發明人：布萊斯　S BLYTHE, SIMON (GB)

(74)代理人：張仲謙

(56)參考文獻：

TW　I547823　TW　I625627

US　2017/0357829A1

審查人員：馮耀嘉

申請專利範圍項數：9 項　圖式數：4　共 21 頁

(54)名稱

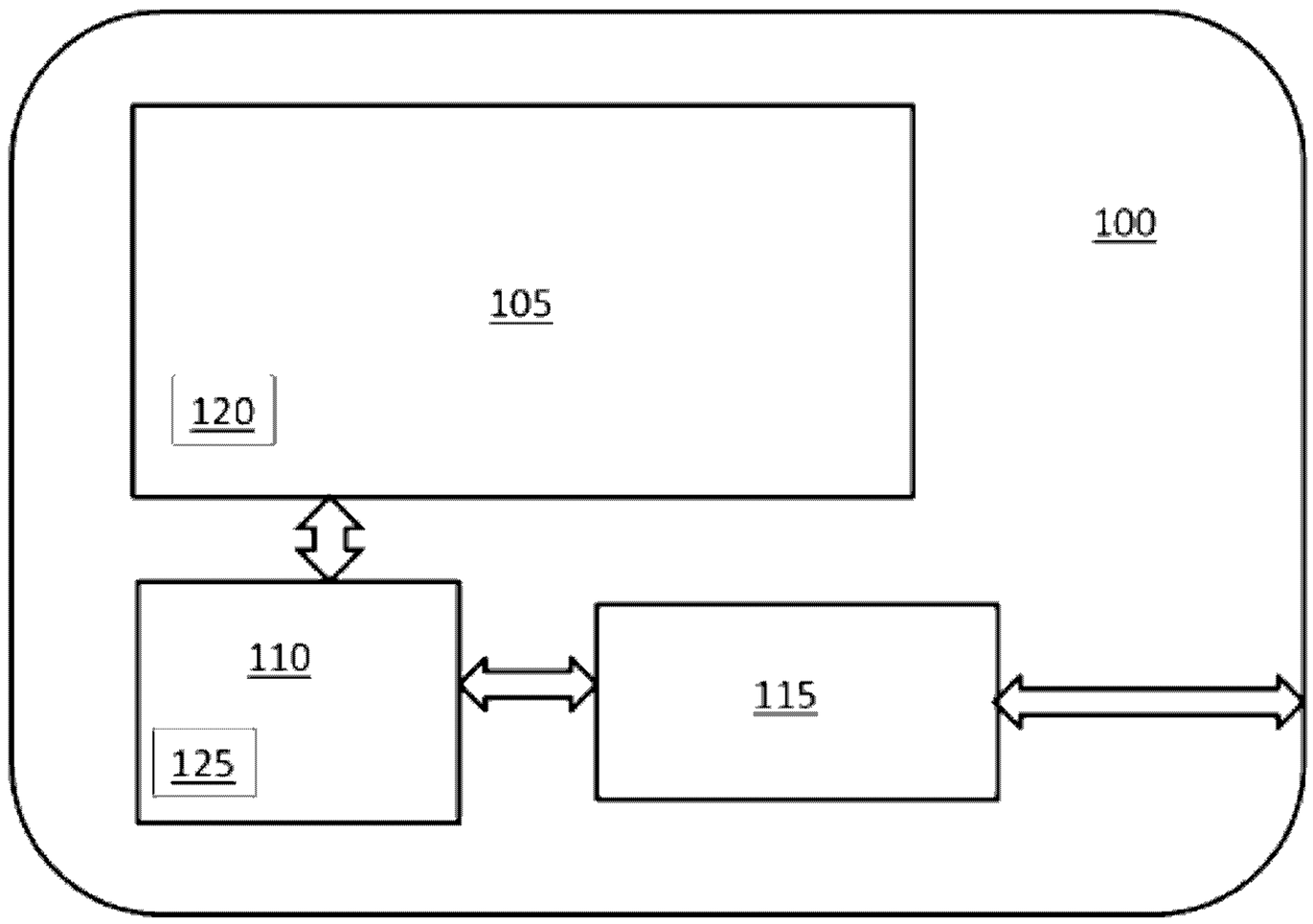
一積體電路、方法以及計算機程式

(57)摘要

本說明係關於一積體電路，該積體電路包括：一處理區域配置為執行複數個指令中之一指令；一第一溫度量測區域，配置為量測該積體電路中該處理區域執行該指令時之一第一量測溫度；該處理區域執行該指令時，該處理區域配置為比較該第一溫度量測區域之該第一量測溫度與一預定溫度，其中當該第一量測溫度超過該預定溫度達一閾值，該處理區域觸發一事件。

An integrated circuit is disclosed. The integrated circuit comprises: a processing region configured to run one instruction from a plurality of instructions; a first temperature measuring region configured to measure a first measured temperature within the integrated circuit in response to the processing region running the one instruction; the processing region being configured to compare the measured first temperature with a predefined temperature at the first temperature measuring region when the processing region runs the one instruction and to trigger an event when the measured first temperature exceeds the predefined temperature by a threshold value.

