I693530

(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 I693530 B**

(45)公告日： 中華民國 109 (2020) 年 05 月 11 日

(21)申請案號：107131405　(22)申請日： 中華民國 107 (2018) 年 09 月 07 日

(51)Int. Cl.：　*G06F21/62　(2013.01)*　*G11C8/20　(2006.01)*

(30)優先權：2017/09/12　美國　62/557,170

(71)申請人：力旺電子股份有限公司 (中華民國) EMEMORY TECHNOLOGY INC.　(TW)
新竹市新竹科學園區園區二路四十七號三〇五室

(72)發明人：陳信銘 CHEN, HSIN-MING (TW)；吳孟益 WU, MENG-YI (TW)；黃柏豪 HUANG, PO-HAO (TW)

(74)代理人：吳豐任；戴俊彥

(56)參考文獻：

TW	201727657A	US	9613714B1
WO	2013/101085A1	WO	2016/102164A1

審查人員：陳奕昌

申請專利範圍項數：23 項　圖式數：5　共 28 頁

(54)名稱

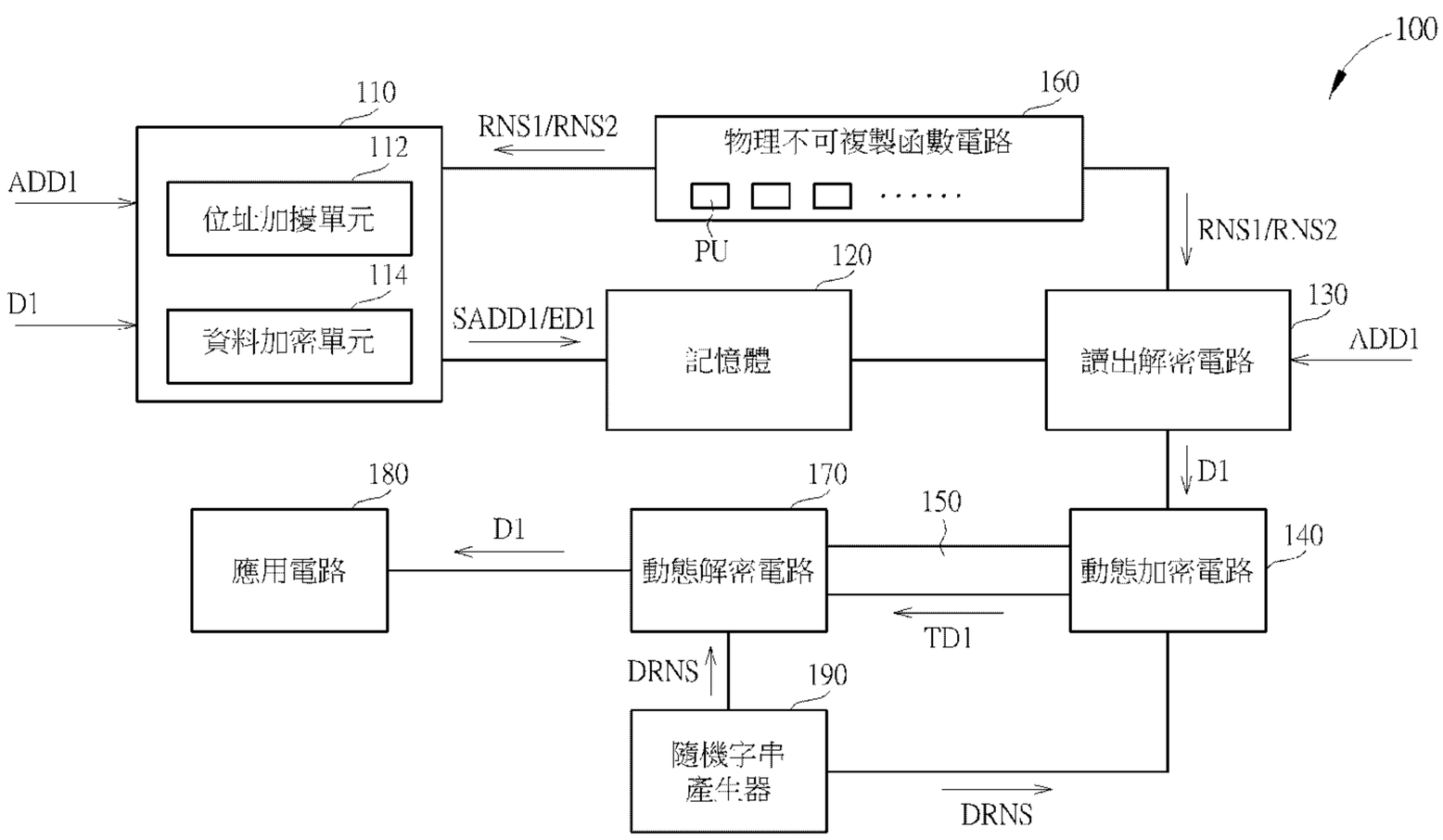
安全系統及安全系統的操作方法

(57)摘要

安全系統包含物理不可複製函數電路、寫入保護電路、記憶體及讀出解密電路。物理不可複製函數電路提供複數個隨機字串。寫入保護電路接收寫入位址及原始資料，並包含位址加擾單元。位址加擾單元根據物理不可複製函數電路所提供的隨機字串加擾寫入位址以產生加擾位址。記憶體根據加擾位址儲存對應於原始資料的儲存資料。讀出解密電路根據寫入位址自記憶體讀出儲存資料以取得原始資料。

A security system includes a physical unclonable function circuit, a write in protection circuit, a memory, and a readout decryption circuit. The physical unclonable function circuit provides a plurality of random bit strings. The write in protection circuit receives a write in address and original data, and includes an address scrambling unit. The address scrambling unit generates a scrambled address by scrambling a write in address according a random bit string provided by the physical unclonable function circuit. The memory stores the storage data corresponding to the original data according to the scrambled address. The readout decryption circuit reads out the storage data from the memory according to the write in address to derive the original data.

指定代表圖：



第1圖

符號簡單說明：

100・・・安全系統

110・・・寫入保護電路

112・・・位址加擾單元

114・・・資料加密單元

120・・・記憶體

130・・・讀出解密電路

140・・・動態加密電路

150・・・傳輸匯流排

160・・・物理不可複製函數電路

170・・・動態解密電路

180・・・應用電路

190・・・隨機字串產生器

RNS1、RNS2・・・隨機字串

DRNS・・・動態隨機字串

D1・・・原始資料

ED1・・・儲存資料

TD1・・・傳輸資料

ADD1・・・寫入位址

SADD1・・・加擾寫入位址

PU・・・物理不可複製函數單元

專利案號：107131405

公告本

I693530

【發明摘要】

【中文發明名稱】安全系統及安全系統的操作方法

【英文發明名稱】SECURITY SYSTEM AND METHOD FOR OPERATING A SECURITY SYSTEM

【中文】

安全系統包含物理不可複製函數電路、寫入保護電路、記憶體及讀出解密電路。物理不可複製函數電路提供複數個隨機字串。寫入保護電路接收寫入位址及原始資料，並包含位址加擾單元。位址加擾單元根據物理不可複製函數電路所提供的隨機字串加擾寫入位址以產生加擾位址。記憶體根據加擾位址儲存對應於原始資料的儲存資料。讀出解密電路根據寫入位址自記憶體讀出儲存資料以取得原始資料。

