公告本

發明專利說明書 I221966

（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：92123814 ※IPC分類：G06F 12/14

※ 申請日期：92.8.28

壹、發明名稱

（中文）以保護位元碼對一程式進行加密保護之裝置

（英文）

貳、發明人（共 1 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）梁伯嵩

（英文）

住居所地址：（中文）高雄市左營區裕誠路406號6樓之1

（英文）

國籍：（中文）中華民國 （英文）

參、申請人（共 1 人）

申請人 1 （如發明人超過一人，請填**說明書申請人續頁**）

姓名或名稱：（中文）凌陽科技股份有限公司

（英文）

住居所或營業所地址：（中文）新竹縣科學園區創新一路19號

（英文）

國籍：（中文）中華民國 （英文）

代表人：（中文）黃洲杰

（英文）

☐ 續發明人或申請人續頁 （發明人或申請人欄位不敷使用時，請註記並使用續頁）

捌、聲明事項

☐ 本案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，其日期爲：＿＿＿＿＿＿＿＿

☐ 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. 無
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.
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）

【一、發明所屬之技術領域】

本發明係關於處理器的資料保護技術，尤指一種以保護位元碼對一程式進行加密保護之裝置。

【二、先前技術】

在這重視智財權的時代，廠商為了保護其辛苦開發之程式、資料等相關的智慧財產，會於離線(off-line)時將該等資料、程式先進行一加密(encrypting)處理，再將加密後的資料予以儲存至一非揮發性記憶體或其他儲存媒體，他人即使拿到存有該加密資料的非揮發性記憶體或其他儲存媒體，由於無法知道該加密處理之過程及處理方法，亦無法正確去還原該等資料、程式，藉此而達到保護之目的。

針對此種資料保護方式，於美國第USP6,408,073號專利案公告中，使用一虛擬亂數產生器(Pseudo Random Generator)及依據一初始值(seed1/seed2)，來對唯讀記憶體(Read Only Memory，ROM)之資料(ROM data)進行編碼以產生編碼資料(Encoded data)，然而此種資料保護方式因使用亂數做加密處理之參數，需有同步之亂數產生器用以進行解碼。需要非常多的亂數的樣型(pattern)，才能有效防止他人還原該等資料、程式，這意味著編碼及解碼的虛擬亂數產生器需要相當複雜的電路，此會增加許多成本。若使用較簡單的編碼及解碼的虛擬亂數產生

器，雖然可節省成本，但卻容易被他人還原該等資料、程式，因此，習知處理器之條件指令處理方法的設計仍有諸多缺失而有予以改進之必要。

發明人爰因於此，本於積極發明之精神，亟思一種可以解決上述問題之「以保護位元碼對一程式進行加密保護之裝置」，幾經研究實驗終至完成此項發明。

【三、發明內容】

本發明之目的係在提供一種以保護位元碼對一程式進行加密保護之裝置，以避免習知技術使用複雜的虛擬亂數產生器，而達可節省成本之目的。同時，由於保護位元碼的產生及去除硬體係相當簡易，以減少加密處理時間，而增進整體系統效率。

依據本發明之一特色，係提出一種以保護位元碼對一程式進行加密保護之裝置，該程式具有複數個指令，該裝置包含一保護位元碼產生裝置、一第一保護位元碼位置產生裝置及一保護位元碼插入裝置。該保護位元碼產生裝置係依據該程式之複數指令以產生複數個保護位元碼，每一指令具有I個位元（I為正整數）。該第一保護位元碼位置產生裝置依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置N（N為正整數）。該保護位元碼插入裝置依據該第一保護位元碼位置產生裝置所產生之插入位置N，分別將每一保護位元碼插入該程式之對應指令之第N-1與第N位元之中，以產生一加密之程式。

依據本發明之另一特色，係提出一種對一加密程式進行解密之裝置，該加密程式係將保護位元碼插置於原始程式中而加密，該加密程式具有複數個指令，該裝置包含一第二保護位元碼位置產生裝置及一保護位元碼去除裝置。該第二保護位元碼位置產生裝置依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置；該保護位元碼去除裝置係輸入該程式，並依據該第二保護位元碼位置產生裝置所產生之每一插入位置N，以將該程式之對應指令之第N位元去除。

依據本發明之又一特色，係提出一種對一加密程式進行解密之裝置，該加密程式係將兩組保護位元碼插置於原始程式中而加密，該加密程式具有複數個指令，其中一個字組可包含二個加密指令，該裝置包含一第三保護位元碼位置產生裝置、一第四保護位元碼位置產生裝置、一第三保護位元碼去除裝置及一第四保護位元碼去除裝置。該第三保護位元碼位置產生裝置依據執行該程式時之處理器狀態以產生每一保護位元碼的第三插入位置；該第四保護位元碼位置產生裝置依據執行該程式時之處理器狀態以產生每一保護位元碼的第四插入位置；該第三保護位元碼去除裝置係輸入該加密程式之低半字組，並依據該第三保護位元碼位置產生裝置所產生之每一第三插入位置N1，以將該該程式之複數指令之第0至（K-1）位元之第N1位元去除；該第四保護位元碼去除裝置係輸入該加密程式之高半字組，並依據該第四保護位元碼位置產生裝置所產生之每一第四插入位置N2，以將

該該程式之複數指令之第K至（2K-1）位元之第N2位元去除。

由於本發明設計新穎，能提供產業上利用，且確有增進功效，故依法申請發明專利。

【四、實施方式】

圖1顯示本發明之以保護位元碼對一程式進行加密保護之裝置的方塊圖，其包含一保護位元碼產生裝置110、一第一保護位元碼位置產生裝置120、一保護位元碼插入裝置130、一第二保護位元碼位置產生裝置210及一保護位元碼去除裝置220。而被加密之程式具有複數之指令，每一個指令具有I個位元（I為正整數），而保護位元碼具有P個位元（P為正整數），在本實施例中，I為31位元，P為1位元，即I+P為32位元，亦可I為32位元，P為1位元。

該保護位元碼產生裝置110係依據該程式之每一個指令以分別產生相對應之保護位元碼，該保護位元碼可為同位檢查位元(Parity bit)、錯誤更正碼(Error Correction Code、ECC)或是指令執行時處理器模式的指示位元。

該第一保護位元碼位置產生裝置120依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置N（N為正整數）。該保護位元碼插入裝置130係依據該第一保護位元碼位置產生裝置120所產生之插入位置N，分別將每一保護位元碼插入該程式之對應指令之第N-1與第N位元之中，以產生一加密之程式。