指定代表圖：



【圖1】

符號簡單說明：

100:積體電路

105:儲存區域

110:處理區域

115:通訊區域

120:第一溫度感測器

125:第二溫度感測器

專利案號：108141447

109年11月02日 所提修正

公告本

I723632

【發明摘要】

【中文發明名稱】 一積體電路、方法以及計算機程式

【英文發明名稱】 AN INTEGRATED CIRCUIT, METHOD AND COMPUTER PROGRAM

【中文】

本說明係關於一積體電路，該積體電路包括：一處理區域配置為執行複數個指令中之一指令；一第一溫度量測區域，配置為量測該積體電路中該處理區域執行該指令時之一第一量測溫度；該處理區域執行該指令時，該處理區域配置為比較該第一溫度量測區域之該第一量測溫度與一預定溫度，其中當該第一量測溫度超過該預定溫度達一閾值，該處理區域觸發一事件。

【英文】

An integrated circuit is disclosed. The integrated circuit comprises: a processing region configured to run one instruction from a plurality of instructions; a first temperature measuring region configured to measure a first measured temperature within the integrated circuit in response to the processing region running the one instruction; the processing region being configured to compare the measured first temperature with a predefined temperature at the first temperature measuring region when the processing region runs the one instruction and to trigger an event when the measured first temperature exceeds the predefined temperature by a threshold value.

【指定代表圖】　　第1圖

【代表圖之符號簡單說明】

100:積體電路

105:儲存區域

110:處理區域

115:通訊區域

120:第一溫度感測器

125:第二溫度感測器

【特徵化學式】

無

【發明說明書】

【中文發明名稱】 一積體電路、方法以及計算機程式

【英文發明名稱】 AN INTEGRATED CIRCUIT, METHOD AND COMPUTER PROGRAM

【技術領域】

【0001】 本說明係關於一積體電路、方法以及計算機程式。

【先前技術】

【0002】 此處描述之「背景技術」係廣泛呈現本說明之內容。因此，皆非明確或暗示地承認背景技術所提及之當前發明者的工作及於申請時可能不算是先前技術之內容是本說明的先前技術。

【0003】 對半導體晶片(chip)(如信用及簽帳卡之智慧卡晶片或行動電話之移動用戶識別卡)的物理性攻擊係已知。此類型攻擊中，駭客可能試圖取得密鑰或其他安全儲存於半導體晶片電路中之機密。此類型攻擊需要對晶片進行物理性存取。

【0004】 此類型攻擊中，光學探測可能發生在晶片自背面向下變薄至10 μm (或更少)的剩餘厚度之處，用雷射進行探測。其他情況下，為了對金屬內連線進行電性或電子束探測，需從選擇區域的背面完整取下半導體。其他物理性攻擊機制，需薄化晶片以進行高解析X光斷層掃描或放光研究。

【0005】減少成功之物理性攻擊的可能性係嘗試及保護半導體晶片的背面。然而，要引入積體電路製程中，仍極少成功找到非過於昂貴或複雜的保護機制。

【0006】因此，需要一方法降低對半導體晶片進行成功物理性攻擊之可能性，而該方法並非只保護半導體晶片背面。此為本說明欲達成之目標。

【發明內容】

【0007】據某一方面，提供一積體電路，包含：一處理區域用以執行複數個指令中之一指令；一第一溫度量測區域，配置為量測該積體電路中該處理區域執行該指令時之一第一量測溫度；該處理區域執行該指令時，該處理區域配置為比較該第一溫度量測區域之該第一量測溫度與一預定溫度，其中當該第一量測溫度超過該預定溫度達一閾值時，該處理區域觸發一事件。

【0008】前述段落已用廣泛的方式介紹，並且無打算限制下列發明專利申請範圍。提及的實施例與進一步優勢，參考下列詳細說明及相關附圖會有最好的理解。

【圖式簡單說明】

【0009】通過參考下列詳細說明同時結合附圖考量，對本說明及其更多附帶優勢會有更完整的理解，其中：

圖1與圖2分別描述本說明之一積體電路及其實施例；

圖3描述本說明實施例之一流程圖；

圖4描述圖3中本說明實施例中儲存溫度之一表格。

【實施方式】

【0010】 參考繪圖，其中相同參考數字表示各圖的相同或相對應之元件。

【0011】 根據本說明實施例，圖1顯示一積體電路100。積體電路100由半導體材料如矽(Si)或砷化鎵(GaAs)製成。本說明實施例中，積體電路100將由包含非接觸技術之晶粒(die)或PIN型信用或簽帳卡。因此，積體電路100可符合EMV標準，或其他標準或根據 ISO/IEC 7816及 ISO/IEC 14443之標準。

【0012】 雖然積體電路100包含數個個別區域，且每一區皆執行各種符合這些標準之功能，但為方便解釋，圖1顯示三個區域。當然，多於或少於三個區域是可以預期的。

【0013】 積體電路100包含一處理區域110以交換及處理資料。通常，資料在應用協定資料單元(Application Protocol Data Units, APDUs)中交換，且根據指令進行處理。例如，傳送指令至處理區域110，處理區域110將適當處理之並與積體電路100中之其他區域交換資料。指令係指自包含多個指令之指令集中所取出之處理區域110的單一操作，並由技術人員完成。

【0014】 晶粒及PIN技術中之指令，例如可為一命令。此一命令可能包括產生應用程序的密碼命令、應用處理區域的命令、外部驗證的命令或類似的命令。這些技術人員已知的命令係由各種標準如 ISO/IEC 7816-3 定義。