【英文】

A security system includes a physical unclonable function circuit, a write in protection circuit, a memory, and a readout decryption circuit. The physical unclonable function circuit provides a plurality of random bit strings. The write in protection circuit receives a write in address and original data, and includes an address scrambling unit. The address scrambling unit generates a scrambled address by scrambling a write in address according a random bit string provided by the physical unclonable function circuit. The memory stores the storage data corresponding to the original data according to the scrambled address. The readout decryption circuit reads out the storage data from the memory according to the write in address to derive the original data.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

100	安全系統
110	寫入保護電路
112	位址加擾單元
114	資料加密單元
120	記憶體
130	讀出解密電路
140	動態加密電路
150	傳輸匯流排
160	物理不可複製函數電路
170	動態解密電路
180	應用電路
190	隨機字串產生器
RNS1、RNS2	隨機字串
DRNS	動態隨機字串
D1	原始資料
ED1	儲存資料
TD1	傳輸資料
ADD1	寫入位址
SADD1	加擾寫入位址
PU	物理不可複製函數單元

【特徵化學式】

無

【發明說明書】

【中文發明名稱】安全系統及安全系統的操作方法

【英文發明名稱】SECURITY SYSTEM AND METHOD FOR OPERATING A SECURITY SYSTEM

【技術領域】

【0001】　本發明是有關於一種安全系統，特別是指一種利用亂數字串來提升資料安全的安全系統。

【先前技術】

【0002】　隨著電子裝置所應用的領域越來越廣，電子裝置所處理的資訊也越來越多。有時電子裝置可能會需要處理較為敏感的資訊。在此情況下，就可能會利用電子裝置中獨特的安全金鑰來做身分識別及資訊保護。然而，由於晶片和裝置的逆向工程方法已經能夠自動化，因此物理和旁通道攻擊也變得越來越強大，且成本也越能夠負擔。因此曝露敏感資訊的問題也引發了人們的擔憂。

【0003】　為防止電子裝置被未授權者存取，電子裝置的製造者常需要投入大量的時間和金錢來發展反測量技術以防範外來的威脅。在先前技術中，由於物理不可複製函數(physical unclonable function，PUF)之積體電路的先天特性，物理不可複製函數之積體電路常被應用於保護系統免於物理攻擊，並提高逆向工程或駭入系統所需跨越的門檻。

【0004】　物理不可複製函數可以根據其在製造過程中無法控制的隨機物理特性產生獨特的位元字串。製程中產生的變異可能會來自製程操作上的極小變動、材料內容及/或環境參數的偏移。這些無法避免且無法預測的變異會被物理

不可複製函數放大，進而產生獨特的位元字串。

【0005】　雖然物理不可複製函數能夠產生難以預測的亂數位元或安全金鑰，然而這些機密資訊需要固定儲存在系統中，所以常常會儲存在非揮發性的記憶體中。因此若是以傳統的方式儲存在記憶體中，對手便很可能在取得記憶體之後，透過旁通道攻擊或其他的駭客手法破解取得其中的資訊，導致整個系統的資訊安全都陷入威脅。因此如何有效提升系統的安全性仍然是有待解決的問題。

【發明內容】

【0006】　本發明之一實施例提供一種安全系統。安全系統包含物理不可複製函數電路、寫入保護電路、記憶體及讀出解密電路。

【0007】　物理不可複製函數電路提供複數個隨機字串。寫入保護電路接收寫入位址及原始資料。寫入保護電路包含位址加擾單元，位址加擾單元根據物理不可複製函數電路所提供的隨機字串加擾寫入位址以產生加擾位址。

【0008】　記憶體耦接於寫入保護電路，並根據加擾位址儲存對應於原始資料之儲存資料。

【0009】　讀出解密電路耦接於記憶體，並根據寫入位址自記憶體讀出儲存資料以取得原始資料。

【0010】　本發明之另一實施例提供一種安全系統的操作方法。安全系統包含寫入保護電路、記憶體、物理不可複製函數電路及讀出解密電路。

【0011】　安全系統的操作方法包含物理不可複製函數電路提供複數個隨機字串以產生隨機字串，寫入保護電路接收寫入位址及原始資料，寫入保護電路根據隨機字串加擾寫入位址以產生加擾位址，記憶體根據加擾位址儲存對應於原始資料之儲存資料，及讀出解密電路根據寫入位址自記憶體讀出儲存資料以取得原始資料。

【圖式簡單說明】

【0012】

第1圖為本發明一實施例之安全系統的示意圖。

第2圖為第1圖物理不可複製函數電路之物理不可複製函數單元的示意圖。

第3圖為本發明另一實施例之物理不可複製函數單元的示意圖。

第4圖為本發明另一實施例之物理不可複製函數單元的示意圖。

第5圖為第1圖之安全系統的操作方法流程圖。

【實施方式】

【0013】　第1圖為本發明一實施例之安全系統100的示意圖。安全系統100包含寫入保護電路110、記憶體120及讀出解密電路130。記憶體120可耦接於寫入保護電路110及讀出解密電路130。

【0014】　在本發明的有些實施例中，記憶體120可以是一次性寫入的記憶體(one-time programmable memory)。為了避免記憶體120中所儲存的資訊被對手竊取，安全系統100可以透過寫入保護電路110將寫入記憶體120的資料加密，並且更動對應的寫入位址。如此一來，在對手無法得知寫入保護電路110是以何種方式進行加密，又以何種規則儲存資料的情況下，將難以辨識出記憶體120中所儲存的資料。舉例來說，即使對手透過逆向工程手法，例如被動式電壓對比方式(Passive voltage contrast)，得知記憶體120中每位元所儲存的資料，但由於記憶體120並非存放原始的機密資訊，所以即使被竊取，也不會危害到整個系統安全，如此一來，進而保護記憶體120的資訊安全。

【0015】　在第1圖中，寫入保護電路110可包含位址加擾單元112及資料加密單元114。在本發明的有些實施例中，當安全系統100欲將原始資料D1儲存至對應

於寫入位址ADD1的記憶體空間時，安全系統100可將原始資料D1及寫入位址ADD1傳送至寫入保護電路110。寫入保護電路110在接收到原始資料D1及寫入位址ADD1之後，便可利用位址加擾單元112根據隨機字串RNS1加擾(scramble)寫入位址ADD1以產生加擾位址SADD1，並可利用資料加密單元114根據隨機字串RNS2加密原始資料D1以產生儲存資料ED1。接著，記憶體120便可根據加擾位址SADD1儲存對應於原始資料D1的儲存資料ED1。

