I785952

(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 I785952 B**

(45)公告日： 中華民國 111 (2022) 年 12 月 01 日

(21)申請案號：110149562 (22)申請日： 中華民國 110 (2021) 年 12 月 30 日

(51)Int. Cl.： ***G06F21/72 (2013.01)***

(71)申請人：新唐科技股份有限公司 (中華民國) NUVOTON TECHNOLOGY CORPORATION (TW)

新竹市研新三路 4 號

(72)發明人：吳坤益 WU, KUN-YI (TW) ；李鈺珊 LI, YU-SHAN (TW)

(74)代理人：洪澄文；洪茂

(56)參考文獻：

TW 201812637A CN 113260994A

US 2019/0386815A1

審查人員：陳奕昌

申請專利範圍項數：10 項 圖式數：5 共 25 頁

(54)名稱

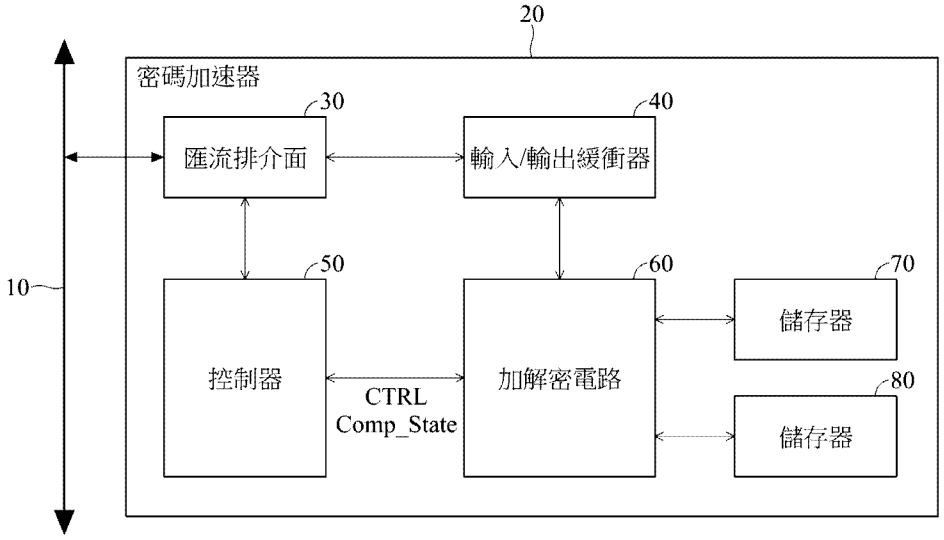
密碼加速器以及加解密運算的差分故障分析方法

(57)摘要

本發明提供密碼加速器。加解密電路用以根據控制信號執行加解密運算。加解密運算包括複數正常回合以及複數冗餘回合。控制器用以根據第一變數和第二變數提供控制信號至加解密電路，以控制加解密電路執行正常回合以及冗餘回合的順序。第一儲存器用以儲存執行正常回合的狀態。第二儲存器用以儲存執行冗餘回合的狀態。加解密電路根據第一變數將正常回合劃分成第一正常部分與第二正常部分，並根據第二變數將冗餘回合劃分成第一冗餘部分與第二冗餘部分。加解密電路是依序執行第一正常部分、第一冗餘部分、第二正常部分以及第二冗餘部分。

A cipher accelerator is provided. An encryption and decryption circuit is configured to perform encryption and decryption operations according to a control signal. Encryption and decryption operations include a plurality of normal rounds and a plurality of redundant rounds. A controller is configured to provide a control signal to the encryption and decryption circuit according to a first variable value and a second variable value, so as to control the sequence of the encryption and decryption circuit to execute the normal rounds and the redundant rounds. A first storage device is configured to store the state of executing the normal rounds. A second storage is configured to store the state of executing the redundant rounds. The encryption and decryption circuit divides the normal rounds into a first normal section and a second normal section according to the first variable value, and divides the redundant rounds into a first redundant section and a second redundant section according to the second variable value. The encryption and decryption circuit is configured to perform the first normal section, the first redundant section, the second normal section, and the second redundant section sequentially.

指定代表圖：



第 2 圖

符號簡單說明：

10:匯流排

20:密碼加速器

30:匯流排介面

40:輸入/輸出緩衝器

50:控制器

60:加解密電路

70,80:儲存器

CTRL:控制信號

Comp_State:信號

專利案號：110149562

公告本

I785952

【發明摘要】

【中文發明名稱】密碼加速器以及加解密運算的差分故障分析方法

【英文發明名稱】CIPHER ACCELERATOR AND DIFFERENTIAL FAULT ANALYSIS METHOD FOR ENCRYPTION AND DECRYPTION OPERATIONS

【中文】

本發明提供密碼加速器。加解密電路用以根據控制信號執行加解密運算。加解密運算包括複數正常回合以及複數冗餘回合。控制器用以根據第一變數和第二變數提供控制信號至加解密電路，以控制加解密電路執行正常回合以及冗餘回合的順序。第一儲存器用以儲存執行正常回合的狀態。第二儲存器用以儲存執行冗餘回合的狀態。加解密電路根據第一變數將正常回合劃分成第一正常部分與第二正常部分，並根據第二變數將冗餘回合劃分成第一冗餘部分與第二冗餘部分。加解密電路是依序執行第一正常部分、第一冗餘部分、第二正常部分以及第二冗餘部分。

【英文】

A cipher accelerator is provided. An encryption and decryption circuit is configured to perform encryption and decryption operations according to a control signal. Encryption and decryption operations include a plurality of

normal rounds and a plurality of redundant rounds. A controller is configured to provide a control signal to the encryption and decryption circuit according to a first variable value and a second variable value, so as to control the sequence of the encryption and decryption circuit to execute the normal rounds and the redundant rounds. A first storage device is configured to store the state of executing the normal rounds. A second storage is configured to store the state of executing the redundant rounds. The encryption and decryption circuit divides the normal rounds into a first normal section and a second normal section according to the first variable value, and divides the redundant rounds into a first redundant section and a second redundant section according to the second variable value. The encryption and decryption circuit is configured to perform the first normal section, the first redundant section, the second normal section, and the second redundant section sequentially.