【0015】 應當理解的是，儘管上述定義之命令是在晶粒及PIN的技術中使用，仍有些命令如外部驗證的命令是在其他晶粒卡應用程序(如符合 ISO/IEC 7816-4 標準之 GSM SIM 卡技術)中使用。因此，本說明書並不限於晶粒及 PIN 的技術，且可同等地應用於任何合適之技術。

【0016】 在指令處理期間，處理區域110可以處理或交換敏感資料。換句話說，處理區域110可以處理或交換資料，但若被惡意第三方擷取資料，可能會

破壞積體電路100的安全性。敏感資料例如可為用來產生密碼之密鑰，或是與積體電路100使用者相關的個人資訊。此敏感資料可以以未加密形式儲存於儲存區域105中之安全部分。例如，用來產生密碼之密鑰以未加密形式儲存於儲存區域105中之安全部分。

【0017】 在操作中，為批准交易，處理區域110可以藉由通訊電路115接收應用密碼的產生指令，作為來自與通訊電路115通訊之讀卡機(未顯示)的指令。除了指令外，處理區域110將接收其他資料單元，如交易數量及與批准來自讀卡機之交易相關的其他資訊。處理區域110將從儲存區域105之安全部分取回密鑰，並將利用密鑰來加密其他資料單元以產生密碼。密碼接著傳送至通訊區域115，再傳送至讀卡機。

【0018】 若惡意第三方對積體電路100執行物理性攻擊，則當密鑰自儲存區域105取回時，第三方能夠從連結處理區域110與儲存區域105之匯流排130中存取密鑰。換句話說，第三方可從讀卡機傳送應用密碼的產生指令。做為回應，未加密之密鑰將從儲存區域105之安全部分中取回，而被第三方以電子或電子束探測暴露的互聯內容時攔截。的確，若一物理性攻擊可直接存取儲存區域105之安全部分，密鑰可直接從儲存區域105之安全部分取回。這將可能破壞積體電路100的安全性。

【0019】 當製造積體電路100時，係包含半導體晶粒上之儲存區域105、處理區域110與通訊區域115，並將散熱材料配置其上。操作積體電路100期間，為確保積體電路100沒有任一部份會過熱、失效或無法操作，會控制散熱材料之分布及其散熱特性。

【0020】 散熱材料可被置於半導體晶粒之任何位置。這包含半導體晶粒之背面。如上述提及，為了對積體電路100取得物理性接觸，會去除至少半導體晶

粒背面的一部分。這意謂，至少有部分散熱材料被去除。這改變了積體電路100中散熱材料的特性。

【0021】特別是，散熱材料自一區域拆除後，比起有散熱材料的區域，在此區域之半導體晶粒的原位溫度顯著增加。這是因為，比起散熱至周圍環境，散熱材料有較佳之散熱特性。

【0022】因此，本說明之實施例中，在積體電路100裝置一個或多個溫度感測器，用以量測積體電路100操作期間中至少一個區域之溫度。在實例中，當區域之溫度超過一閾值，一事件被觸發。換句話說，若區域之溫度超過閾值，則可以假設積體電路100已遭受一物理性侵入。因此，事件可能為：刪除或毀損儲存區域105或儲存區域105之一部分(如安全儲存部分)中的資料，破壞處理區域110，或自安全部分發布虛假資料以混淆敏感資料等。換句話說，此事件防止駭客取得敏感資訊。

【0023】如上述提及，儲存區域105及處理區域110係駭客欲取得物理性接觸之位在半導體晶粒(die)上之積體電路100的區域。具體來說，不限於實施例，儲存區域105之安全部分以及處理區域110與安全部分通訊之區域，係物理駭客特別想接觸之區域。

【0024】因此，於儲存區域105之安全區域上製造一第一溫度感測器120，並於處理區域110製造一第二溫度感測器125。換句話說，實施例中，第一溫度感測器120及第二溫度感測器125位於積體電路100的多個區域上，在一物理性攻擊期間，這些區域可能被暴露或被更動。當然，本說明並非如此受限，且感測器可位於積體電路100上之任何位置，如較少被當作攻擊目標的區域，以提供背景溫度的讀數。這些溫度感測器係以已知技術來製造，且可包含重新使用這些區域中已製造的電晶體。為求簡潔，由於溫度感測器於半導體晶粒及積體電路100的製造方法為已知，因此以下將不會詳細解釋之。

【0025】在物理侵入事件中，由於半導體晶粒上之散熱材料被移除，第一溫度感測器120及第二溫度感測器125量測之溫度皆會超過散熱材料未被移除時區域之溫度。特別是，當散熱材料存在，處理區域110執行一給定指令，並給定一環境溫度，第一溫度感測器120及/或第二溫度感測器125量測之溫度將會很好地被定義之。換句話說，當散熱材料存在，在處理區域110執行一特定指令時，將會很好定義處理區域110及/或儲存區域105之安全區域的溫度上升。

【0026】然而，在物理性攻擊期間，在已以任何方式移除、毀損或破壞散熱材料的區域，對於給定的指令，第一溫度感測器120及/或第二溫度感測器125量測之溫度將會與預期非常不同。

【0027】因此，本說明之實施例中，對於給定指令，若第一溫度感測器120及/或第二溫度感測器125量測之溫度高於預期溫度達一預定數值時，則可確認有物理性攻擊。

【0028】圖2依據實施例顯示一積體電路100。於圖2積體電路100中，顯示數個參考到圖1的零件。這些零件具有共同參考數字，且讀者可以參考圖1之討論。另外，在通訊電路115中有第三溫度感測器210，以及在儲存區域105之非安全部分設有第四溫度感測器205。