【0016】　也就是說，對手在不知道位址加擾單元112是以何種方式進行加擾的情況下，就無法根據寫入位址ADD1在記憶體120取出儲存資料ED1，而在不知道資料加密單元114是以何種方式進行加密的情況下，也無法將儲存資料ED1還原成系統實際上使用的原始資料D1。由於對手無法得知位址與資料的對應關係，也無法從竊取的資料中直接得知系統實際使用的資料，因此安全系統100能夠有效提升記憶體120的資料安全性。在本發明得有些實施例中，倘若利用位址加擾單元112便足以保護記憶體120中的資料安全，則設計者也可將資料加密單元114省略。在此情況下，儲存資料ED1與所對應的原始資料D1也可具有相同的內容。

【0017】　在本發明的有些實施例中，位址加擾單元112可將隨機字串RNS1與寫入位址ADD1進行互斥或(exclusive OR)運算以產生加擾位址SADD1。舉例來說，若寫入位址ADD1為01100100而隨機字串RNS1為10111101，則在經過位址加擾單元112加擾所產生的加擾位址SADD1即為兩者進行互斥或運算後的結果11011001。然而本發明並不限定以互斥或運算來對寫入位址ADD1進行加擾，在本發明的其他實施例中，位址加擾單元112也可以使用其他可逆的運算方式來對寫入位址ADD1進行加擾。

【0018】　此外，資料加密單元114可更動原始資料D1的排列順序，並根據隨機字串RNS2更動原始資料D1的內容，以產生儲存資料ED1。舉例來說，若原始資

料D1的內容為00011000，則資料加密單元114可以先改變原始資料D1的排列順序，例如每兩個位元的位置互換，而成為00100100，接著再與隨機字串RNS2進行互斥或運算以改變原始資料D1的內容並產生儲存資料ED1。如此一來，即便對手自記憶體120中取得了儲存資料ED1，也將難以還原出實際系統所使用的原始資料D1。

【0019】　再者，在本發明的有些實施例中，資料加密單元114也可以先根據隨機字串RNS2更動原始資料D1的內容，再進一步更動原始資料D1的排列順序，或者資料加密單元114可以更動原始資料D1的排列順序而不另外更動原始資料D1的內容，又或者更動原始資料D1的內容而不另外更動原始資料D1的排列順序。

【0020】　在本發明的有些實施例中，資料加密單元114可透過與記憶體120的位元線的耦接關係直接在儲存資料時，以固定的方式將原始資料D1的排列順序打亂，也可能是根據另外的隨機字串來決定如何更動原始資料D1的排列順序，並在更動原始資料D1的排列順序後，才繼續進行加密操作或者存入記憶體120中。再者，本發明也不限定資料加密單元114需以互斥或運算來更動原始資料D1的內容，在本發明的其他實施例中，資料加密單元114也可以使用其他可逆的運算方式來對原始資料D1進行加密。

【0021】　在將儲存資料ED1儲存至記憶體120中對應於加擾位址SADD1的空間之後，讀出解密電路130可根據寫入位址ADD1將儲存資料ED1讀出以協助取出原始資料D1。舉例來說，讀出解密電路130可以和位址加擾單元112以相同的方式對當初的寫入ADD1位址進行加擾，如此一來，讀出解密電路130將能夠根據隨機字串RNS1及寫入位址ADD1產生加擾位址SADD1以讀出其中的儲存資料ED1。在讀出儲存資料ED1之後，讀出解密電路130還可進一步將儲存資料ED1還原成原始資料D1。也就是說，讀出解密電路130可根據隨機字串RNS2還原原始資料D1的內容，並將原始資料D1的排列順序還原。也就是說，雖然記憶體120

是以加擾之後的位址配置來儲存加密過的原始資料D1以達到資安保護的目的，然而系統仍然可以透過正常的位址取得原先的儲存資料以完成所需的操作。

【0022】　在本發明的有些實施例中，為確保寫入位址在加擾之後不會與其他的寫入位址產生衝突，也確保讀出解密電路130能夠正確地還原取出原始資料D1，隨機字串RNS1及隨機字串RNS2可以設計成不隨時間更新變化的固定字串。也就是說，寫入保護電路110可以利用固定的隨機字串RNS1來對寫入位址進行加擾，並利用固定的隨機字串RNS2來對原始資料D1進行加密，而讀出解密電路130也將利用相同的隨機字串RNS1及隨機字串RNS2自記憶體120中還原取出原始資料D1。在本發明的有些實施例中，隨機字串RNS1及隨機字串RNS2實質上也可以是相同的隨機字串。

【0023】　在第1圖的實施例中，安全系統100還可包含物理不可複製函數(Physical Unclonalbe Function，PUF)電路160。物理不可複製函數電路160可提供複數個隨機字串以產生寫入保護電路110及讀出解密電路130所需的隨機字串RNS1及RNS2。第2圖為物理不可複製函數單元PU的示意圖。物理不可複製函數電路160可包含複數個物理不可複製函數單元PU，而物理不可複製函數單元PU可利用一次性寫入記憶體單元的結構來實作。舉例來說，物理不可複製函數單元PU可包含選擇電晶體S1、S2、開關電晶體W1及W2及反熔絲電晶體AT1及AT2。

【0024】　選擇電晶體S1具有第一端、第二端及控制端，選擇電晶體S1之第一端耦接於位元線BL，而選擇電晶體S1之控制端耦接於字元線WL。開關電晶體W1具有第一端、第二端及控制端，開關電晶體W1的第一端耦接於選擇電晶體S1之第二端，而開關電晶體W1的控制端耦接於開關控制線SWL。反熔絲電晶體AT1具有第一端、第二端及閘極結構，反熔絲電晶體AT1的第一端耦接於開關電晶體W1之第二端，反熔絲電晶體AT1的閘極結構耦接於反熔絲控制線AF1。

【0025】　此外，選擇電晶體S2具有第一端、第二端及控制端，選擇電晶體S2

之第一端耦接於位元線BL，而選擇電晶體S2之控制端耦接於字元線WL。開關電晶體W2具有第一端、第二端及控制端，開關電晶體W2的第一端耦接於選擇電晶體S2之第二端，而開關電晶體W2的控制端耦接於開關控制線SWL。反熔絲電晶體AT2具有第一端、第二端及閘極結構，反熔絲電晶體AT2的第一端耦接於開關電晶體W2之第二端，反熔絲電晶體AT2的第二端可耦接於反熔絲電晶體AT1之第二端，而反熔絲電晶體AT2的閘極結構耦接於反熔絲控制線AF2。也就是說，反熔絲電晶體AT1及AT2可相耦接，開關電晶體W1及W2可由相同的控制線SWL所控制，而選擇電晶體S1及S2可由相同的字元線WL所控制。

【0026】　當物理不可複製函數單元PU執行寫入操作時，反熔絲電晶體AT1及AT2的閘極結構將同時透過反熔絲控制線AF1及AF2接收到相同的高電壓，而反熔絲電晶體AT1及AT2的第一端及第二端(即汲極及源極)則將經由開關電晶體W1及W2以及選擇電晶體S1及S2接收到低電壓。在此情況下，由於製程差異會造成反熔絲電晶體AT1及AT2在先天結構特性上的差異，例如閘極氧化層品質的差異、局部缺陷分布的差異、閘極氧化層厚度的差異...等等，因此在寫入操作的過程中，反熔絲電晶體AT1及AT2的其中一者的閘極氧化層會先被破壞。而被破壞的反熔絲電晶體會導致反熔絲電晶體AT1及AT2之間的結點電壓被耦合(couple)至一中間電位，且此中間電位與反熔絲電晶體AT1及AT2所接受的高電壓其壓差(voltage difference)並不足以將另一反熔絲電晶體破壞。也就是說，在正常的情況下，反熔絲電晶體AT1及AT2中只有一個反熔絲電晶體會在寫入操作的過程中被破壞。