【指定代表圖】第2圖

【代表圖之符號簡單說明】

10:匯流排

20:密碼加速器

30:匯流排介面

40:輸入/輸出緩衝器

50:控制器

60:加解密電路

70, 80:儲存器

CTRL:控制信號

Comp_State:信號

【特徵化學式】

無。

【發明說明書】

【中文發明名稱】 密碼加速器以及加解密運算的差分故障分析方法

【英文發明名稱】 CIPHER ACCELERATOR AND DIFFERENTIAL FAULT ANALYSIS METHOD FOR ENCRYPTION AND DECRYPTION OPERATIONS

【技術領域】

【0001】 本發明係有關於一種密碼加速器，且特別係有關於執行差分故障分析的密碼加速器。

【先前技術】

【0002】 近年來，加解密應用廣泛地使用各種電子產品中，而加解密應用非常重視如何保護機密資訊，以避免運算資料被分析而遭竊取。

【0003】 在加解密的過程中，電壓毛刺攻擊（Voltage Glitch attack）是通過快速改變輸入到積體電路的電壓，使得積體電路的一些電晶體會受到影響而產生錯誤的輸出值，從而導致處理器會操作錯誤或是對錯誤的資料進行處理。此外，積體電路內隱藏的資訊也會隨著處理器發生的錯誤而洩露出來。

【0004】 因此，分析運算中的資料是否被攻擊是加解密應用中需解決的問題之一。

【發明內容】

【0005】　本發明提供一種密碼加速器。上述密碼加速器包括一加解密電路、一控制器、一第一儲存器以及一第二儲存器。上述加解密電路用以根據一控制信號，執行一加解密運算。上述加解密運算包括複數正常回合以及複數冗餘回合。上述控制器用以根據一第一變數和一第二變數，提供上述控制信號至上述加解密電路，以控制上述加解密電路執行上述正常回合以及上述冗餘回合的順序。上述第一儲存器用以儲存執行上述正常回合的狀態。上述第二儲存器用以儲存執行上述冗餘回合的狀態。上述加解密電路根據上述控制信號的上述第一變數將上述正常回合劃分成一第一正常部分與一第二正常部分，以及根據上述控制信號的上述第二變數將上述冗餘回合劃分成一第一冗餘部分與一第二冗餘部分。上述加解密電路是依序執行上述第一正常部分、上述第一冗餘部分、上述第二正常部分以及上述第二冗餘部分，以完成上述加解密運算。

【0006】　再者，本發明提供一種加解密運算的差分故障分析方法，其中一加解密運算包括複數正常回合以及複數冗餘回合。經由一亂數產生器，得到一第一變數和一第二變數。根據上述第一變數，將上述正常回合劃分成一第一正常部分與一第二正常部分，並根據上述第二變數，將上述冗餘回合劃分成一第一冗餘部分與一第二冗餘部分。根據一時脈週期，依序執行上述第一正常部分、上述第一冗餘部分、上述第二正常部分以及上述第二冗餘部分。根據來自一第一儲存器且對應於上述第二正常部分的一第一狀態以及來自一第二儲存器且

對應於上述第二冗餘部分的一第二狀態，判斷上述加解密運算是否成功。

【圖式簡單說明】

【0007】

第1圖係顯示根據本發明一些實施例所述之執行加解密演算法的示意圖。

第2圖係顯示根據本發明一些實施例所述之密碼加速器。

第3圖係顯示根據本發明一些實施例所述之第2圖的控制器。

第4圖係顯示根據本發明一些實施例所述之執行加解密運算的差分故障分析方法。

第5圖係顯示根據本發明一些實施例所述之使用第4圖之方法執行加解密演算法的示意圖。

【實施方式】

【0008】 為讓本發明之上述和其他目的、特徵、和優點能更明顯易懂，下文特舉出較佳實施例，並配合所附圖式，作詳細說明如下：

【0009】 第1圖係顯示根據本發明一些實施例所述之執行加解密演算法的示意圖。在一些實施例中，加解密演算法可以是進階加密標準（Advanced Encryption Standard，AES）演算法，其是現

今被多方分析且廣為使用的演算法。在一些實施例中，加解密演算法可以是查查（ChaCha）演算法。

【0010】 在第1圖中，加解密演算法會執行多次的回合（round）。此外，每一回合是使用相同的電路來對前一回合的狀態執行相同或相似的運算。在第1圖中，加解密演算法會執行10個回合R1-R10。首先，根據輸入資料IN，第一回合R1會被執行，以得到輸出O1。接著，第一回合R1的輸出O1會被代入到第二回合R2進行運算，以得到輸出O2。接著，第二回合R2的輸出O2會被代入到第三回合R3進行運算，以得到輸出O3並被代入到第四回合R4。以此類推，第四回合R4至第十回合R10會依序被執行，並分別產生輸出O4至輸出O10。於是，完成具有10個回合R1-R10的加解密演算之後，可得到運算後的最後輸出O10。

【0011】 在積體電路執行加解密（加密/解密）運算的過程中，可透過正常回合R1-R10以及冗餘回合R1-R10來執行差分故障（differential fault）分析，以判斷加解密過程是否受到惡意攻擊（例如電壓毛刺（Voltage Glitch）攻擊）。首先，可根據輸入資料的初始狀態來執行正常回合R1-R10（以下稱為正常回合NR1-NR10），並得到由正常回合NR10所產生的正常回合輸出NO10。接著，根據輸入資料的初始狀態來執行冗餘的回合R1-R10（以下稱為冗餘回合）RR1-RR10，並得到由冗餘回合RR10所產生的冗餘回合輸出RO10。接著，判斷正常回合輸出NO10與冗餘回合輸出RO10是否相同。如果正常回合輸出NO10與冗餘回合輸出RO10一致，則表示加解密運算並

未發生故障(即加解密過程未被攻擊)。於是,可將正常回合輸出NO10傳送給其他電路,以執行後續操作。相反地,如果正常回合輸出NO10不同於冗餘回合輸出RO10,則表示加解密運算發生故障(即加解密過程被攻擊)。於是,積體電路會重新執行正常回合NR1-NR10以及冗餘回合RR1-RR10,直到正常回合輸出NO10與冗餘回合輸出RO10會一致。在一些實施例中,當正常回合輸出NO10不同於冗餘回合輸出RO10時,積體電路會直接結束加解密運算,並通知其他電路(例如藉由傳送特定值)加解密過程被攻擊而運算失敗。