【0029】一般來說，在物理性攻擊期間，通訊電路115周圍之散熱材料保持不受影響。這意謂第三溫度感測器210可量測環境溫度或積體電路100之背景溫度。當然，本說明並非如此受限，為了量測積體電路100之環境溫度，第三溫度感測器210可被設於積體電路100中任何較不可能發生物理性攻擊之位置。

【0030】如上述提及，在儲存區域105之非安全部分設有第四溫度感測器205。與通訊電路115類似，儲存區域105之非安全部分係較不可能被侵入，儲存區域105之非安全部分周圍之散熱材料通常維持原樣。因此，第四溫度感測器205也可用於量測積體電路100之環境溫度。

【0031】 應注意，提供一個或多個環境溫度感測器係可選擇的。

【0032】 圖3顯示描述本說明實施例之一流程圖300。流程圖300使用存於儲存區域105之軟體，於實施例的積體電路100中執行。

【0033】 流程圖300自步驟305開始。處理區域110執行一指令時，程序進行至步驟310。一實例指令，係藉一讀卡機與通訊電路115通訊，接收應用程序的密碼指令。由於指令是由處理區域110執行，處理區域110調查第一溫度感測器120，並接收第一溫度感測器120量測之溫度。此係步驟315。當處理區域110調查第二溫度感測器125，並接收第二溫度感測器125量測之溫度時，程序進行至步驟320。當然可預期的，處理區域110可能調查第三溫度感測器205及/或第四溫度感測器210，以補充或代替第一溫度感測器120及第二溫度感測器125。換句話說，可預期於一物理性攻擊期間，一第一量測溫度讀數將來自一較可能損毀之區域，且一第二量測溫度讀數將來自另一較可能或較不可能損毀之區域。

【0034】 處理區域110接著比較第一及第二量測溫度之差距。此係步驟325。當建立一檢查，係第一與第二溫差是否超過一閾值溫度，程序進行至步驟330。此於圖4更詳細描述。在差距超過閾值溫度之事件，即一物理性攻擊被探測，選擇「是」路徑，進行至步驟335，且如上述解釋，將執行一事件如至少刪除儲存區域105之安全部分。程序接著進行至步驟340，流程圖即結束。

【0035】 回歸至步驟330，若溫差未超過閾值溫度，選擇「否」路徑，進行至流程終點，即步驟340。

【0036】 流程圖330提及，當執行一特定指令時，溫差超過一閾值溫度，則為偵測到物理性攻擊。當執行指令時，測量而得之一溫度可能為環境溫度或可能皆為積體電路100中之特定區域或受物理性攻擊影響之區域。

【0037】 一些狀況下，執行一特定指令時，物理性攻擊可能會因三個或更多溫度量測之間的差距超過一閾值而被偵測到。

【0038】 應注意，本說明並非僅受限於複數個溫度量測。例如，當處理區域110執行一指令時，較可能受物理性攻擊傷害之區域的溫度量測超過一特定溫度達一預定數值時，可能表示偵測到物理性攻擊。換句話說，當處理區域110執行一特定指令，而絕對溫度量測超過一特定溫度時，可能表示偵測到一物理性攻擊。

【0039】 圖4顯示一表格。在一實施例中，表格存放於儲存區域105。表格可存放於儲存區域105的安全部分，以確保表格的完整性。表格可以是與由處理區域110在第一溫度感測器120、第二溫度感測器125、第三溫度感測器205和第四溫度感測器210處的期望溫度來運行指令相關聯的任何數據結構。換句話說，當處理區域110執行一特定指令且散熱材料係完整的，表格存放各溫度感測器之期望溫度。當給定一環境溫度時，上述期望溫度係各溫度感測器之絕對溫度。

【0040】 如上述實施例，二量測溫度之差距係用以判斷是否發生物理性攻擊。透過考量溫差，對於減緩環境溫度的影響特別有效。換句話說，當絕對溫度列入考量，在高溫環境下，即使沒有物理性攻擊發生，絕對溫度仍可能超過閾值。然而，當使用二量測所得溫度的差值來偵測物理性攻擊，則可以減輕大環境溫度的影響。這減低了偵測物理性攻擊時發生錯誤的可能性。

【0041】 在圖4的實例表格中，程序區域110執行之指令係一應用程序密碼指令，且散熱材料係完整的，第一溫度感測器120量測之第一量測溫度係攝氏55度，第二溫度感測器125量測之第二量測溫度係攝氏85度，第三溫度感測器205量測之第三溫度係攝氏45度，以及第四溫度感測器210量測之第四溫度係攝氏40度。此溫度分布顯示指令是由處理區域110所執行。換句話說，當應用程序密碼指令運行時，處理區域110將接收來自儲存區域105之安全部分的密碼。由於這是一個複雜的命令，因此需要處理區域110進行密集操作，這意味著第二量測溫