該第二保護位元碼位置產生裝置210依據執行該程式時之處理器狀態以產生該每一保護位元碼的插入位置。該保護位元碼去除裝置220係輸入一加密程式，該加密程式係將保護位元碼插置於原始程式中而予以加密，並依據該第二保護位元碼位置產生裝置210所產生之每一插入位置N，以將該加密程式之每一指令中之保護位元碼去除。

該第一保護位元碼位置產生裝置120及該第二保護位元碼位置產生裝置210係依據執行該程式時之處理器狀態以產生插入位置，圖2係其電路圖。每一第一及第二保護位元碼位置產生裝置包含一存取狀態暫存器(Access Status Register、ASR)310、一程式狀態暫存器(Program Status Register、PSR)320、一多工器330及複數個插入位置產生裝置340~380。

該存取狀態暫存器(ASR)310為1位元，其值為1時，代表處理器存取資料區段，其值為0時，代表處理器存取程式區段。該程式狀態暫存器(PSR)320為3位元，其值為1xx時，代表處理器重置後進入自動開機執行BIOS程式狀態；其值為01x時，代表處理器處在作業系統核心(OS Kernel)狀態；其值為001時，代表處理器處在一特殊認證程式狀態；其值為000時，代表處理器處在一個一般使用者程式狀態。

圖2中之PPG_Mode訊號係用來選擇該多工器330之輸出訊號PBP與輸入訊號之間的關係。該PPG_Mode訊號係由該存取狀態暫存器(ASR)310及該程式狀態暫存器

(PSR)320所組合而成，亦即PPG_Mode={ASR，PSR[2:0]}。當處理器存取資料區段時，該存取狀態暫存器(ASR)310之值為1，PPG_Mode=1xxx，該多工器330會選擇插入位置產生裝置380之輸出做為該多工器330之輸出訊號PBP。而當處理器重置後，進入自動開機執行BIOS程式狀態時，該存取狀態暫存器(ASR)310之值為0，該程式狀態暫存器(PSR)320之值為1xx，該多工器330會選擇插入位置產生裝置340之輸出做為該多工器330之輸出訊號PBP。

該複數個插入位置產生裝置340~380係依據其預定之功能以產生插入位置。其中，該插入位置產生裝置380可為一空裝置，以表示無插入位置，其輸出訊號為000000b。該插入位置產生裝置340係將一給定值x經由模數運算以產生插入位置，亦即，F1(x)=(x mod 32)。該插入位置產生裝置350係將一第一給定值減去經由模數運算之一第二給定值，以產生插入位置，亦即，F2(x)=31-(x mod 32)。

該插入位置產生裝置360係將一第一給定值與該處理器之部分位址線值結合後，再經由模數運算，以產生插入位置，亦即，F3(x,a) = [(x + { a[0], a[1], a[2], a[3], a[4] }) mod 32]。該插入位置產生裝置370係將一給定值x[4:0]反置，以產生插入位置，亦即，F4(x) = { x[0], x[1], x[2], x[3], x[4] }。該插入位置產生裝置亦可將該存取狀態暫存器(ASR)310與該程式狀態暫存器(PSR)320結合後，以產生插入位置，或是將該位置狀態暫存器與該程

式狀態暫存器結合後，再經由模數運算，以產生插入位置。

圖2中之K1、K2、K3及K4分別對該複數個插入位置產生裝置340~380提供一給定值，其可先予以燒錄至一硬體電路，亦可為暫存器，而由系統去設定。如此，可對不同程式及處理器所處狀態產生不同之保護位元碼插入位置。

圖3係顯示K1=K2=K3=K4=3時，該複數個插入位置產生裝置340、350及380所產生不同之保護位元碼插入位置。其中，F1(x) = (x mod 32) = 3，代表處理器重置後，進入自動開機執行BIOS程式狀態時，其保護位元碼插入位置為位元3。F2(x) = [31 - (x mod 32)] = 28，代表處理器處在作業系統核心(OS Kernel)狀態時，其保護位元碼插入位置為位元28。F4(x) = { x[0], x[1], x[2], x[3], x[4] } = { 11000b} = 24，代表處理器處在一個一般使用者程式狀態時，其保護位元碼插入位置為位元24。

圖4係顯示K3= 3時，該插入位置產生裝置360所產生不同之保護位元碼插入位置。F3(x,a) = (x + { a[0], a[1], a[2], a[3], a[4] }) mod 32 = (3 + { a[0], a[1], a[2], a[3], a[4] }) mod 32。代表處理器處在一個認證程式時，其保護位元碼插入位置將會呈現如圖4所示之變化，而使得該認證程式碼難以盜取或解譯。

該多工器330之輸出訊號PBP(P-bit Bit Position)係為由6個位元所組成，其中PBP[5]之布林值代表PBP[4:0]中是否為保護位元碼插入位置。當PBP[5:0]=0xxxxxb時，表

示PBP[4:0]無保護位元碼插入位置。當PBP[5:0]=100101b時，表示PBP[4:0]為保護位元碼插入位置，且該保護位元碼插入位置在00101b=5的位置。由於該複數個插入位置產生裝置340~370均會產生保護位元碼插入位置，故其輸出訊號會與一高電位組合，而形成該多工器330之輸出訊號PBP[5:0]，其中，該高電位形成PBP[5](即PBP[5]=1)，以表示表示PBP[4:0]為保護位元碼插入位置。而該複數個插入位置產生裝置380為一空裝置，以表示無插入位置，故其輸出訊號為000000b，表示PBP[4:0]無保護位元碼插入位置。

圖5為該保護位元碼去除裝置220之電路圖，其主要包含多工器510、520及530。其係輸入端540輸入一32位元之加密程式，該加密程式係將保護位元碼插置於原始程式中而予以加密，並依據該第二保護位元碼位置產生裝置210所產生之複數個插入位置PBP[4:0]，以將該加密程式之複數指令中之保護位元碼去除。當PBP[5]=0時，表示PBP[4:0]無保護位元碼插入位置，故該多工器510則將輸入端540直接輸出。當PBP[5]=1時，表示PBP[4:0]為保護位元碼插入位置，該多工器520依據該PBP[4:0]訊號，而輸出該保護位元碼，該多工器530依據該PBP[4:0]訊號，輸出不具有該保護位元碼之指令，該保護位元碼與該不具有該保護位元碼之指令又組合成一32位元之字組，而該多工器510因PBP[5]=1，則將其接輸出。

於本實施例中，該保護位元碼產生裝置110、第一保護位元碼位置產生裝置120、及保護位元碼插入裝置130

可以使用硬體予以實現，亦可以使用軟體離線處理，而產生一加密之程式。該保護位元碼去除裝置220及該第二保護位元碼位置產生裝置210可與一處理器核心結合，該保護位元碼去除裝置220輸入該加密程式，並依據該第二保護位元碼位置產生裝置210所產生之複數個插入位置N，以將該加密程式之複數個指令中之保護位元碼去除。如此，該處理器核心可正確執行該解密後之程式，而加密之程式則不必擔心輕易被他人所破解，而達到保護之目的。