【0027】　因此，在寫入操作之後，反熔絲電晶體AT1及AT2的破裂狀態(rupture condition)將會彼此相異。透過分別在反熔絲電晶體AT1及AT2的閘極結構上施加相同的讀取電壓，就可以經由開關電晶體W1及W2以及選擇電晶體S1及S2來讀出對應電流，以判讀兩者的破裂狀態。由於反熔絲電晶體AT1及AT2的破裂狀態

是因為無法控制的製程變異所造成，因此自物理不可複製函數單元PU中讀出的位元具有不可預測性，而可用來做為亂數位元，而物理不可複製函數電路160則可透過其中複數個物理不可複製函數單元PU來組合產生所需的隨機字串。

【0028】　此外，第2圖所示的物理不可複製函數單元PU僅為本發明的一實施例。在本發明的其他實施例中，物理不可複製函數電路160也可利用其他的結構實作，例如第3圖及第4圖是本發明其他實施例的物理不可複製函數單元PU1及PU2的示意圖。第3圖的物理不可複製函數單元PU1與第2圖的物理不可複製函數單元PU差別在於物理不可複製函數單元PU1可省略開關電晶體W1及W2。也就是說，物理不可複製函數單元PU1可只包含選擇電晶體S1、S2及反熔絲電晶體AT1及AT2，在此情況下，選擇電晶體S1及S2的第一端可直接耦接於位元線BL，而其他接線部份則與第2圖中的物理不可複製函數單元PU雷同，所以不再複述。

【0029】　此外，物理不可複製函數單元PU也可利用如第4圖的結構來實現。在第4圖中，物理不可複製函數單元PU2可將選擇電晶體S1及S2也一併省略，而只包含反熔絲電晶體AT1及AT2。在此情況下，反熔絲電晶體AT1及AT2的第一端可以直接耦接至位元線BL，且反熔絲電晶體AT1及AT2可具有雙厚度的閘氧化層(dual gate oxide thickness)，其中反熔絲電晶體AT1及AT2的第一端可以用來控制操作選擇，而反熔絲電晶體AT1及AT2的第二端則可能會在寫入操作的過程中被破壞。如此一來，就可以將選擇電晶體S1及S2省略，並達到與物理不可複製函數單元PU相似的功能。

【0030】　在有些實施例中，寫入保護電路110、記憶體120、物理不可複製函數電路160可以互相整合在相同的電路中，使得記憶體120中所儲存的機密資訊就能夠獲得更加完善的保護，而不容易被對手破解取得。另外，當安全系統100係建構在一晶片上時，因物理不可複製函數電路160所產生的每一隨機字串都是唯一(unique)，所以每一顆晶片從物理不可複製函數電路160所取得的隨機字串皆

不相同。也就是說，每一顆晶片其寫入保護電路110所採用的加密方式也會相異。當外界想要破解每一顆晶片時，會因為其中採用的加密方式皆不相同，所以破解相當不易且成本也非常高昂。

【0031】　此外，安全系統100中的元件可能會設置在不同的晶片上，而不同晶片中的元件則可透過傳輸匯流排來傳輸資訊。為了避免對手從傳輸匯流排上取得資訊，安全系統100還可包含動態加密電路140。在第1圖中，動態加密電路140可耦接於讀出解密電路130及傳輸匯流排150。安全系統100可在將原始資料D1傳送至傳輸匯流排150之前，先透過動態加密電路140處理。動態加密電路140可以根據動態隨機字串DRNS加密原始資料D1以產生傳輸資料TD1，並將傳輸資料TD1傳送至傳輸匯流排150。如此一來，即便對手透過側錄或其他駭客侵入的手段，自傳輸匯流排150取得傳輸資料TD1，也難以從中辨識出系統實際上所欲傳送的原始資料D1。

【0032】　在第1圖中，安全系統100還可包含動態解密電路170及應用電路180。動態解密電路170耦接於傳輸匯流排150，並可接收傳輸資料TD1。動態解密電路170可根據動態隨機字串DRNS將傳輸資料TD1解密還原成原始資料D1，使得應用電路180能夠根據原始資料D1執行對應的操作。

【0033】　此外，安全系統100還可包含隨機字串產生器190。隨機字串產生器190可以在應用電路180欲接收原始資料D1時，更新產生動態隨機字串DRNS，並將更新後的動態隨機字串DRNS傳送至動態加密電路140及動態解密電路170。也就是說，每次透過傳輸匯流排150傳送資訊時，動態加密電路140都會使用不一樣的動態隨機字串DRNS來對傳送資料進行加密，而動態解密電路170則可根據對應的動態隨機字串DRNS來對傳送資料進行解密。如此一來，就能夠減少對手在長時間觀測傳輸匯流排150上的資訊後，破解安全系統100的加密方式或所使用的隨機字串的可能性，使得安全系統100能夠更有效地保護系統中的敏感資

訊。

【0034】　另外，隨機字串產生器190的實作方式可以有很多種，包括利用硬體實作出來的真實亂數產生器(true random number generator)或是利用軟體產生隨機字串的確定性隨機位元產生器(deterministic random bit generator)，又或者是利用軟硬體結合所實作出的混合亂數產生器(hybrid random number generator)。舉例來說，混合亂數產生器可以透過將確定性隨機位元產生器及物理不可複製函數電路加以結合來實作。在此情況下，物理不可複製函數電路可以每隔一段間就將確定性隨機位元產生器所需的種子(seed)更新，藉此提高該混合亂數產生器的亂度(randomness)。

【0035】　此外，在本發明的部分實施例中，寫入保護電路110、記憶體120、讀出解密電路130及動態加密電路140可設置在相同的晶片上或屬於相同的硬體巨集(hardware macro)，而動態解密電路170、應用電路180及隨機字串產生器190則可能設置在另一個相同的晶片上或屬於另一個相同的硬體巨集。在此情況下，寫入保護電路110可以保護記憶體120中所儲存的資料，而動態加密電路140則可以保護在傳輸匯流排150上傳輸的資料。

【0036】　在第1圖的實施例中，隨機字串RNS1及RNS2可以由物理不可複製函數電路160所提供，然而本發明並不以此為限。在本發明的其他實施例中，隨機字串RNS1及RNS2也可以由隨機字串產生器190產生。此外，在本發明的其他實施例中，動態隨機字串DRNS、隨機字串RNS1及RNS2也都可以由外部的電路提供。