度（與處理區域110相關的溫度）將會很高。另外，儲存區域105之安全部分操作時，第一量測溫度(與儲存區域105相關之溫度)會上升。

【0042】 由於通訊電路115及儲存區域105之非安全部分並無密集操作，第三量測溫度及第四量測溫度係約為環境溫度。

【0043】 在圖4實例表格中，處理區域110執行之指令係一確認讀卡機的命令，且散熱材料係完整的，第一溫度感測器120量測之第一溫度係攝氏40度，第二溫度感測器125量測之第二量測溫度係攝氏55度，第三溫度感測器量測之第三溫度係攝氏40度，以及第四溫度感測器210量測之第四溫度係攝氏70度。再一次，此溫度分布顯示此指令是由處理區域110執行的。明確地說，確認讀卡機的命令無須存取儲存區域105之安全部分。因此，第一溫度感測器120量測之第一量測溫度係約環境溫度。因指令並不複雜，處理區域110無須密集操作。這表示，相較於複雜操作時之溫度，第二量測溫度(處理區域110之溫度)很低。再者，由於儲存區域105非安全部分無需處理確認讀卡機的指令，與儲存區域105之非安全部分相關聯之第三溫度係低溫。最終，由於通訊電路115必須與讀卡機通訊以處理指令，第四溫度感測器210量測之通訊電路115的溫度上升。

【0044】 相應地，當在處理區域110上運行特定指令並且積體電路100具有完整的散熱材料時，圖4的表包括與每個溫度感測器相關聯的預定溫度。儲存溫度中之任二者的差距即為預定義溫度差距。

【0045】 因此，回到圖3步驟330，對於其中處理區域110正在運行特定指令的積體電路100，決定二量測溫度之溫差。對同一指令，將儲存在圖4表中的兩個測得溫度之間的預定溫差進行比較。例如，二量測溫度差高於預定溫度差之10%的閾值達之，則流程進行至步驟335。或者，若量測溫度小於或等於閾值，流程進行至步驟340，如圖3之相關解釋。當然，雖然前文以溫度差高於預定溫

度差之10%的閾值為例，本說明並非如此受限。差距可以是一相異的百分比或一絕對數值。

【0046】如上述本說明實施例解釋，積體電路100執行一指令時，各部分的溫度係積體電路100之特性。這表示，雖然上文已對是否從半導體晶粒移除散熱材料作描述，本說明並非如此受限。舉例來說，某些狀況下，有必要確保指令僅於特定(即合法)積體電路上執行。為了避免個人於其他積體電路執行指令，可以採用類似上文描述之系統。換句話說，可以在執行一指令時，測量積體電路中一或多部分的溫度，並於一合法積體電路執行相同指令時與一預定溫度作比較，接著於量測溫度高於閾值時觸發一事件。若製造商希望軟體僅運行於特定且認證的積體電路時，此係有用的。因此，以上技術能用於識別何時在未認證的積體電路上運行這種軟體，因為當軟體於未認證的積體電路上執行指令時之溫度會有別於在已認證積體電路上執行指令時之溫度。

【0047】明顯地，根據上述指示，本說明的多種修改及變化係可能實現的。因此可以了解，於申請專利範圍內，本說明能以有別於此處描述之方式來實施之。

【0048】就已實施之本說明實施例而言，透過軟體控制的數據處理儀器能夠理解，裝有軟體之一非暫態機器可讀取媒介(non-transitory machine-readable medium)，如一光碟、一磁碟、半導體記憶體或其他，皆可用以代表本說明之實施例。

【0049】應理解的，以上描述為了清楚起見，已參考不同功能元件、電路及/或處理器。但明顯地，在無背離實施例的情況下，不同功能元件、電路及/或處理器中任何功能布局皆有可能使用。

【0050】描述之實施例可實施於任何合適之形式，包括硬體、軟體、韌體或前述任何組合。描述之實施例至少可選擇性實施於部分執行於一或更多資料

之處理器及/或數位訊號處理器之計算機軟體。任何實施例之元件及組件可以以任何合適之物理地、功能性地與合邏輯之方式實現。實際上，功能性可以以單一單元、複數個單元或以其他功能單元之部分來實施。如此，本說明之實施例可於單一單元實現，或物理地及功能性地分布於不同單元、電路及/或處理器之間。

【0051】 儘管本說明已描述相當多實施例，但此處闡述並非意圖限制於特定形式。此外，儘管本說明之特點已結合特定實施例進行描述，但本領域之技術人員可能將了解，所述實施例之各種特點可與任何合適之實施技術結合。

【0052】 本說明之實施例可依據下列編號條款定義：

【0053】 1. 一種積體電路，包含：

一處理區域，配置為執行複數個指令中之一指令；

一第一溫度量測區域，配置為量測該積體電路中該處理區域執行該指令時之一第一量測溫度，其中：

該處理區域執行一指令時，該處理區域配置為比較該第一溫度量測區域之該第一量測溫度與一預定溫度，其中當該第一量測溫度超過該預定溫度達一閾值，該處理區域觸發一事件。

【0054】 2. 如條款1所述的積體電路，更包含：

一第二溫度量測區域，配置為量測該積體電路中該處理區域執行該指令時之該第二量測溫度，其中當該第一量測溫度與該第二量測溫度之差距超過一預定溫差(a predefined temperature difference)達一預設值，該處理區域觸發一事件。