【0012】 第2圖係顯示根據本發明一些實施例所述之密碼加速器(Cipher Accelerator)20。密碼加速器20實施於積體電路中,用以對經由匯流排10來自其他電路的資料進行加解密,並將已加密/已解密的資料傳送回原來的電路或是傳送至其他電路。

【0013】 密碼加速器20包括匯流排介面30、輸入/輸出緩衝器40、控制器50、加解密電路60、儲存器70和儲存器80。在一些實施例中,儲存器70和80可以是記憶體或是暫存器。匯流排介面30耦接於匯流排10。匯流排介面30可將匯流排10上其他電路的指令傳送至控制器50,並將控制器50所提供的回應傳送至匯流排10。此外,匯流排介面30可將欲加密或欲解密的資料傳送至輸入/輸出緩衝器40,並將來自輸入/輸出緩衝器40的已加密或已欲解密的資料傳送至匯流排10。

【0014】 相應於來自匯流排介面30的指令,控制器50會提供控制信號至加解密電路60,而控制信號CTRL包括加解密運算相關的有限狀態機(finite state machine,FSM)資訊。在一些實施例中,

控制器50可提供具有對應於正常模式的有限狀態機資訊或是對應於差分故障分析模式的有限狀態機資訊的控制信號CTRL至加解密電路60。

【0015】　在正常模式下，控制信號CTRL僅指示加解密電路60執行正常加解密運算而不會執行冗餘加解密運算，即加解密電路60僅執行正常回合NR。因此，在完成正常回合NR之後，加解密電路60會得到已加密/已解密資料，並將已加密/已解密資料傳送至輸入/輸出緩衝器40。於是，已加密/已解密資料會經由匯流排介面30而提供至匯流排10，以供其他電路執行後續程序。

【0016】　在差分故障分析模式下，除了正常加解密運算之外，控制信號CTRL更指示加解密電路60執行冗餘加解密運算，即加解密電路60會進一步執行冗餘回合RR。在完成正常加解密運算與冗餘加解密運算之後，加解密電路60會將兩者的結果進行比較，以判斷正常加解密運算與冗餘加解密運算的運算結果是否一致。如果正常加解密運算與冗餘加解密運算的運算結果不一致，則加解密電路60會提供信號Comp_State至控制器50，以便通知控制器50有故障發生。反之，如果正常加解密運算與冗餘加解密運算的運算結果為相同，加解密電路60會將已加密/已解密資料傳送至輸入/輸出緩衝器40。於是，已加密/已解密資料會經由匯流排介面30而提供至匯流排10，以供其他電路執行後續程序。

【0017】　在差分故障分析模式下，密碼加速器20執行正常加解密運算過程中所產生的結果（狀態）是儲存在儲存器70，而執行冗

餘加解密運算過程中所產生的結果（狀態）是儲存在儲存器80。此外，執行冗餘加解密運算所需的冗餘回合RR的數量會少於執行正常加解密運算所需的正常回合NR的數量。換言之，執行冗餘加解密運算所需的時間（即時脈週期的數量）是少於執行正常加解密運算所需的時間（即時脈週期的數量）。因此，使用密碼加速器20可加速差分故障分析操作並減少所需要的分析時間。

【0018】　第3圖係顯示根據本發明一些實施例所述之第2圖的控制器50。控制器50包括多工器（multiplexer，MUX）150、處理器110、正常模式有限狀態機單元120、分析模式有限狀態機單元130以及亂數產生器140。在第3圖中，為了簡化說明，控制器50僅描述相關的電路，而其他電路將省略。

【0019】　在正常模式下，處理器110會控制正常模式有限狀態機單元120產生對應於正常加解密運算的有限狀態機資訊Normal_FSM。此外，在差分故障分析模式下，處理器110會控制分析模式有限狀態機單元130產生對應於正常加解密運算結合冗餘加解密運算的有限狀態機資訊TRRSM_FSM。值得注意的是，分析模式有限狀態機單元130會根據來自亂數產生器的隨機變數RNG而提供有限狀態機資訊TRRSM_FSM。此外，執行冗餘加解密運算所需的冗餘回合RR的數量是由隨機變數RNG所決定。換言之，每次執行冗餘加解密運算所需的冗餘回合RR的數量是可變的。

【0020】　同時參考第2圖和第3圖，在正常模式下，處理器110會控制多工器150選擇來自正常模式有限狀態機單元120的有限狀態

機資訊Normal_FSM，以作為控制信號CTRL。此外，在差分故障分析模式下，處理器110會控制多工器150選擇來自分析模式有限狀態機單元130的有限狀態機資訊TRRSM_FSM，以作為控制信號CTRL。

【0021】 如先前所描述，在差分故障分析模式下，加解密電路60會判斷正常加解密運算與冗餘加解密運算的運算結果是否一致，並提供信號Comp_State至控制器50，以便通知控制器50是否有故障發生。當信號Comp_State指示有故障發生時，處理器110會控制分析模式有限狀態機單元130再次產生有限狀態機資訊TRRSM_FSM，以便控制加解密電路60重新執行正常加解密運算與冗餘加解密運算。在一些實施例中，當信號Comp_State指示有故障發生時，處理器110會直接結束加解密運算，並通知其他電路（例如藉由傳送特定值）加解密過程被攻擊而運算失敗。

【0022】 第4圖係顯示根據本發明一些實施例所述之執行加解密運算的差分故障分析方法200。根據差分故障分析方法200，密碼加速器20可提供具有時間冗餘隨機交換機制（timing redundancy random swapping mechanism）的有限狀態機資訊TRRSM_FSM來執行差分故障分析。第5圖係顯示根據本發明一些實施例所述之使用第4圖之差分故障分析方法200執行加解密演算法的示意圖。為了方便說明，假設第5圖中正常回合NR的總數量為10，即加解密運算需要執行正常回合NR1-NR10。

【0023】 同時參考第4圖和第5圖，首先，在步驟S210，得到隨機變數RNG。隨機變數RNG包括第一變數x以及第二變數y。當正

常回合NR的總數量為10時，第一變數x可以是整數1至整數7之間的隨機值（即1≤x≤7），而第二變數y可以是0至整數10減去第一變數x之間的隨機值（即0≤y≤(10-x)）。在此實施例中，假設第一變數x為5（即x=5）而第二變數y為2（即y=2）。此外，第一變數x與第二變數y的總和是小於或等於正常回合NR的總數量（即x+y≤10）。