圖6係本發明之另一實施例，係對將兩組保護位元碼插置於原始程式中的加密程式進行解密之裝置，該加密程式具有複數之指令，其中一個字組可包含二個加密指令，每一加密指令為16位元。該裝置包含一第三保護位元碼位置產生裝置610、一第四保護位元碼位置產生裝置620、一第三保護位元碼去除裝置630及一第四保護位元碼去除裝置640。

該第三保護位元碼位置產生裝置610及第四保護位元碼位置產生裝置620分別依據執行該程式時之處理器狀態以產生每一保護位元碼的第三插入位置PBP1[4:0]及第四插入位置PBP2[4:0]。

該第三保護位元碼去除裝置630係輸入該加密程式之低半字組(low half word)，並依據該第三保護位元碼位置產生裝置630所產生之每一第三插入位置PBP1[4:0]，以將該該程式之複數指令之第0至15位元之第PBP1[4:0]位元去除。該第四保護位元碼去除裝置640係輸入該加密程

式之高半字組(high half word)，並依據該第四保護位元碼位置產生裝置所產生之每一第四插入位置PBP2[4:0]，以將該該程式之對應指令之第16至31位元之第PBP2[4:0]位元去除。

由上述之說明可知，由上述之說明可知，本發明之技術僅需簡易之硬體即可達成加密及解密之功能，無需像習知技術使用複雜的虛擬亂數產生器，而可節省成本，同時，保護位元碼的產生及去除硬體係相當簡易，並不會如習知技術一般會增加加密及解密處理時間，而遠較習知技術需花費的加密及解密處理時間為少，故其執行效能遠較習知技術更好。

綜上所陳，本發明無論就目的、手段及功效，在在均顯示其迥異於習知技術之特徵，實為一極具實用價值之發明，懇請　貴審查委員明察，早日賜准專利，俾嘉惠社會，實感德便。惟應注意的是，上述諸多實施例僅係為了便於說明而舉例而已，本發明所主張之權利範圍自應以申請專利範圍所述為準，而非僅限於上述實施例。

【五、圖式簡單說明】

圖1：係本發明之以保護位元碼對一程式進行加密保護之裝置的方塊圖。

圖2：係本發明之第二保護位元碼位置產生裝置之電路圖。

圖3~圖4：係本發明之第二保護位元碼位置產生裝置所產生插入位置的之示意圖。

圖5：係本發明之保護位元碼去除裝置之電路圖。

圖6：係本發明之以保護位元碼對一程式進行加密保護之裝置另一實施例的方塊圖。

【圖號說明】

保護位元碼產生裝置	110	第一保護位元碼位置產生裝置	120
保護位元碼插入裝置	130	第二保護位元碼位置產生裝置	210
保護位元碼去除裝置	220		
存取狀態暫存器	310	程式狀態暫存器	320
多工器	330	插入位置產生裝置	340
插入位置產生裝置	350	插入位置產生裝置	360
插入位置產生裝置	370	插入位置產生裝置	380
多工器	510	多工器	520
多工器	530	第三保護位元碼位置產生裝置	610
第四保護位元碼位置產生裝置	620	第三保護位元碼去除裝置	630
第四保護位元碼去除裝置	640		

肆、中文發明摘要

本發係提出一種以保護位元碼對一程式進行加密保護之裝置，該程式具有複數之指令（P為正整數），該裝置包含一保護位元碼產生裝置、一第一保護位元碼位置產生裝置及一保護位元碼插入裝置。該保護位元碼產生裝置係依據該程式之複數指令以產生複數個保護位元碼，該複數個指令具有複數個位元I（I為正整數）；該第一保護位元碼位置產生裝置依據執行該程式時之處理器狀態以產生該複數個保護位元碼的複數個插入位置N（N為正整數）；該保護位元碼插入裝置依據該第一保護位元碼位置產生裝置所產生之插入位置N，分別將該複數個保護位元碼插入該程式之複數指令之第N-1與第N位元之中，以產生一加密之程式。

伍、英文發明摘要

陸、(一)、本案指定代表圖爲：圖 1

(二)、本代表圖之元件代表符號簡單說明：

保護位元碼產生裝置	110	第一保護位元碼位置產生裝置	120
保護位元碼插入裝置	130	第二保護位元碼位置產生裝置	210
保護位元碼去除裝置	220		

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

「無」

拾、申請專利範圍

1. 一種以保護位元碼對一程式進行加密保護之裝置，該程式具有複數個指令，每一指令具有I位元（I為正整數），該裝置包含：

一保護位元碼產生裝置，係依據該程式之複數個指令以產生對應之複數個保護位元碼，每一保護位元碼具有P個位元（P為正整數）；

一第一保護位元碼位置產生裝置，其依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置N（N為正整數）；以及

一保護位元碼插入裝置，係依據該第一保護位元碼位置產生裝置所產生之插入位置N，分別將每一保護位元碼插入該程式之對應指令之第N-1與第N位元之中，以產生一加密之程式。

2. 如申請專利範圍第1項所述之裝置，其更包含：

一第二保護位元碼位置產生裝置，其依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置N；以及

一保護位元碼去除裝置，係輸入該程式，並依據該第二保護位元碼位置產生裝置所產生之插入位置N，以將該程式之對應指令之第N位元去除。

3. 如申請專利範圍第2項所述之裝置，其中，該第一及第二保護位元碼位置產生裝置係依據執行該程式時之處理器狀態以產生插入位置，每一第一及第二保護位元碼位置產生裝置包含：

一位置狀態暫存器，用以指示該處理器係存取資料區段或是存取程式區段；

一程式狀態暫存器，用以指示該處理器所處之狀態；

複數個插入位置產生裝置，依據其預定之功能以產生插入位置；以及

一多工器，其具有複數個輸入端，以耦合至該複數個插入位置產生裝置之輸出端，並依據該位置狀態暫存器及該程式狀態暫存器，由複數個輸入端中選擇一插入位置以做為輸出。

4. 如申請專利範圍第3項所述之裝置，其中，該複數個插入位置產生裝置可為一空裝置，以表示無插入位置。

5. 如申請專利範圍第3項所述之裝置，其中，該複數個插入位置產生裝置可將一給定值經由函數運算以產生插入位置。

6. 如申請專利範圍第3項所述之裝置，其中，該複數個插入位置產生裝置可將一第一給定值減去經由函數運算之一第二給定值，以產生插入位置。

7. 如申請專利範圍第3項所述之裝置，其中，該複數個插入位置產生裝置可將一第一給定值與該處理器之部分位址值結合後，再經由函數運算，以產生插入位置。

8. 如申請專利範圍第3項所述之裝置，其中，該複數個插入位置產生裝置可將該位置狀態暫存器與該程式狀態暫存器結合後，以產生插入位置。

9. 如申請專利範圍第3項所述之裝置，其中，該複數個插入位置產生裝置可將該位置狀態暫存器與該程式狀態暫存器結合後，再經由函數運算，以產生插入位置。

10. 如申請專利範圍第2項所述之裝置，其中，該保護位元碼去除裝置更可依據該第二保護位元碼位置產生裝置所產生之插入位置N，而將該程式之對應指令之第N位元移至最高位元處。