【0055】 3. 如條款1或2所述的積體電路，其中該事件係偵測對該積體電路之一物理性攻擊。

【0056】 4. 如第條款3所述的積體電路，更包含：

一包含安全區域及一非安全區域之存儲區域，其中當該物理性攻擊事件被偵測，該處理區域配置為刪除該安全區域之資料。

【0057】 5. 一種偵測一積體電路中之一物理性攻擊方法，其包含步驟有：

執行複數個指令中之一指令；以及

量測該積體電路執行該指令時之一第一量測溫度；以及

當執行該指令時，比較該第一量測溫度及該第一溫度量測區域之一預定溫度；以及

當該第一量測溫度超過該預定溫度之一閾值時，觸發一事件。

【0058】 6. 如條款5所述一種偵測一積體電路中之一物理性攻擊的方法，更包含：

量測該積體電路執行該指令時之一第二量測溫度；以及

當該第一量測溫度及該第二量測溫度之差距超過一預定溫差達一預設值時，觸發該事件。

【0059】 7. 如條款5或6所述偵測一積體電路中之一物理性攻擊的方法，其中該事件係偵測對該積體電路之一物理性攻擊。

【0060】 8. 如條款7所述偵測一積體電路中之一物理性攻擊的方法，其中當該物理性攻擊事件被偵測，該方法配置為刪除該積體電路中一安全區域之資料。

【0061】 9. 一計算機程式，用於計算機可讀取之指令，當該程式上載於一計算機，配置該計算機以執行如條款5-8任一項所述之方法。

【符號說明】

100:積體電路

105:儲存區域

110:處理區域

115:通訊區域

120:第一溫度感測器

125:第二溫度感測器

205:第三溫度感測器

210:第四溫度感測器

300:流程圖

305,310,315,320,325,330,335,340:步驟

【發明申請專利範圍】

【請求項1】 一種積體電路，包含：

一處理區域，配置為執行複數個指令中之一指令；

一第一溫度感測器被配置於該積體電路中的一第一溫度量測區域上，該第一溫度感測器係配置以量測該第一溫度量測區域執行該指令時之一第一量測溫度，其中：

該處理區域執行一指令時，該處理區域配置為比較該第一溫度量測區域之該第一量測溫度與一預定溫度，其中當該第一量測溫度超過該預定溫度達一閾值時，該處理區域觸發一事件；

其中該預定溫度是根據執行該指令時相對於該第一溫度量測區域的散熱材料的條件所設定的。

【請求項2】 如請求項1所述的積體電路，更包含：

一第二溫度量測區域，配置為量測該積體電路中該處理區域執行該指令時之該第二量測溫度，其中當該第一量測溫度與該第二量測溫度之差距超過一預定溫差達一預設值時，該處理區域觸發一事件。