【0024】 在步驟S220，根據第一變數x，將正常回合NR1-NR10劃分成第一正常部分NR_SEC1以及第二正常部分NR_SEC2。如第5圖所顯示，第一正常部分NR_SEC1包括正常回合NR1、NR2、NR3、NR4和NR5，而第二正常部分NR_SEC2包括正常回合NR6、NR7、NR8、NR9和NR10。再者，根據第一變數x以及正常回合NR的總數量，可得到冗餘回合RR的數量為5（即10-x=5）。值得注意的是，每一冗餘回合RR的操作是相同於所對應的正常回合NR。例如，冗餘回合RR6、RR7、RR8、RR9和RR10的操作是分別對應於正常回合NR6、NR7、NR8、NR9和NR10的操作。換言之，冗餘回合RR6-RR10的數量是相同於第二正常部分NR_SEC2中正常回合NR6-NR10的數量，且冗餘回合RR6-RR10的操作是相同於第二正常部分NR_SEC2。

【0025】 接著，根據第二變數y，將冗餘回合RR6-RR10劃分成第一冗餘部分RR_SEC1以及第二冗餘部分RR_SEC2。如第5圖所顯示，第一冗餘部分RR_SEC1包括冗餘回合RR6和RR7，而第二冗餘部分RR_SEC2包括冗餘回合RR8、RR9和RR10。

【0026】　在步驟S230中，分析模式有限狀態機單元130會產生有限狀態機資訊TRRSM_FSM，以便控制加解密電路60根據一時脈週期來依序執行第一正常部分NR_SEC1、第一冗餘部分RR_SEC1、第二正常部分NR_SEC2以及第二冗餘部分RR_SEC2。

【0027】　如第5圖所顯示，第一正常部分NR_SEC1的正常回合NR1會被先執行，以得到輸出NO1，並將輸出NO1儲存在儲存器70。接著，正常回合NR1的輸出NO1會被代入到正常回合NR2進行運算，以得到輸出NO2，並將輸出NO2儲存在儲存器70。於是，儲存在儲存器70內執行正常加解密運算所產生的狀態會被更新為輸出NO2。以此類推，正常回合NR3至正常回合NR5會依序被執行，並分別產生輸出NO3至NO5。此外，儲存在儲存器70內執行正常加解密運算所產生的狀態會依序被更新為輸出NO3、NO4和NO5。於是，完成第一正常部分NR_SEC1。

【0028】　在一些實施例中，在完成正常回合NR5之後，除了將輸出NO5儲存至儲存器70之外，加解密電路60更將輸出NO5儲存至儲存器80。

【0029】　在完成第一正常部分NR_SEC1之後，加解密電路60會將輸出NO5代入到第一冗餘部分RR_SEC1的冗餘回合RR6進行運算，以得到輸出RO6，並將輸出RO6儲存在儲存器80。於是，儲存在儲存器80內的狀態會被更新為輸出RO6。接著，冗餘回合RR6的輸出RO6會被代入到冗餘回合RR7進行運算，以得到輸出RO7，並將輸出RO7儲存在儲存器80。於是，儲存在儲存器80內執行冗餘加解密運算

所產生的狀態被更新為輸出RO7。於是，完成第一冗餘部分RR_SEC1。

【0030】 在完成第一冗餘部分RR_SEC1之後，加解密電路60會將儲存在儲存器70內的輸出NO5代入到第二正常部分NR_SEC2的正常回合NR6進行運算，以得到輸出NO6，並將輸出NO6儲存在儲存器70。接著，正常回合NR6的輸出NO6會被代入到正常回合NR7進行運算，以得到輸出NO7，並將輸出NO7儲存在儲存器70。以此類推，正常回合NR8至正常回合NR10會依序被執行，並分別產生輸出NO8至NO10。此外，儲存在儲存器70內執行正常加解密運算所產生的狀態會依序被更新為輸出NO8、NO9和NO10。於是，完成第二正常部分NR_SEC2，以及儲存在儲存器70內執行正常加解密運算所產生的狀態最後被更新為輸出NO10。

【0031】 在完成第二正常部分NR_SEC2之後，加解密電路60會將儲存在儲存器80內的輸出RO7代入到第二冗餘部分RR_SEC2的冗餘回合RR8進行運算，以得到輸出RO8，並將輸出RO8儲存在儲存器80。接著，冗餘回合RR8的輸出RO8會被代入到冗餘回合RR9進行運算，以得到輸出RO9，並將輸出RO9儲存在儲存器80。接著，冗餘回合RR9的輸出RO9會被代入到冗餘回合RR10進行運算，以得到輸出RO10，並將輸出RO10儲存在儲存器80。於是，儲存在儲存器80內執行冗餘加解密運算所產生的狀態最後被更新為輸出RO10。於是，完成第二冗餘部分RR_SEC2。

【0032】　參考回差分故障分析方法200，在步驟S240中，加解密電路60會比較儲存在儲存器70內的正常回合NR的最後輸出NR10以及儲存在儲存器80內的冗餘回合RR的最後輸出RR10是否一致。如果輸出NR10相同於輸出RR10，則加解密電路60會根據輸出NR10完成加解密運算，並提供已完成加解密的資料至輸入/輸出緩衝器40，以便經由匯流排介面30傳送至匯流排10。反之，如果輸出NR10不同於輸出RR10，則加解密電路60會提供信號Comp_State至控制器50，以便通知控制器50有故障發生。

【0033】　在第5圖中，第一正常部分NR_SEC1是在時間t0（例如t0=0）開始執行。接著，第一冗餘部分RR_SEC1是在時間t1（例如t1=x）開始執行。接著，第二正常部分NR_SEC2是在時間t2（例如t2=x+y）開始執行。接著，第二冗餘部分RR_SEC2是在時間t3（例如t3=10+y）開始執行。最後，第二冗餘部分RR_SEC2是在時間t4（例如t4=20-y）執行結束。換言之，正常回合NR與冗餘回合RR是交互執行。此外，僅有後半部之冗餘回合RR（例如冗餘回合RR6-RR10）需要被執行。相較於需執行全部冗餘回合RR（例如冗餘回合RR1-RR10）或是需加入附加隨機時脈周期（random cycle）/閒置周期（idle cycle）的傳統差分故障分析，本發明實施例僅需執行部分之冗餘回合RR，於是可減少分析時間。