11. 如申請專利範圍第2項所述之裝置，其中，該保護位元碼去除裝置更可依據該第二保護位元碼位置產生裝置所產生之插入位置N，而將該程式之對應指令之第N位元移至最低位元處。

12. 如申請專利範圍第2項所述之裝置，其中，該保護位元碼去除裝置更可依據該第二保護位元碼位置產生裝置所產生之插入位置N，而將該程式之對應指令直接輸出。

13. 如申請專利範圍第3項所述之裝置，其中，I+P=32。

14. 如申請專利範圍第3項所述之裝置，其中，I=32。

15. 一種對一加密程式進行解密之裝置，該加密程式係將保護位元碼插置於原始程式中而加密，該加密程式具有複數之指令，該裝置包含：

一第二保護位元碼位置產生裝置，其依據執行該程式時之處理器狀態以產生該複數個保護位元碼的插入位置；以及

一保護位元碼去除裝置，係輸入該程式，並依據該第二保護位元碼位置產生裝置所產生之插入位置N，以將該程式之對應指令之第N位元去除。

16. 如申請專利範圍第15項所述之裝置，其中，該第二保護位元碼位置產生裝置係依據執行該程式時之處理器狀態以產生插入位置，該第二保護位元碼位置產生裝置包含：

一位置狀態暫存器，用以指示該處理器係存取資料區段或是存取程式區段；

一程式狀態暫存器，用以指示該處理器所處之狀態；

複數個插入位置產生裝置，依據其預定之功能以產生插入位置；以及

一多工器，其具有複數個輸入端，以耦合至該複數個插入位置產生裝置之輸出端，並依據該位置狀態暫存器及該程式狀態暫存器，由複數個輸入端中選擇一插入位置以做為輸出。

17. 如申請專利範圍第16項所述之裝置，其中，該複數個插入位置產生裝置可為一空裝置，以表示無插入位置。

18. 如申請專利範圍第16項所述之裝置，其中，該複數個插入位置產生裝置可將一給定值經由函數運算以產生插入位置。

19. 如申請專利範圍第16項所述之裝置，其中，該複數個插入位置產生裝置可將一第一給定值減去經由函數運算之一第二給定值，以產生插入位置。

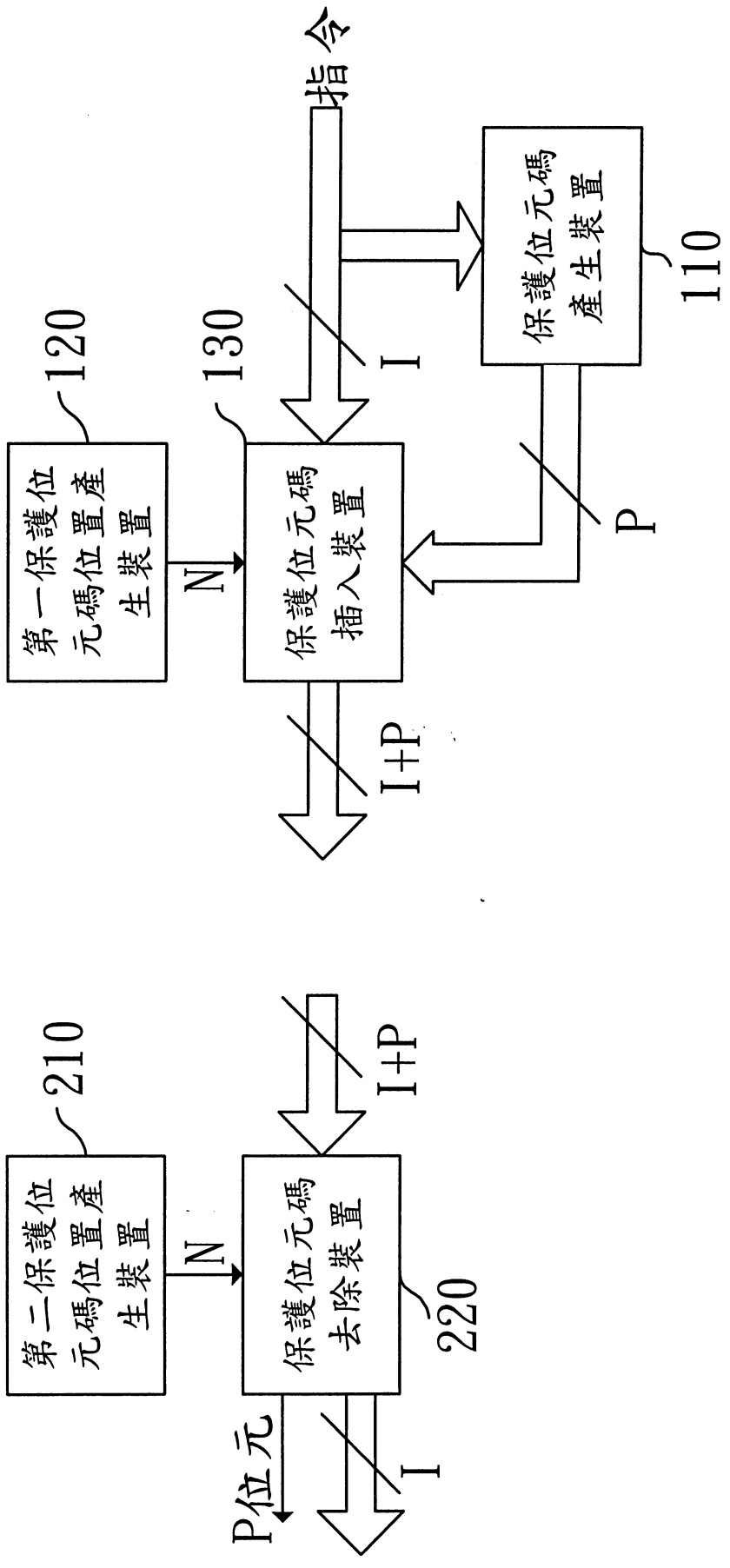
指令
保護位元碼
產生裝置
110
I
P
第一保護位
元碼位置產
生裝置
120
N
保護位元碼
插入裝置
130
I+P
第二保護位
元碼位置產
生裝置
210
N
保護位元碼
去除裝置
220
I+P
P位元
I