【請求項3】 如請求項1或第2所述的積體電路，其中該事件係偵測對該積體電路進行之一物理性攻擊。

【請求項4】 如請求項3所述的積體電路，更包含：

包含安全區域及一非安全區域之一存儲區域，其中當該物理性攻擊的事件被偵測到時，該處理區域配置為刪除該安全區域之資料。

【請求項5】 一種偵測一積體電路中之一物理性攻擊方法，其包含步驟有：

執行複數個指令中之一指令；以及

量測該積體電路中的一第一溫度量測區域於執行該指令時之一第一量測溫度；以及

當執行該指令時，比較該第一量測溫度及該第一溫度量測區域之一預定溫度；以及

當該第一量測溫度超過該預定溫度之一閾值時，觸發一事件；

其中該預定溫度是根據執行該指令時相對於該第一溫度量測區域的散熱材料的條件所設定的。

【請求項6】 如請求項5所述偵測一積體電路中之一物理性攻擊的方法，更包含：

量測該積體電路執行該指令時之一第二量測溫度；以及

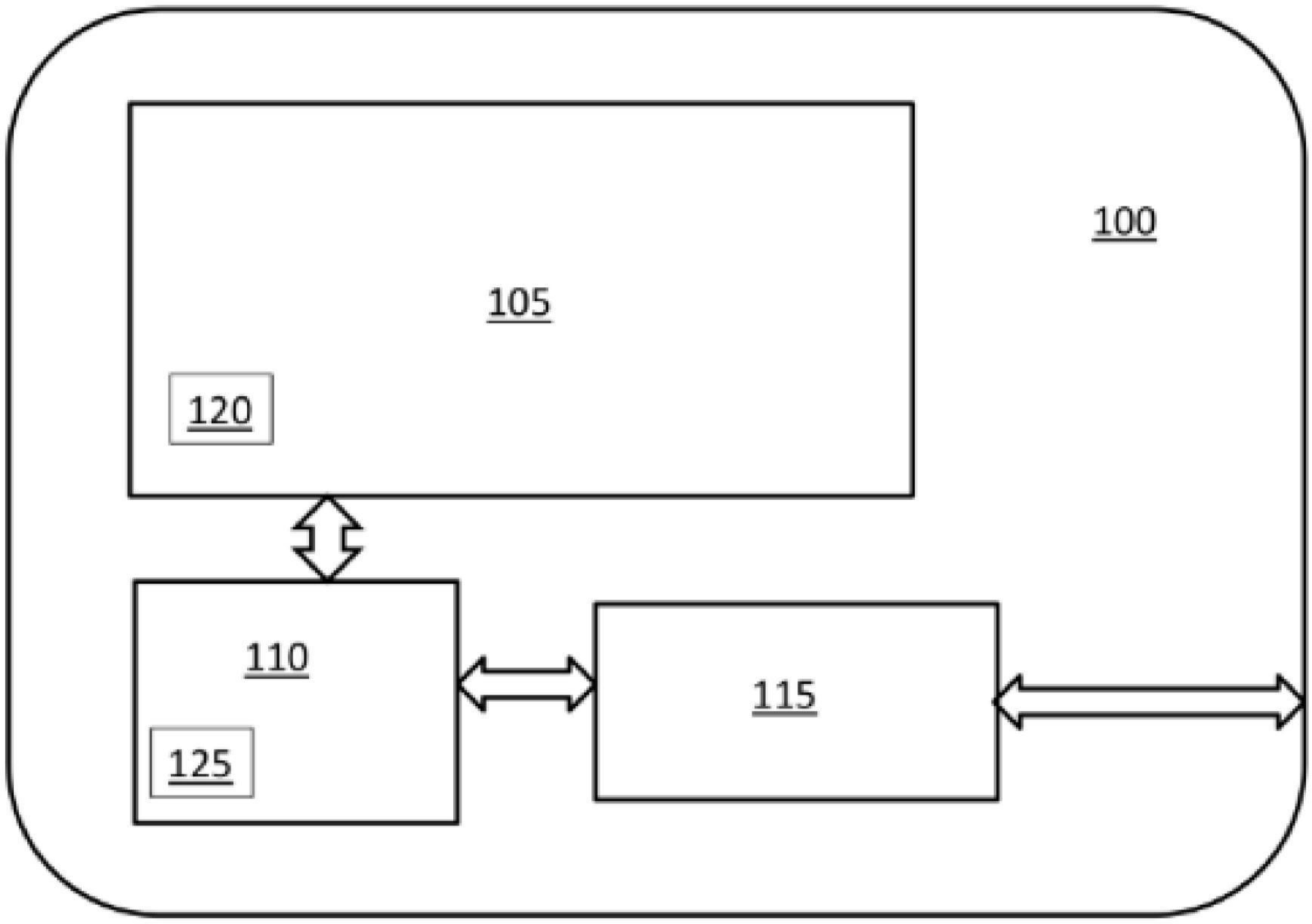
當該第一量測溫度及該第二量測溫度之差距超過一預定溫差達一預設值時，觸發該事件。

【請求項7】 如請求項5或6所述偵測一積體電路中之一物理性攻擊的方法，其中該事件係偵測對該積體電路之一物理性攻擊。

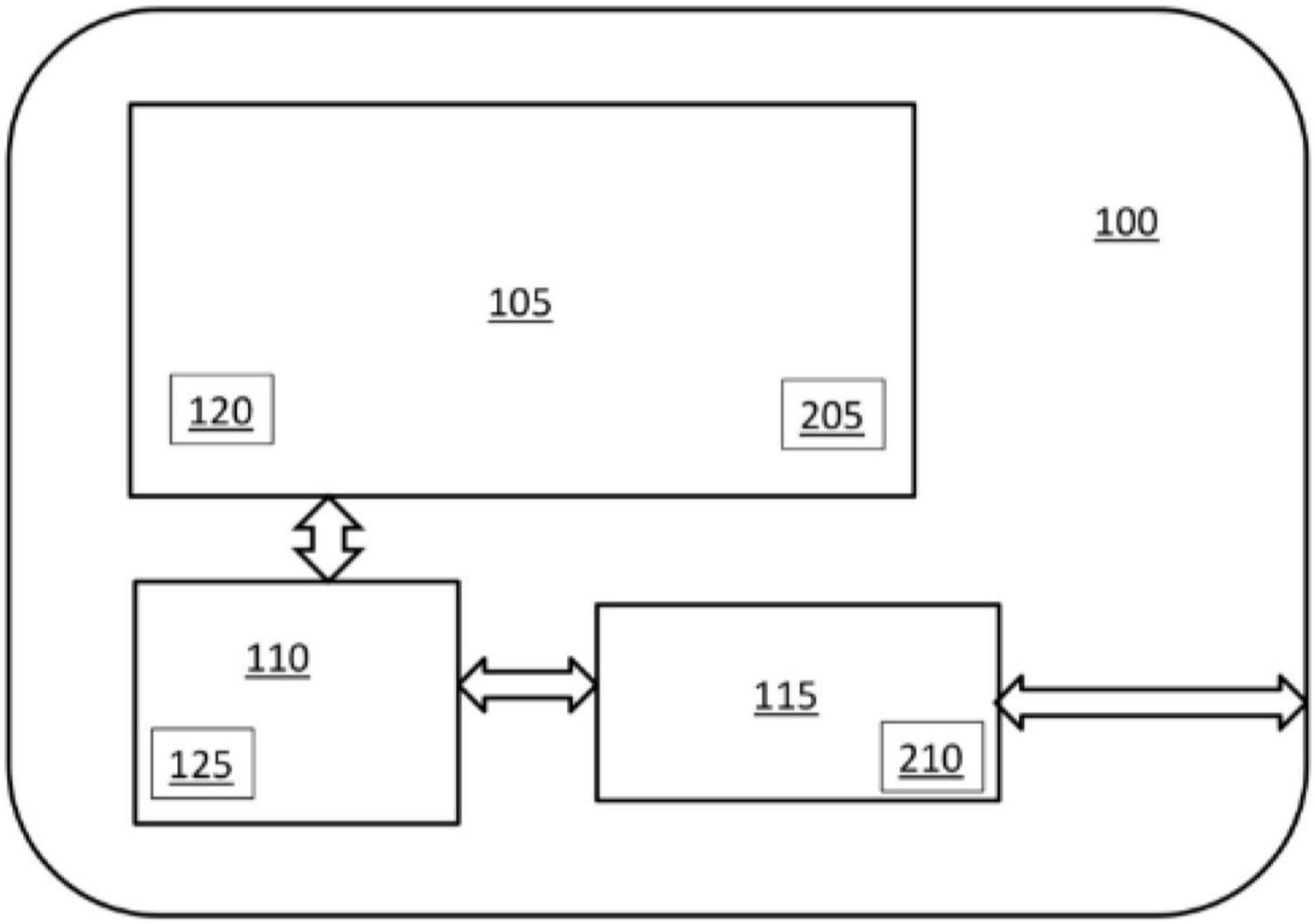
【請求項8】 如請求項7所述偵測一積體電路中之一物理性攻擊的方法，其中當該物理性攻擊事件被偵測，該方法配置為刪除該積體電路中一安全區域之資料。