【0037】　第5圖為本發明一實施例之安全系統100的操作方法200之流程圖，方法200包含步驟S210至S290，但不限於第5圖所示的順序。

【0038】　S210： 物理不可複製函數電路160提供複數個隨機字串以產生隨機字串RNS1及RNS2

【0039】　S220：寫入保護電路110接收寫入位址ADD1及原始資料D1；

【0040】　S230：寫入保護電路110根據隨機字串RNS1加擾寫入位址ADD1以產生加擾位址SADD1；

【0041】　S232：寫入保護電路110根據隨機字串RNS2加密原始資料D1以產生儲存資料ED1；

【0042】　S240：記憶體120根據加擾位址SADD1儲存對應於原始資料D1的儲存資料ED1；

【0043】　S250：讀出解密電路130根據寫入位址ADD1自記憶體120讀出儲存資料ED1；

【0044】　S252：讀出解密電路130將儲存資料ED1還原成原始資料D1；

【0045】　S260：當應用電路180欲接收原始資料D1時，隨機字串產生器190更新產生動態隨機字串DRNS以傳送至動態加密電路140及動態解密電路170；

【0046】　S270：動態加密電路140根據動態隨機字串DRNS加密原始資料D1以產生傳輸資料TD1；

【0047】　S272：動態加密電路140將傳輸資料TD1經由傳輸匯流排150傳送至動態解密電路170；

【0048】　S280：動態解密電路170根據動態隨機字串DRNS將傳輸資料TD1解密還原成原始資料D1；

【0049】　S290：應用電路180根據原始資料D1執行對應操作。

【0050】　在步驟S230中，寫入保護電路110可以例如將隨機字串RNS1與寫入位址ADD1進行互斥或運算以產生加擾位址SADD1，然而本發明並不以此為限。在本發明的其他實施例中，寫入保護電路110也可以利用其他的運算操作來將寫入位址ADD1與隨機字串RNS1絞合(entangle)以產生加擾位址SADD1。

【0051】　此外，在步驟S232中，寫入保護電路110可以更動原始資料D1的排列

順序，並根據隨機字串RNS2更動原始資料D1的內容，例如但不限於利用隨機字串RNS2與原始資料D1進行互斥或運算來產生儲存資料ED1。在本發明的其他實施例中，寫入保護電路110也可能利用其他的運算方式來將隨機字串RNS2與原始資料D1絞合，並可根據其他的隨機字串來更動原始資料D1的排列順序。

【0052】　在第1圖中，寫入保護電路110可利用不同的單元來執行步驟S230及步驟S232，因此在本發明的有些實施例中，步驟S230及S232也可平行進行，而不限定彼此之間的執行順序。

【0053】　透過步驟S230及S232，記憶體120便可根據加擾位址SADD1儲存儲存資料ED1，使得對手難以從記憶體120中取得實際上系統使用的原始資料D1。

【0054】　而當安全系統100欲自記憶體120中取出原始資料D1時，讀出解密電路130便會在步驟S250及S252自記憶體120讀出儲存資料ED1，並將儲存資料ED1還原成原始資料D1。舉例來說，讀出解密電路130可將儲存資料ED1根據隨機字串RNS2解密，並將原始資料D1的排列順序還原，以取得原始資料D1的內容。也就是說，讀出解密電路130會根據寫入保護電路110對原始資料D1進行加密的方式來進行解密，以還原出原先的原始資料D1。在本發明的有些實施例中，若安全系統100是單純透過位址加擾的方式來保護記憶體120中所儲存的資料，而並未利用對原始資料D1本身進行加密，則方法200也可將步驟S232省略。在此情況下，記憶體120在步驟S240中所儲存的儲存資料ED1實質上便可能會和原始資料D1相同，而讀出解密電路130也無需執行步驟S252。

【0055】　在本發明的有些實施例中，隨機字串RNS1及RNS2可以是不隨時間更新變化的固定字串，以便寫入保護電路110及讀出解密電路130能夠有效保護記憶體120中的資訊，而不至於在加擾記憶體位址後，在記憶體120的儲存空間中產生衝突。

【0056】　此外，透過步驟S260至S280，方法200就可以在傳輸匯流排150的傳

輸過程中，避免原始資料D1被對手竊取。此外，由於步驟S260會在每一次傳輸資料時，更新產生不同的動態隨機字串DRNS，因此能夠進一步加強對傳輸資料的保護，避免加密機制或動態隨機字串的內容被對手得知。

【0057】　綜上所述，本發明的實施例所提供的安全系統及操作安全系統的方法可以有效地保護記憶體中的資訊，並且在透過匯流排傳輸資料的過程中，也能夠提供動態的加密保護，使得安全系統中的資訊難以被對手取得或破解，提升系統中的資訊安全。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明之涵蓋範圍。

【符號說明】

【0058】

100	安全系統
110	寫入保護電路
112	位址加擾單元
114	資料加密單元
120	記憶體
130	讀出解密電路
140	動態加密電路
150	傳輸匯流排
160	物理不可複製函數電路
170	動態解密電路
180	應用電路
190	隨機字串產生器
RNS1、RNS2	隨機字串

DRNS	動態隨機字串
D1	原始資料
ED1	儲存資料
TD1	傳輸資料
ADD1	寫入位址
SADD1	加擾寫入位址
PU	物理不可複製函數單元
S1、S2	選擇電晶體
W1、W2	開關電晶體
AT1、AT2	反熔絲電晶體
BL	位元線
WL	字元線
SWL	開關控制線
AF1、AF2	反熔絲控制線
200	方法
S210至S290	步驟

【發明申請專利範圍】

【第1項】 一種安全系統，包含：

一物理不可複製函數(Physical Unclonalbe Function，PUF)電路，用以提供複數個隨機字串;

一寫入保護電路，用以接收一寫入位址及一原始資料，該寫入保護電路包含：

一位址加擾單元，用以根據該物理不可複製函數電路所提供的一第一隨機字串加擾該寫入位址以產生一加擾位址；

一記憶體，耦接於該寫入保護電路，用以根據該加擾位址儲存對應於該原始資料之一儲存資料；及

一讀出解密電路，耦接於該記憶體，用以根據該寫入位址自該記憶體讀出該儲存資料以取得該原始資料。

【第2項】 如請求項1所述之安全系統，其中該寫入保護電路另包含一資料加密單元，用以至少根據該物理不可複製函數電路提供的一第二隨機字串對該原始資料加密以產生對應於該原始資料之該儲存資料。

【第3項】 如請求項2所述之安全系統，其中該第一隨機字串及該第二隨機字串係為相同字串。

【第4項】 如請求項2所述之安全系統，其中該第一隨機字串及該第二隨機字串係不隨時間更新變化的固定字串。

【第5項】 如請求項2所述之安全系統，其中該資料加密單元係更動該原始資

料的一排列順序，及根據該第二隨機字串更動該原始資料的內容，以產生該儲存資料。

【第6項】 如請求項5所述之安全系統，其中該讀出解密電路係將該儲存資料根據該第二隨機字串解密，及將該排列順序還原，以取得該原始資料。

【第7項】 如請求項1所述之安全系統，另包含一動態加密電路，耦接於該讀出解密電路及一傳輸匯流排，該動態加密電路用以根據一動態隨機字串加密該原始資料以產生一傳輸資料，並將該傳輸資料傳送至該傳輸匯流排。