圖 1

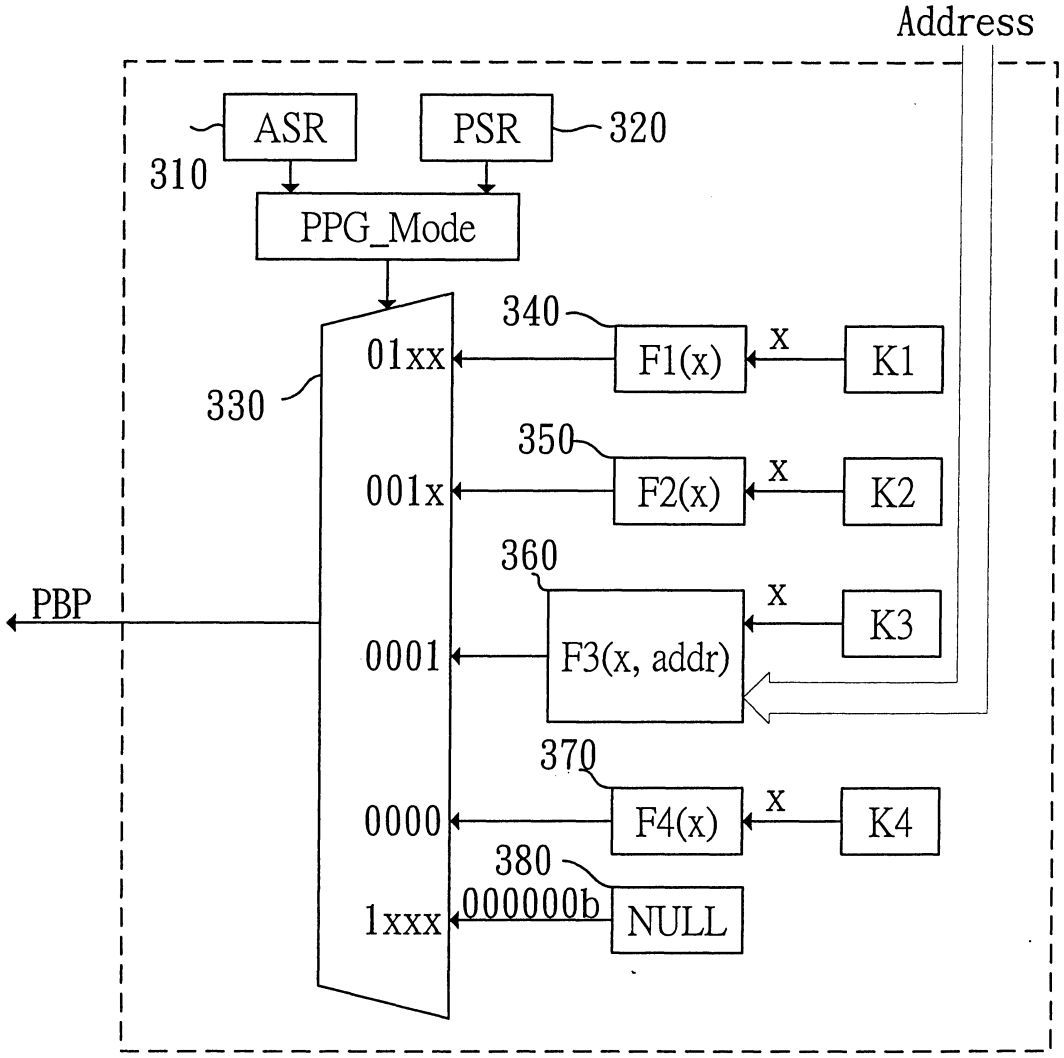
Address
ASR
PSR
320
310
PPG_Mode
340
F1(x)
x
K1
330
01xx
350
F2(x)
x
K2
001x
360
PBP
x
K3
0001
F3(x, addr)
370
F4(x)
x
K4
0000
380
000000b
NULL
1xxx

圖 2

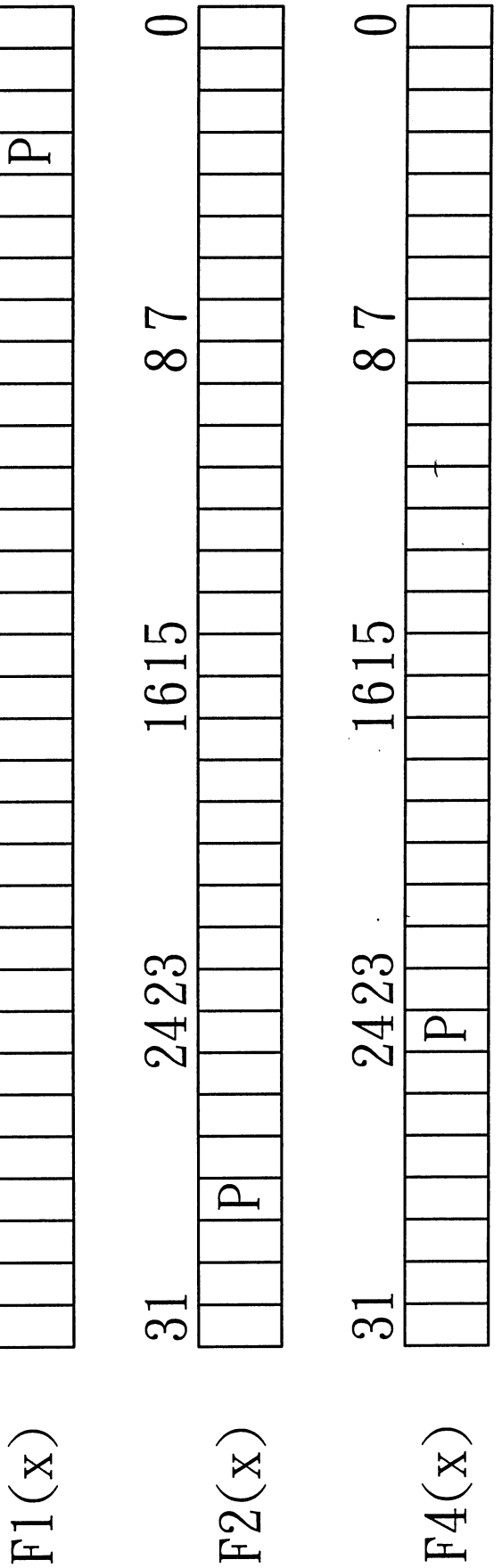

圖 3

Address	F3(x, a)
1F00 0000	3
1F00 0001	19
1F00 0010	11
1F00 0011	27
1F00 0100	7
1F00 0101	23
1F00 0110	15
1F00 0111	31