【0034】　在本發明實施例中，正常回合NR與冗餘回合RR各自的結束時間是由隨機變數RNG所保護。例如，可使用第一變數x來保護冗餘回合RR的結束時間（例如冗餘回合RR10的結束時間），並使

用第二變數y來保護正常回合NR的結束時間(例如正常回合NR10的結束時間）。由於冗餘回合RR的結束時間與正常回合NR的結束時間是分別由不同的變數（例如第一變數x和第二變數y）所決定，因此增加了攻擊的難度。相較於冗餘回合RR與/或正常回合NR具有固定結束時間的傳統差分故障分析，本發明實施例可避免攻擊者在正常回合NR和冗餘回合RR的關鍵時間點製造相同的故障，進而改善時間冗餘機制。

【0035】　雖然本發明已以較佳實施例發明如上，然其並非用以限定本發明，任何所屬技術領域中包括通常知識者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【符號說明】

【0036】

10:匯流排

20:密碼加速器

30:匯流排介面

40:輸入/輸出緩衝器

50:控制器

60:加解密電路

70, 80:儲存器

110:處理器

120:正常模式有限狀態機單元

130:分析模式有限狀態機單元

140:亂數產生器

150:多工器

200:方法

CTRL:控制信號

Comp_State:信號

IN:輸入資料

Normal_FSM, TRRSM_FSM:有限狀態機資訊

NR, NR1-NR10:正常回合

NR_SEC1:第一正常部分

NR_SEC2:第二正常部分

NO1-NO10, O1-O10, RO6-RO10:輸出

R1-R10:回合

RNG:隨機變數

RR, RR6-RR10:冗餘回合

RR_SEC1:第一冗餘部分

RR_SEC2:第二冗餘部分

S210-S240:步驟

t0-t4:時間

x:第一變數

y:第二變數

【發明申請專利範圍】

【請求項1】 一種密碼加速器，包括：

一加解密電路，用以根據一控制信號，執行一加解密運算，其中上述加解密運算包括複數正常回合以及複數冗餘回合；

一控制器，用以根據一第一變數和一第二變數，提供上述控制信號至上述加解密電路，以控制上述加解密電路執行上述正常回合以及上述冗餘回合，以便完成上述加解密運算；

一第一儲存器，用以儲存執行上述正常回合的狀態；以及

一第二儲存器，用以儲存執行上述冗餘回合的狀態；

其中上述加解密電路根據上述控制信號的上述第一變數將上述正常回合劃分成一第一正常部分與一第二正常部分，使得上述第一正常部分的上述正常回合的數量相同於上述第一變數，以及上述加解密電路根據上述控制信號的上述第二變數將上述冗餘回合劃分成一第一冗餘部分與一第二冗餘部分，使得上述第一冗餘部分的上述冗餘回合的數量相同於上述第二變數；

其中上述加解密電路是依序執行上述第一正常部分、上述第一冗餘部分、上述第二正常部分以及上述第二冗餘部分，以完成上述加解密運算。

【請求項2】 如請求項1之密碼加速器，其中上述冗餘回合的操作是相同於上述第二正常部分。

【請求項3】 如請求項1之密碼加速器，其中上述冗餘回合的數量是相同於上述第二正常部分的上述正常回合的數量。

【請求項4】 如請求項1之密碼加速器，其中當上述加解密電路依序執行上述第一正常部分的每一上述正常回合至一第一正常回合時，上述加解密電路將對應於上述第一正常回合的一第一狀態儲存至上述第一儲存器，並根據上述第一狀態執行上述第一冗餘部分。

【請求項5】 如請求項4之密碼加速器，其中當上述加解密電路根據上述第一狀態依序執行上述第一冗餘部分的每一上述冗餘回合至一第一冗餘回合時，上述加解密電路將對應於上述第一冗餘回合的一第二狀態儲存至上述第二儲存器，並根據儲存在上述第一儲存器的上述第一狀態執行上述第二正常部分。

【請求項6】 如請求項5之密碼加速器，其中當上述加解密電路根據上述第一狀態依序執行上述第二正常部分的每一上述正常回合至一第二正常回合時，上述加解密電路將對應於上述第二正常回合的一第三狀態儲存至上述第一儲存器，並根據儲存在上述第二儲存器的上述第二狀態依序執行上述第二冗餘部分。

【請求項7】 如請求項6之密碼加速器，其中當上述加解密電路依據上述第二狀態依序執行上述第二冗餘部分的每一上述冗餘回合至一第二冗餘回合時，上述加解密電路將對應於上述第二冗餘回合的一第四狀態儲存至上述第二儲存器。

【請求項8】 如請求項7之密碼加速器，其中當上述第一儲存器的上述第三狀態相同於上述第二儲存器的上述第四狀態時，上述加解密電路判斷上述加解密運算為成功。

【請求項9】 一種加解密運算的差分故障分析方法，其中一加解密運算包括複數正常回合以及複數冗餘回合，上述差分故障分析方法包括：

經由一亂數產生器，得到一第一變數和一第二變數；

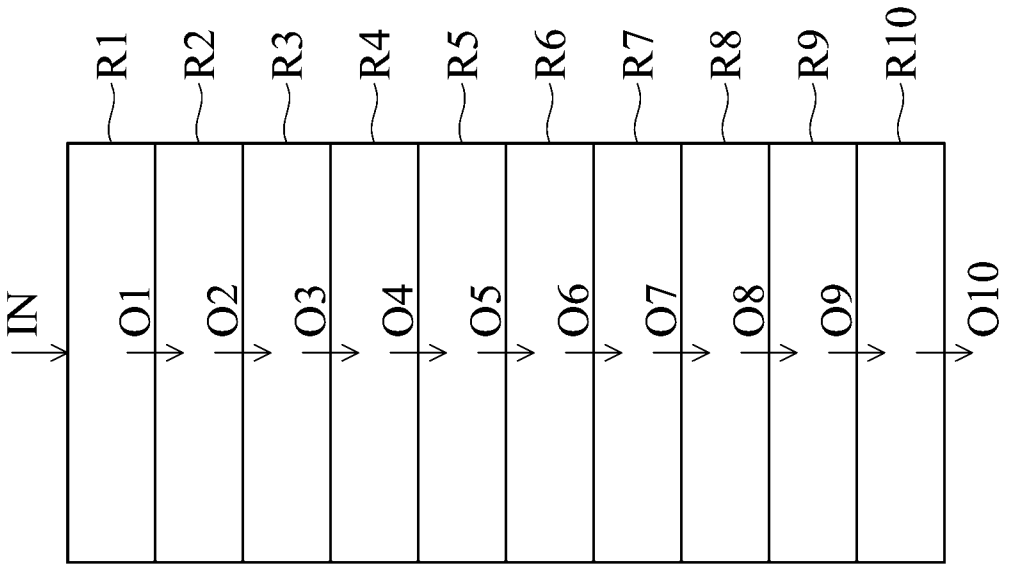
根據上述第一變數，將上述正常回合劃分成一第一正常部分與一第二正常部分，使得上述第一正常部分的上述正常回合的數量相同於上述第一變數，並根據上述第二變數，將上述冗餘回合劃分成一第一冗餘部分與一第二冗餘部分，使得上述第一冗餘部分的上述冗餘回合的數量相同於上述第二變數；