【請求項9】 一計算機程式，用於計算機可讀取之指令，當該程式上載於一計算機時，配置該計算機以執行如請求項5-8任一項所述之方法。

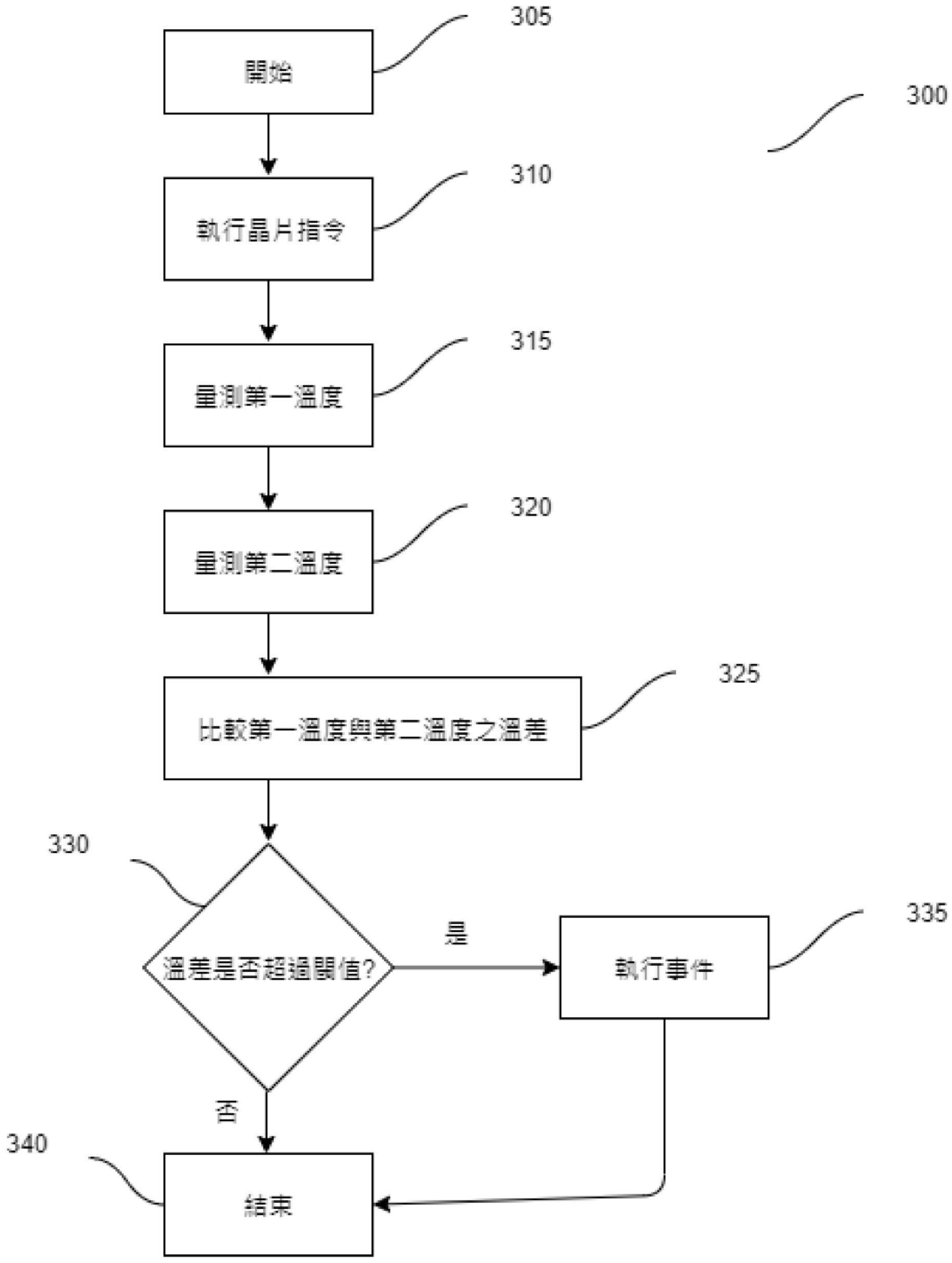
【發明圖式】



【圖1】



【圖2】


300
305
開始
310
執行晶片指令
315
量測第一溫度
320
量測第二溫度
325
比較第一溫度與第二溫度之溫差
330
溫差是否超過閾值?
是
335
執行事件
否
340
結束

【圖3】

指令	第一溫度	第二溫度	第三溫度	第四溫度
密碼	55	85	45	40
讀卡機	40	55	40	70
....				

【圖4】