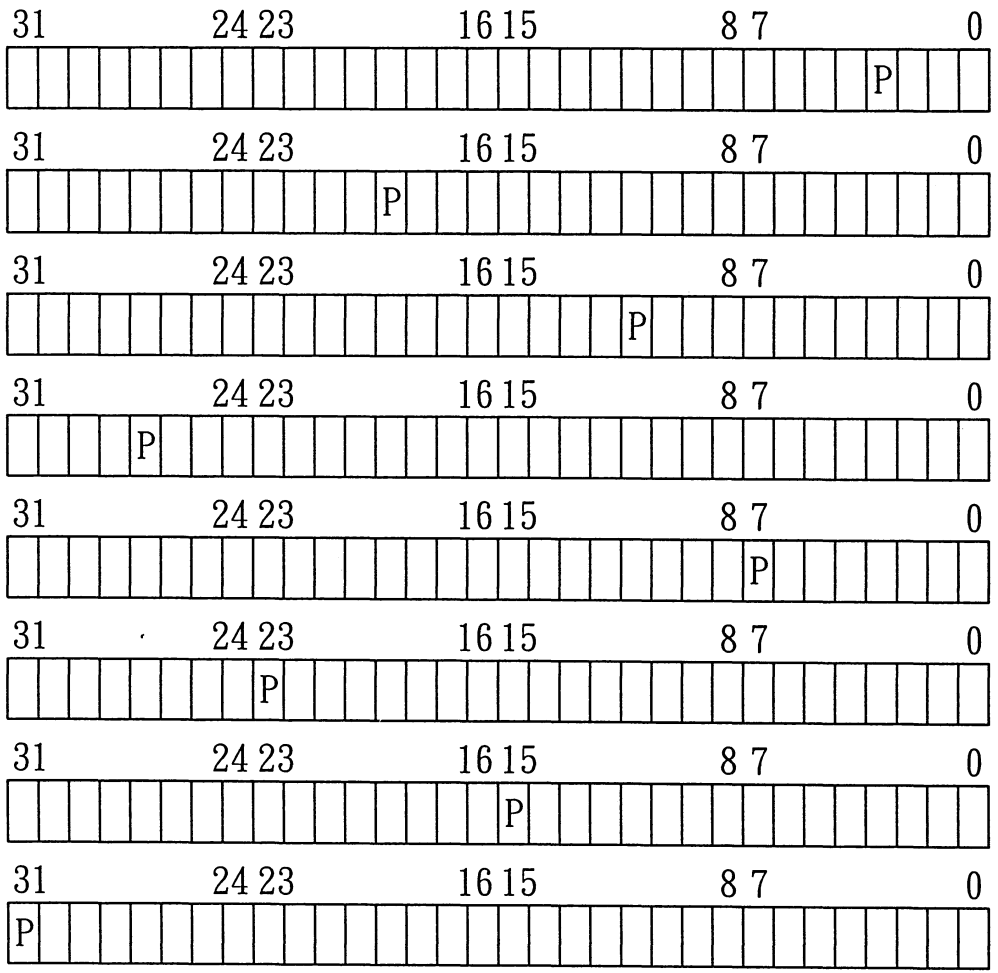

圖 4

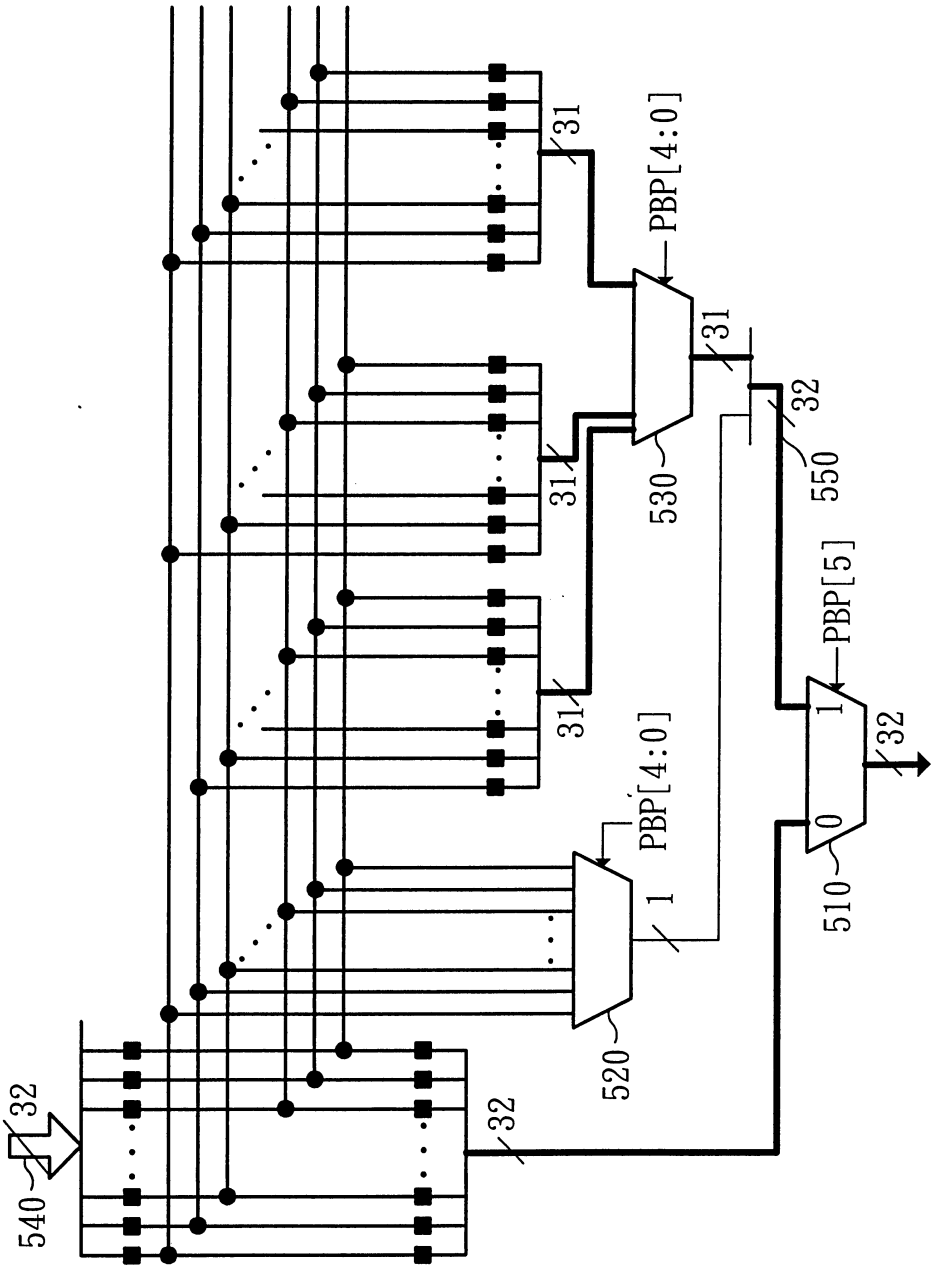

圖 5

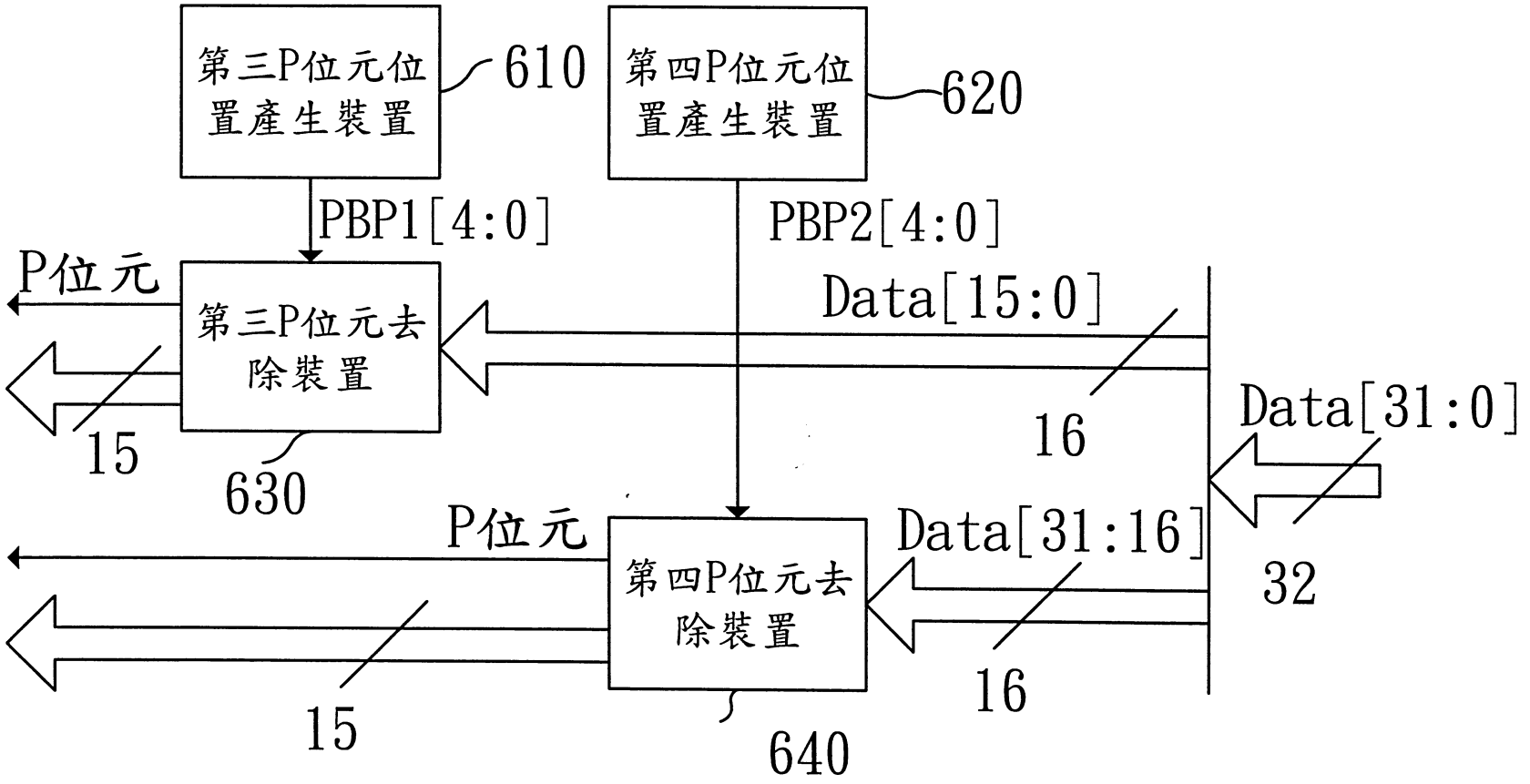
第三P位元位置產生裝置
610
第四P位元位置產生裝置
620
PBP1[4:0]
PBP2[4:0]
P位元
第三P位元去除裝置
Data[15:0]
15
630
16
Data[31:0]
P位元
第四P位元去除裝置
Data[31:16]
32
15
16
640

圖 6

20. 如申請專利範圍第16項所述之裝置，其中，該複數個插入位置產生裝置可將一第一給定值與該處理器之部分位址值值結合後，再經由函數運算，以產生插入位置。

21. 如申請專利範圍第16項所述之裝置，其中，該複數個插入位置產生裝置可將該位置狀態暫存器與該程式狀態暫存器結合後，以產生插入位置。

22. 如申請專利範圍第16項所述之裝置，其中，該複數個插入位置產生裝置可將該位置狀態暫存器與該程式狀態暫存器結合後，再經由函數運算，以產生插入位置。

23. 如申請專利範圍第16項所述之裝置，其中，I+P=32。

24. 如申請專利範圍第16項所述之裝置，其中，I=32。

25. 一種對一加密程式進行解密之裝置，該加密程式係將兩組保護位元碼插置於原始程式中而加密，該加密程式具有複數之指令，其中一個字組可包含二個加密指令，該裝置包含：

一第三保護位元碼位置產生裝置，其依據執行該程式時之處理器狀態以產生該複數個保護位元碼的第三插入位置；

一第四保護位元碼位置產生裝置，其依據執行該程式時之處理器狀態以產生該複數個保護位元碼的第四插入位置；以及

X
93 2 13

一第三保護位元碼去除裝置，係輸入該加密程式之低半字組，並依據該第三保護位元碼位置產生裝置所產生之第三插入位置N1，以將該該程式之對應指令之第0至（K-1）位元之第N1位元去除；以及

一第四保護位元碼去除裝置，係輸入該加密程式之高半字組，並依據該第四保護位元碼位置產生裝置所產生之第四插入位置N2，以將該該程式之對應指令之第K至（2K-1）位元之第N2位元去除。