根據一時脈週期，依序執行上述第一正常部分、上述第一冗餘部分、上述第二正常部分以及上述第二冗餘部分；以及

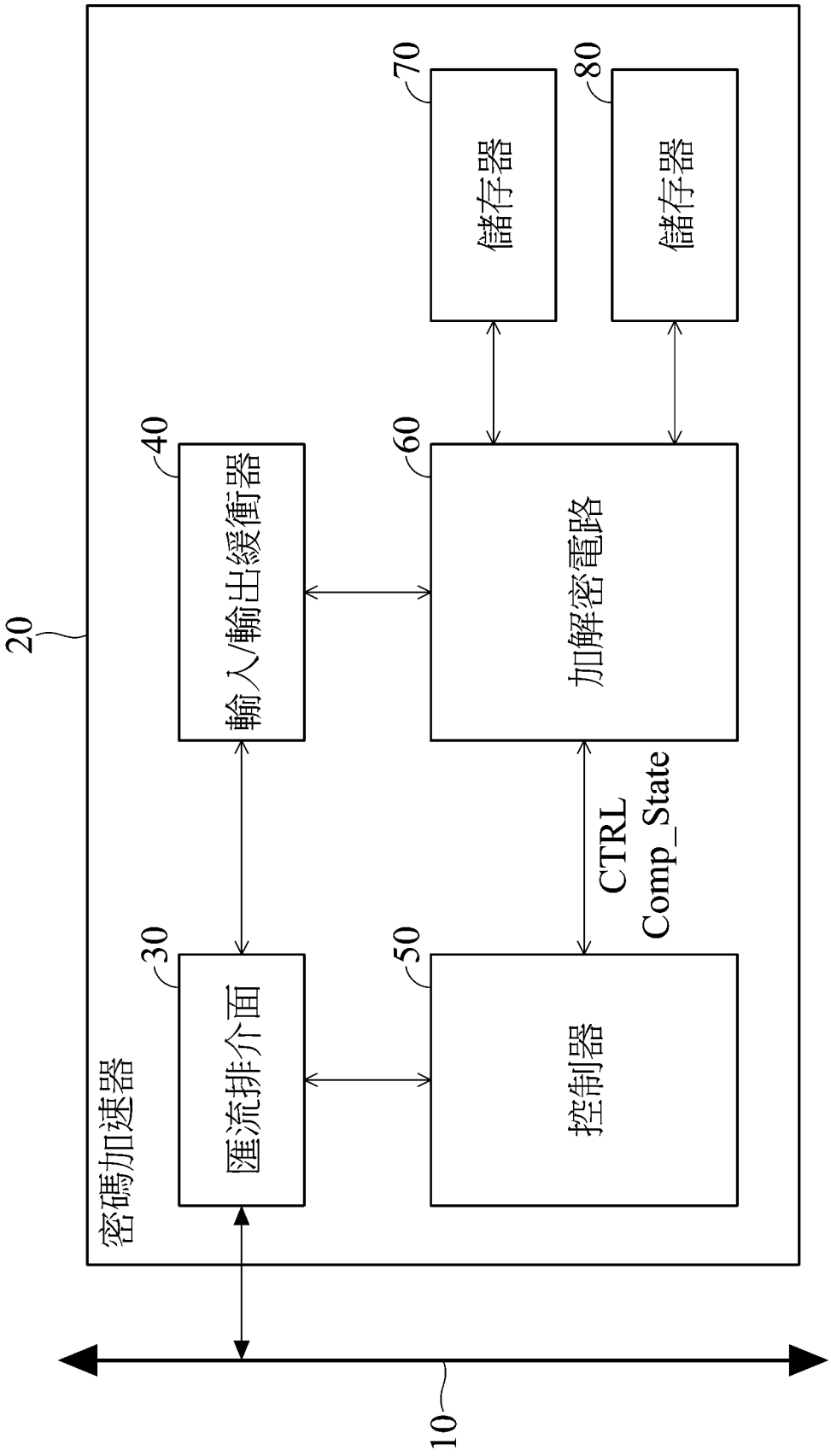
根據來自一第一儲存器且對應於上述第二正常部分的一第一狀態以及來自一第二儲存器且對應於上述第二冗餘部分的一第二狀態，判斷上述加解密運算是否成功。

【請求項10】 如請求項9之加解密運算的差分故障分析方法；其中上述正常回合的數量是大於上述冗餘回合的數量，以及上述冗餘回合的數量是等於上述正常回合的數量減去上述第一變數，其中上述第一變數與上述第二變數的總和是小於或等於上述正常回合的數量。