【第8項】 如請求項7所述之安全系統，另包含：

一動態解密電路，耦接於該傳輸匯流排，用以接收該傳輸資料，並根據該動態隨機字串將該傳輸資料解密還原成該原始資料；及

一應用電路，用以根據該原始資料執行一對應操作。

【第9項】 如請求項8所述之安全系統，另包含：

一隨機字串產生器，用以當該應用電路欲接收該原始資料時，更新產生該動態隨機字串，並將更新後的該動態隨機字串傳送至該動態加密電路及該動態解密電路。

【第10項】如請求項1所述之安全系統，其中該物理不可複製函數電路包含複數個物理不可複製函數單元，每一物理不可複製函數單元包含：

一第一選擇電晶體，具有一第一端耦接於一位元線，一第二端，及一控制端耦接於一字元線；

一第一開關電晶體，具有一第一端耦接於該第一選擇電晶體的該第二端，一第二端，及一控制端耦接於一開關控制線；

一第一反熔絲電晶體，具有一第一端耦接於該第一開關電晶體之該第二端，一第二端，及一閘極結構耦接於一第一反熔絲控制線；

一第二選擇電晶體，具有一第一端耦接於該位元線，一第二端，及一控制端耦接於該字元線；

一第二開關電晶體，具有一第一端耦接於該第二選擇電晶體的該第二端，一第二端，及一控制端耦接於該開關控制線；及

一第二反熔絲電晶體，具有一第一端耦接於該第二開關電晶體之該第二端，一第二端耦接於該第一反熔絲電晶體的該第二端，及一閘極結構耦接於一第二反熔絲控制線。

【第11項】　如請求項1所述之安全系統，其中該物理不可複製函數電路包含複數個物理不可複製函數單元，每一物理不可複製函數單元包含：

一第一選擇電晶體，具有一第一端耦接於一位元線，一第二端，及一控制端耦接於一字元線；

一第一反熔絲電晶體，具有一第一端耦接於該第一選擇電晶體之該第二端，一第二端，及一閘極結構耦接於一第一反熔絲控制線；

一第二選擇電晶體，具有一第一端耦接於該位元線，一第二端，及一控制端耦接於該字元線；及

一第二反熔絲電晶體，具有一第一端耦接於該第二選擇電晶體之該第二端，一第二端耦接於該第一反熔絲電晶體的該第二端，及一閘極結構耦接於一第二反熔絲控制線。

【第12項】　如請求項1所述之安全系統，其中該物理不可複製函數電路包含複數個物理不可複製函數單元，每一物理不可複製函數單元包含：

一第一反熔絲電晶體，具有一第一端耦接於一位元線，一第二端，及一閘極結構耦接於一第一反熔絲控制線；及

一第二反熔絲電晶體，具有一第一端耦接於該位元線，一第二端耦接於該第一反熔絲電晶體的該第二端，及一閘極結構耦接於一第二反熔絲控制線。

【第13項】如請求項1所述之安全系統，其中該位址加擾單元係將該第一隨機字串與該寫入位址進行互斥或(exclusive OR)運算以產生該加擾位址。

【第14項】一種安全系統的操作方法，該安全系統包含一寫入保護電路、一記憶體、一物理不可複製函數電路及一讀出解密電路，該方法包含：

該物理不可複製函數電路提供複數個隨機字串以產生一第一隨機字串；

該寫入保護電路接收一寫入位址及一原始資料；

該寫入保護電路根據該第一隨機字串加擾該寫入位址以產生一加擾位址；

該記憶體根據該加擾位址儲存對應於該原始資料之一儲存資料；及

該讀出解密電路根據該寫入位址自該記憶體讀出該儲存資料以取得該原始資料。

【第15項】如請求項14所述之方法，另包含該寫入保護電路至少根據該物理不可複製函數電路所產生的一第二隨機字串對該原始資料加密以產生該儲存資料。

【第16項】如請求項15所述之方法，其中該寫入保護電路至少根據該物理不可複製函數電路所產生的該第二隨機字串對該原始資料加密以產生該儲存資料包含：

該寫入保護電路更動該原始資料的一排列順序；及

該寫入保護電路根據該第二隨機字串更動該原始資料的內容以產生該儲存資料。

【第17項】如請求項16所述之方法，其中該讀出解密電路根據該寫入位址自該記憶體讀出該儲存資料以取得該原始資料包含：

該讀出解密電路將該儲存資料根據該第二隨機字串解密；及

該讀出解密電路將該排列順序還原。

【第18項】如請求項15所述之方法，其中該第一隨機字串及該第二隨機字串係為相同的固定字串。

【第19項】 如請求項15所述之方法，其中該第一隨機字串及該第二隨機字串係不隨時間更新變化的固定字串。

【第20項】如請求項14所述之方法，其中該寫入保護電路根據該第一隨機字串加擾該寫入位址以產生該加擾位址係該寫入保護電路將該第一隨機字串與該寫入位址進行互斥或(exclusive OR)運算以產生該加擾位址。