26. 如申請專利範圍第25項所述之裝置，其中，K=16。

27. 一種以保護位元碼對一程式進行加密保護之方法，該程式具有複數個指令，每一指令具有I位元（I為正整數），該方法包含下列步驟：

一保護位元碼產生步驟，係依據該程式之複數個指令以產生對應之複數個保護位元碼，每一保護位元碼具有P個位元（P為正整數）；

一第一保護位元碼位置產生步驟，其依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置N（N為正整數）；以及

一保護位元碼插入步驟，係依據該第一保護位元碼位置產生步驟所產生之插入位置N，分別將每一保護位元碼插入該程式之對應指令之第N-1與第N位元之中，以產生一加密之程式。

28. 如申請專利範圍第27項所述之方法，其更包含下列步驟：

一第二保護位元碼位置產生步驟，其依據執行該程式時之處理器狀態以產生每一保護位元碼的插入位置N；以及

一保護位元碼去除步驟，係輸入該程式，並依據該第二保護位元碼位置產生步驟所產生之插入位置N，以將該程式之對應指令之第N位元去除。

29. 如申請專利範圍第28項所述之方法，其中，該第一及第二保護位元碼位置產生步驟係依據執行該程式時之處理器狀態以產生插入位置，其中，一位置狀態旗標係用以指示該處理器係存取資料區段或是存取程式區段，一程式狀態旗標係用以指示該處理器所處之狀態，每一第一及第二保護位元碼位置產生步驟更包含下列步驟：

複數個插入位置產生步驟，依據其預定之功能以產生插入位置；以及

一多工步驟，依據該位置狀態旗標及該程式狀態旗標，由複數個插入位置產生步驟之輸出，選擇一插入位置以做為輸出。

30. 如申請專利範圍第29項所述之方法，其中，該複數個插入位置產生步驟可為一空步驟，以表示無插入位置。

31. 如申請專利範圍第29項所述之方法，其中，該複數個插入位置產生步驟可將一給定值經由函數運算以產生插入位置。

32. 如申請專利範圍第29項所述之方法，其中，該複數個插入位置產生步驟可將一第一給定值減去經由函數運算之一第二給定值，以產生插入位置。

33. 如申請專利範圍第29項所述之方法，其中，該複數個插入位置產生步驟可將一第一給定值與該處理器之部分位址值結合後，再經由函數運算，以產生插入位置。

34. 如申請專利範圍第29項所述之方法，其中，該複數個插入位置產生步驟可將該位置狀態旗標與該程式狀態旗標結合後，以產生插入位置。

35. 如申請專利範圍第29項所述之方法，其中，該複數個插入位置產生步驟可將該位置狀態旗標與該程式狀態旗標結合後，再經由函數運算，以產生插入位置。

36. 如申請專利範圍第28項所述之方法，其中，該保護位元碼去除步驟更可依據該第二保護位元碼位置產生步驟所產生之插入位置N，而將該程式之對應指令之第N位元移至最高位元處。

37. 如申請專利範圍第28項所述之方法，其中，該保護位元碼去除步驟更可依據該第二保護位元碼位置產生步驟所產生之插入位置N，而將該程式之對應指令之第N位元移至最低位元處。

38. 如申請專利範圍第28項所述之方法，其中，該保護位元碼去除步驟更可依據該第二保護位元碼位置產生步驟所產生之插入位置N，而將該程式之對應指令直接輸出。

39. 如申請專利範圍第29項所述之方法，其中，I+P=32。

40. 如申請專利範圍第29項所述之方法，其中，I=32。

41. 一種對一加密程式進行解密之方法，該加密程式係將保護位元碼插置於原始程式中而加密，該加密程式具有複數之指令，該方法包含下列步驟：

一第二保護位元碼位置產生步驟，其依據執行該程式時之處理器狀態以產生該複數個保護位元碼的插入位置；以及

一保護位元碼去除步驟，係輸入該程式，並依據該第二保護位元碼位置產生步驟所產生之插入位置N，以將該程式之對應指令之第N位元去除。

42. 如申請專利範圍第41項所述之方法，其中，該第二保護位元碼位置產生步驟係依據執行該程式時之處理器狀態以產生插入位置，其中，一位置狀態旗標係用以指示該處理器係存取資料區段或是存取程式區段，一程式狀態旗標係用以指示該處理器所處之狀態，該第二保護位元碼位置產生步驟更包含下列步驟：

複數個插入位置產生步驟，依據其預定之功能以產生插入位置；以及

一多工步驟，依據該位置狀態旗標及該程式狀態旗標，由複數個插入位置產生步驟之輸出，選擇一插入位置以做為輸出。

43. 如申請專利範圍第42項所述之方法，其中，該複數個插入位置產生步驟可為一空步驟，以表示無插入位置。

44. 如申請專利範圍第42項所述之方法，其中，該複數個插入位置產生步驟可將一給定值經由函數運算以產生插入位置。

45. 如申請專利範圍第42項所述之方法，其中，該複數個插入位置產生步驟可將一第一給定值減去經由函數運算之一第二給定值，以產生插入位置。

46. 如申請專利範圍第42項所述之方法，其中，該複數個插入位置產生步驟可將一第一給定值與該處理器之部分位址值結合後，再經由函數運算，以產生插入位置。

47. 如申請專利範圍第42項所述之方法，其中，該複數個插入位置產生步驟可將該位置狀態暫存器與該程式狀態暫存器結合後，以產生插入位置。

48. 如申請專利範圍第42項所述之方法，其中，該複數個插入位置產生步驟可將該位置狀態暫存器與該程式狀態暫存器結合後，再經由函數運算，以產生插入位置。

49. 如申請專利範圍第42項所述之方法，其中，I+P=32。

50. 如申請專利範圍第42項所述之方法，其中，I=32。

修正替換頁
更
93年2月13日

51. 一種對一加密程式進行解密之方法，該加密程式係將兩組保護位元碼插置於原始程式中而加密，該加密程式具有複數之指令，其中一個字組可包含二個加密指令，該方法包含下列步驟：

一第三保護位元碼位置產生步驟，其依據執行該程式時之處理器狀態以產生該複數個保護位元碼的第三插入位置；

一第四保護位元碼位置產生步驟，其依據執行該程式時之處理器狀態以產生該複數個保護位元碼的第四插入位置；以及

一第三保護位元碼去除步驟，係輸入該加密程式之低半字組，並依據該第三保護位元碼位置產生步驟所產生之第三插入位置N1，以將該該程式之對應指令之第0至（K-1）位元之第N1位元去除；以及

一第四保護位元碼去除步驟，係輸入該加密程式之高半字組，並依據該第四保護位元碼位置產生步驟所產生之第四插入位置N2，以將該該程式之對應指令之第K至（2K-1）位元之第N2位元去除。

52. 如申請專利範圍第51項所述之方法，其中，K=16。