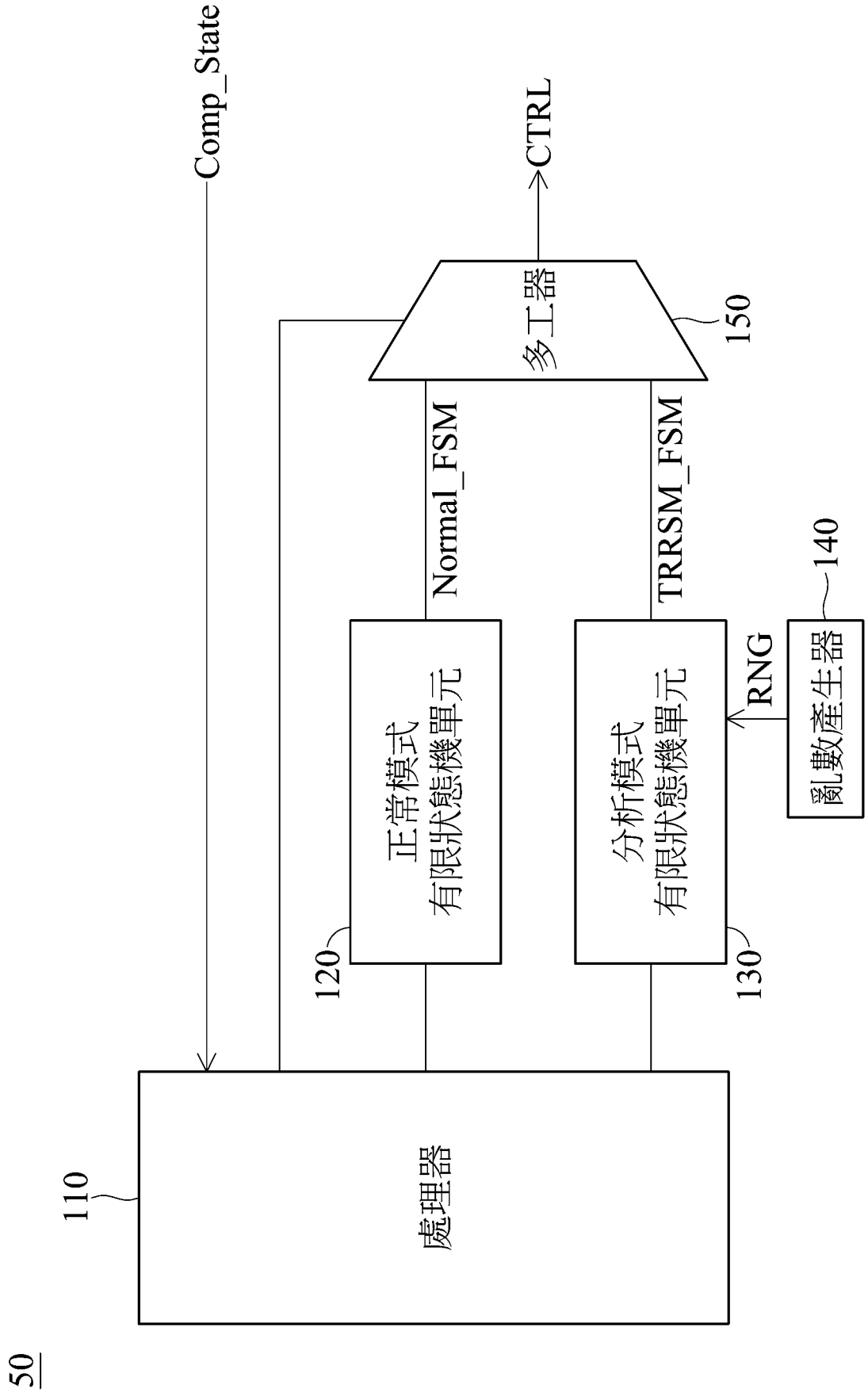
【發明圖式】



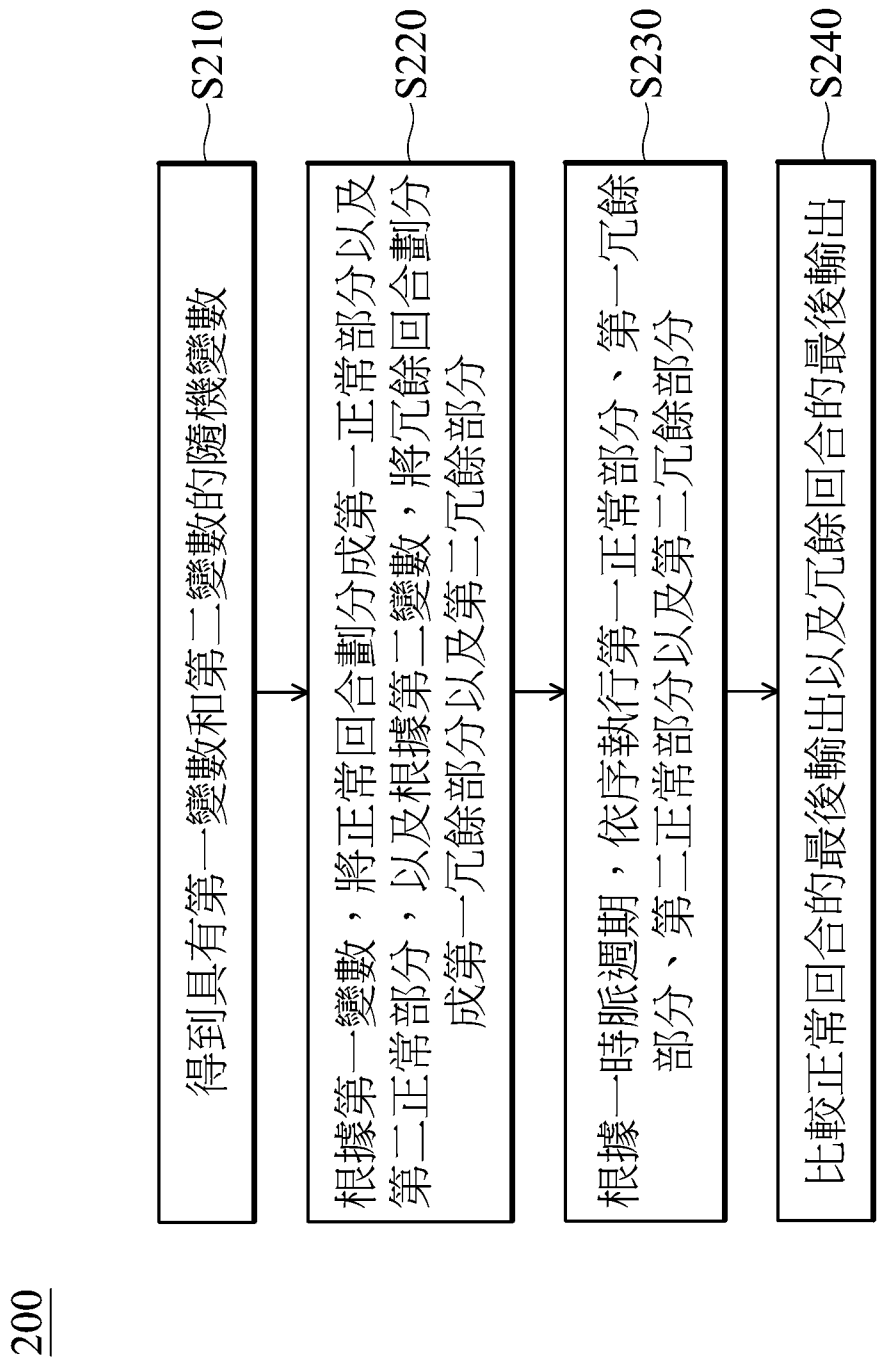
第 1 圖


20
密碼加速器
30
匯流排介面
40
輸入/輸出緩衝器
50
控制器
60
加解密電路
70
儲存器
80
儲存器
CTRL
Comp_State
10

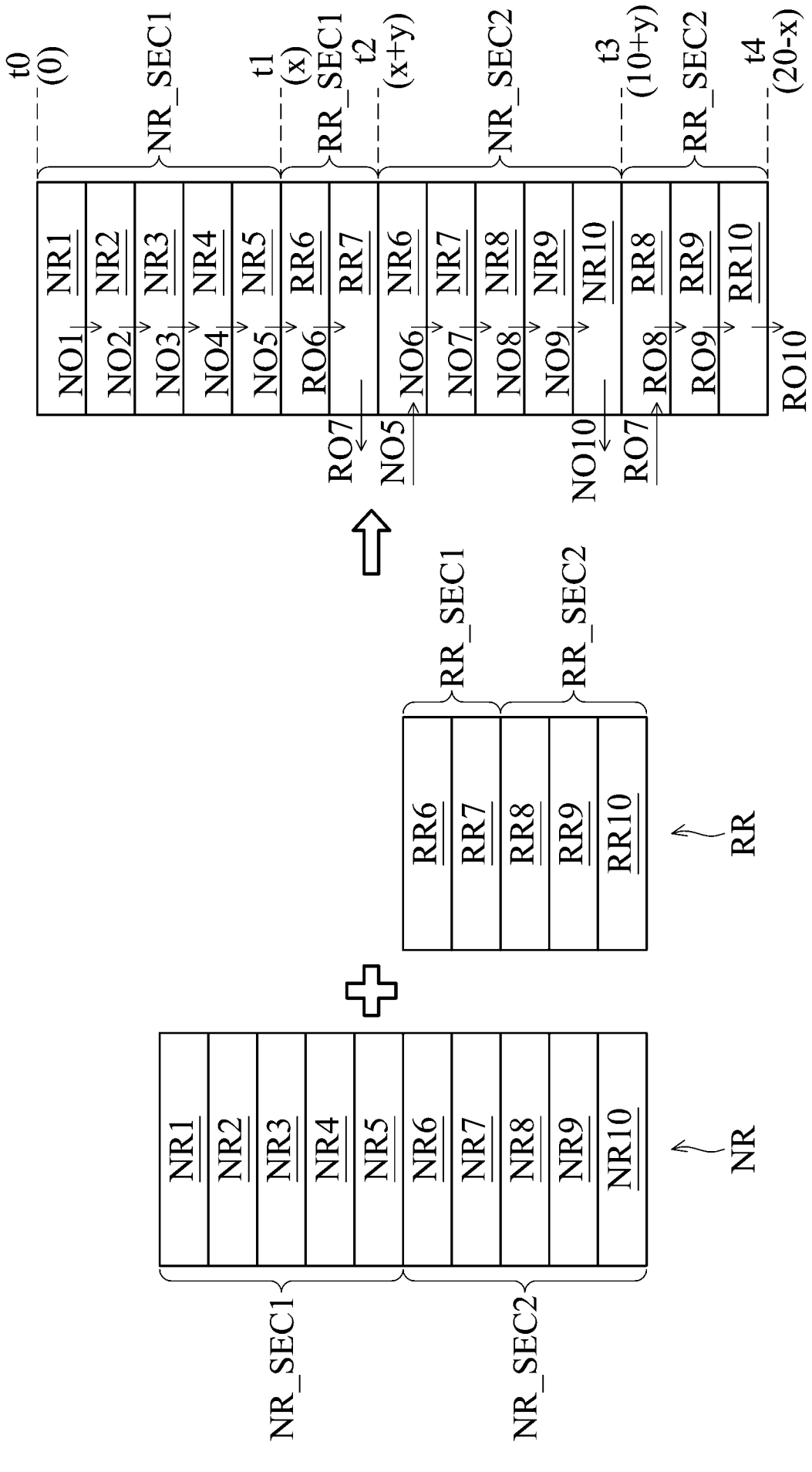
第 2 圖


50
110
處理器
120
正常模式
有限狀態機單元
130
分析模式
有限狀態機單元
140
亂數產生器
RNG
Normal_FSM
TRRSM_FSM
150
多工器
CTRL
Comp_State

第 3 圖


200
S210
得到具有第一變數和第二變數的隨機變數
S220
根據第一變數，將正常回合劃分成第一正常部分以及第二正常部分，以及根據第二變數，將冗餘回合劃分成第一冗餘部分以及第二冗餘部分
S230
根據一時脈週期，依序執行第一正常部分、第一冗餘部分、第二正常部分以及第二冗餘部分
S240
比較正常回合的最後輸出以及冗餘回合的最後輸出

第 4 圖


t0
(0)
NR_SEC1
t1
(x)
RR_SEC1
t2
(x+y)
NR_SEC2
t3
(10+y)
RR_SEC2
t4
(20-x)
NR1
NR2
NR3
NR4
NR5
RR6
RR7
NR6
NR7
NR8
NR9
NR10
RR8
RR9
RR10
NO1
NO2
NO3
NO4
NO5
RO6
RO7
NO6
NO7
NO8
NO9
NO10
RO8
RO9
RO10
RO7
NO5
NO10
RO7
RR_SEC1
RR_SEC2
RR6
RR7
RR8
RR9
RR10
RR
NR1
NR2
NR3
NR4
NR5
NR6
NR7
NR8
NR9
NR10
NR
NR_SEC1
NR_SEC2

第 5 圖