【第21項】如請求項14所述之方法，其中該安全系統另包含一動態加密電路，及該方法另包含：

該動態加密電路根據一動態隨機字串加密該原始資料以產生一傳輸資料；

及

該動態加密電路將該傳輸資料傳送至一傳輸匯流排。

【第22項】如請求項21所述之方法，其中該安全系統另包含一動態解密電路及一應用電路，及該方法另包含：

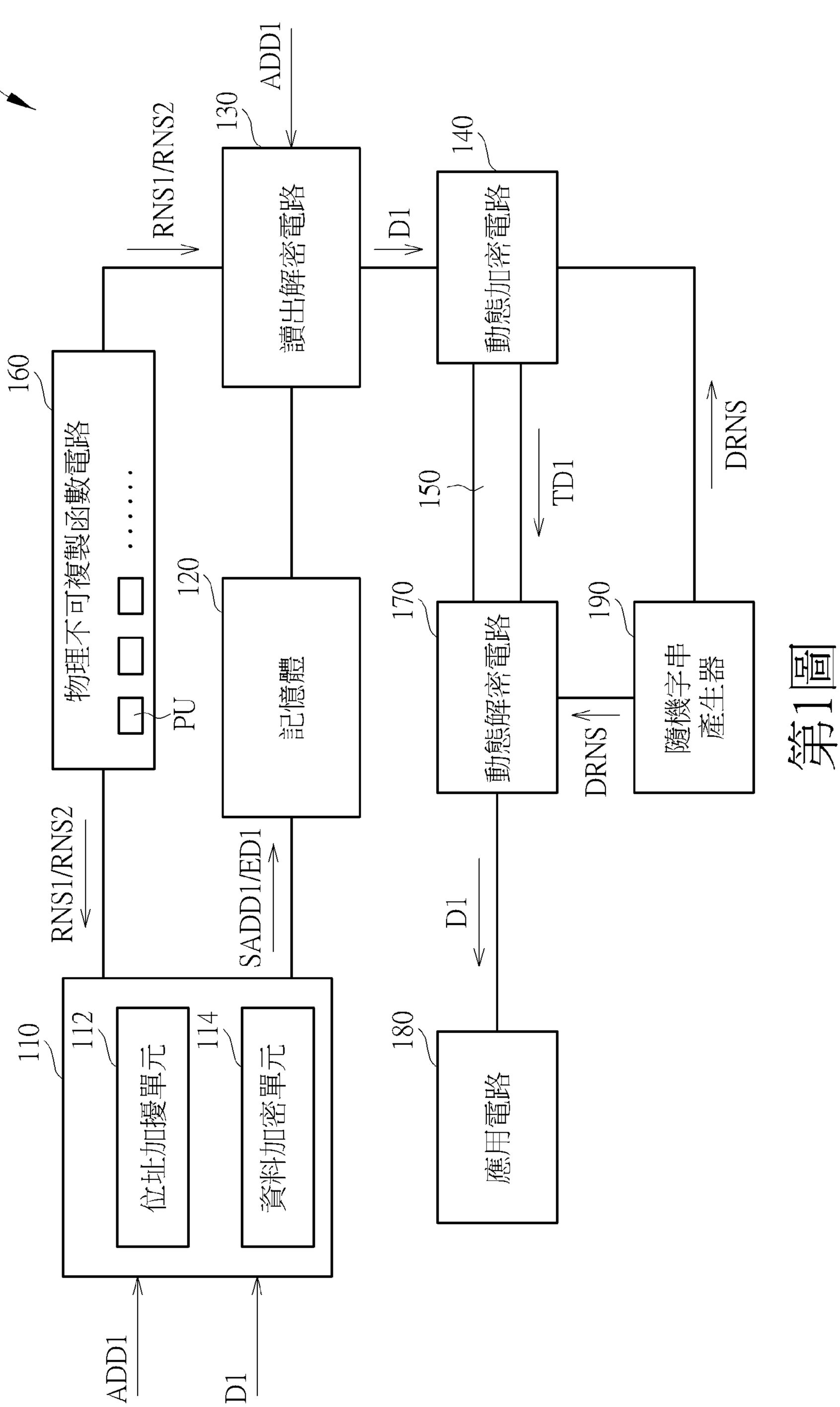
該動態解密電路根據該動態隨機字串將該傳輸資料解密還原成該原始資料；及

該應用電路根據該原始資料執行一對應操作。

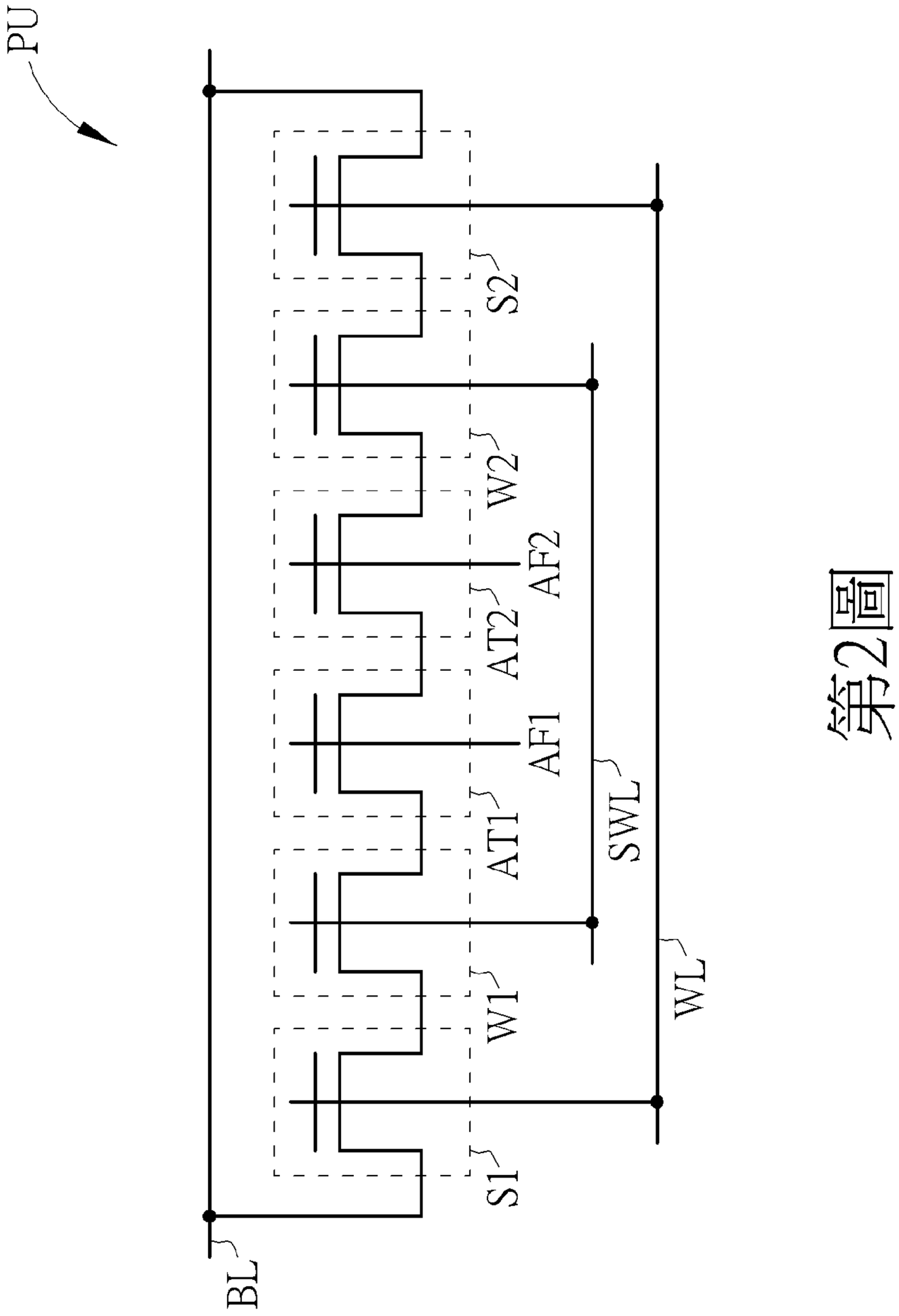
【第23項】如請求項22所述之方法，其中該安全系統另包含一隨機字串產生器，及該方法另包含：

當該應用電路欲接收該原始資料時，該隨機字串產生器更新產生該動態隨機字串以傳送至該動態加密電路及該動態解密電路。

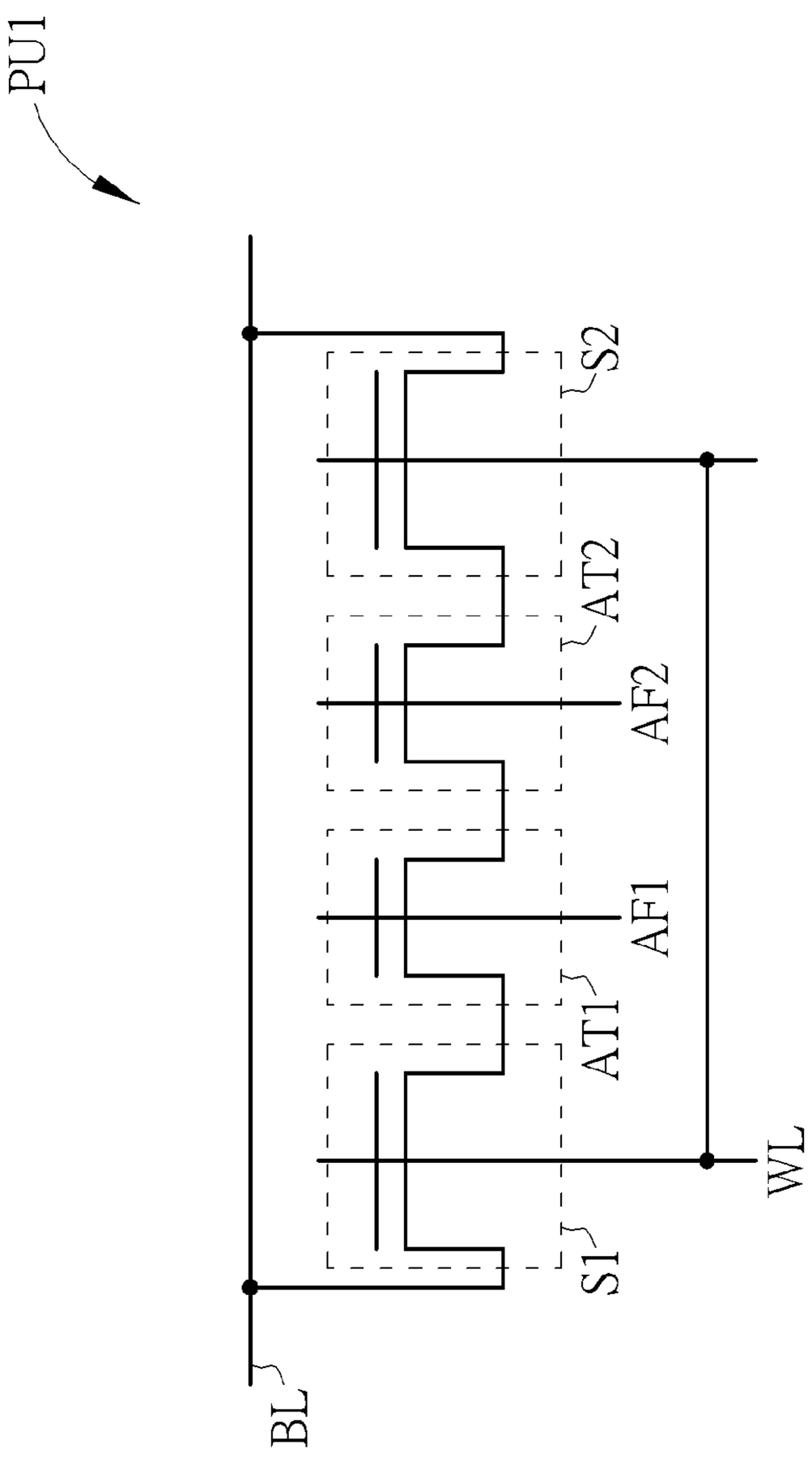
【發明圖式】


100
ADD1
130
RNS1/RNS2
讀出解密電路
140
D1
動態加密電路
160
物理不可複製函數電路
PU
RNS1/RNS2
120
記憶體
SADD1/ED1
150
TD1
DRNS
170
動態解密電路
190
隨機字串
產生器
DRNS
D1
180
應用電路
110
112
位址加擾單元
114
資料加密單元
ADD1
D1

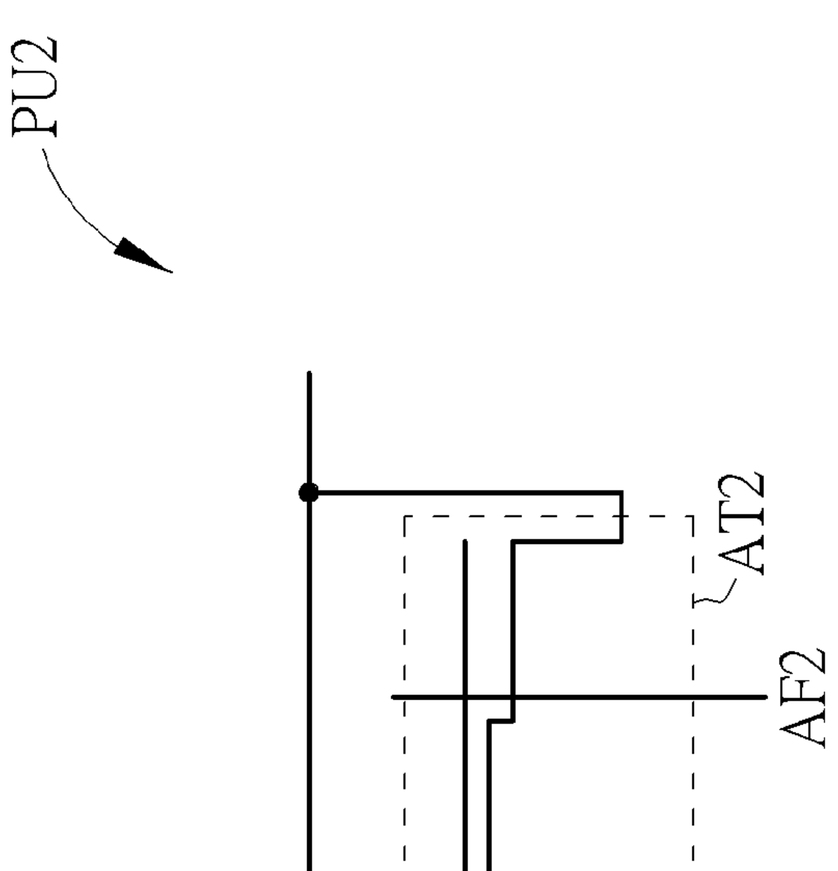
第1圖



第2圖



第3圖



第4圖


200
物理不可複製函數電路提供複數個隨機字串以產生第一隨機字串及第二隨機字串
S210
寫入保護電路接收寫入位址及原始資料
S220
寫入保護電路根據第一隨機字串加擾寫入位址以產生加擾位址
S230
寫入保護電路根據第二隨機字串加密原始資料以產生儲存資料
S232
記憶體根據加擾位址儲存對應於原始資料的儲存資料
S240
讀出解密電路根據寫入位址自記憶體讀出儲存資料
S250
讀出解密電路將儲存資料還原成原始資料
S252
當應用電路欲接收原始資料時，隨機字串產生器更新產生動態隨機字串以傳送至動態加密電路及動態解密電路
S260
動態加密電路根據動態隨機字串加密原始資料以產生傳輸資料
S270
動態加密電路將傳輸資料經由傳輸匯流排傳送至動態解密電路
S272
動態解密電路根據動態隨機字串將傳輸資料解密還原成原始資料
S280
應用電路根據原始資料執行對應操作
S290

第5圖