I631482

(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 I631482 B**

(45)公告日： 中華民國 107 (2018) 年 08 月 01 日

(21)申請案號：105125524 (22)申請日： 中華民國 105 (2016) 年 08 月 10 日

(51)Int. Cl.： *G06F21/71 (2013.01)* *G11C7/24 (2006.01)*

(30)優先權：2015/08/17 美國 14/828,151

(71)申請人：美光科技公司 (美國) MICRON TECHNOLOGY, INC. (US)
美國

(72)發明人：李 佩瑞 V LEA, PERRY V. (US)

(74)代理人：陳長文

(56)參考文獻：

CN	100424611C	CN	104272251A
US	7073059B2	US	8799678B2
US	2015/0186296A1		

審查人員：李榮祥

申請專利範圍項數：21 項 圖式數：6 共 44 頁

(54)名稱

計算記憶體中可執行指令之加密之方法及設備

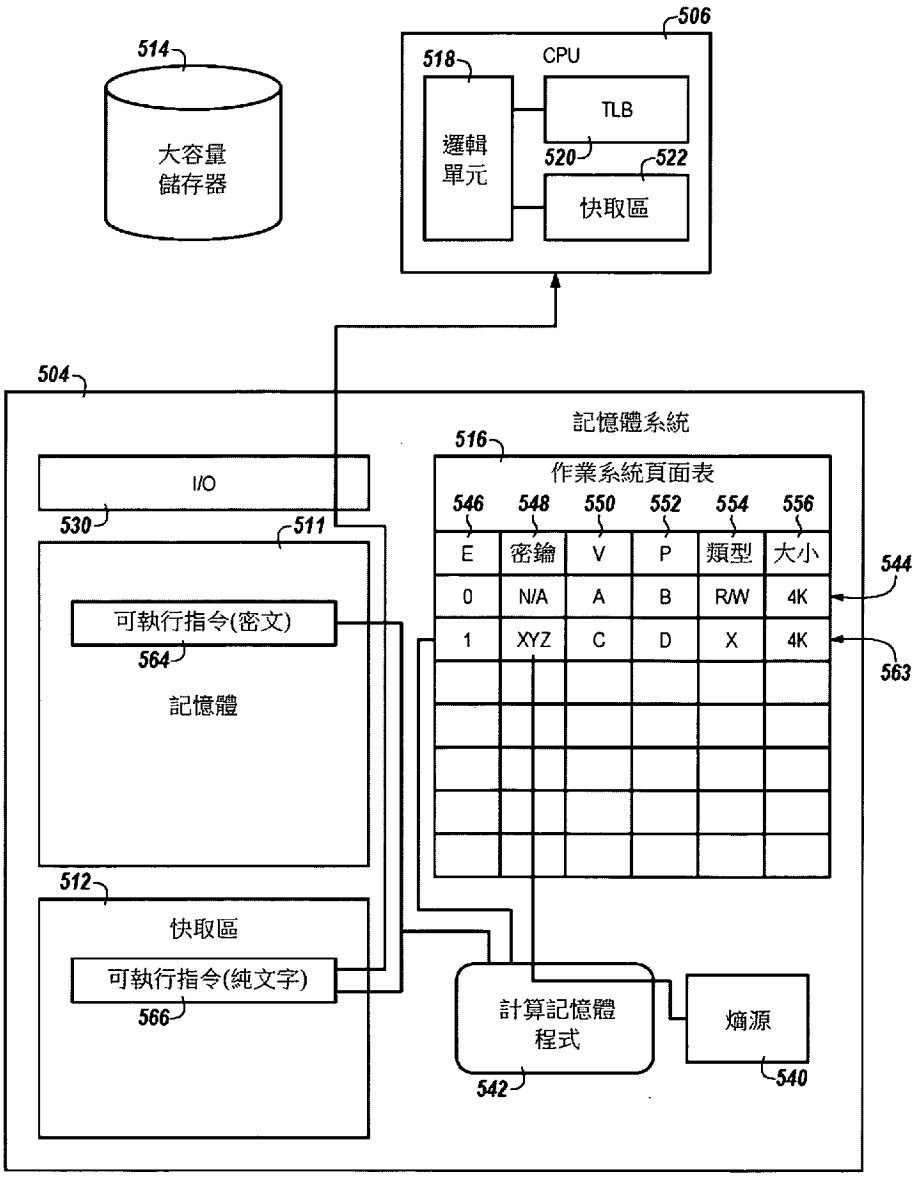
METHOD AND APPARATUS OF ENCRYPTION OF EXECUTABLES IN COMPUTATIONAL MEMORY

(57)摘要

本發明係關於計算記憶體中之可執行指令之加密。計算記憶體可周遊該計算記憶體體中之一作業系統頁面表以尋找標記為可執行指令之一頁面。回應於尋找到標記為可執行指令之一頁面，該計算記憶體可判定標記為可執行指令之該頁面是否已加密。回應於判定標記為可執行指令之該頁面未加密，該計算記憶體可針對標記為可執行指令之該頁面產生一密鑰。該計算記憶體可使用該密鑰加密標記為可執行指令之該頁面。

The present disclosure is related to encryption of executables in computational memory. Computational memory can traverse an operating system page table in the computational memory for a page marked as executable. In response to finding a page marked as executable, the computational memory can determine whether the page marked as executable has been encrypted. In response to determining that the page marked as executable is not encrypted, the computational memory can generate a key for the page marked as executable. The computational memory can encrypt the page marked as executable using the key.

指定代表圖：



【圖 5】

符號簡單說明：

504・・・計算記憶體系統

506・・・中央處理單元

511・・・記憶體陣列

512・・・計算記憶體系統快取區

514・・・大容量儲存裝置

516・・・作業系統頁面表

518・・・邏輯單元

520・・・轉譯後備緩衝器

522・・・CPU 快取區

530・・・I/O 電路

540・・・熵源

542・・・計算記憶體程式

546・・・加密指示欄位

548・・・密鑰欄位

550・・・虛擬位址欄位

552・・・實體位址欄位

554・・・類型欄位

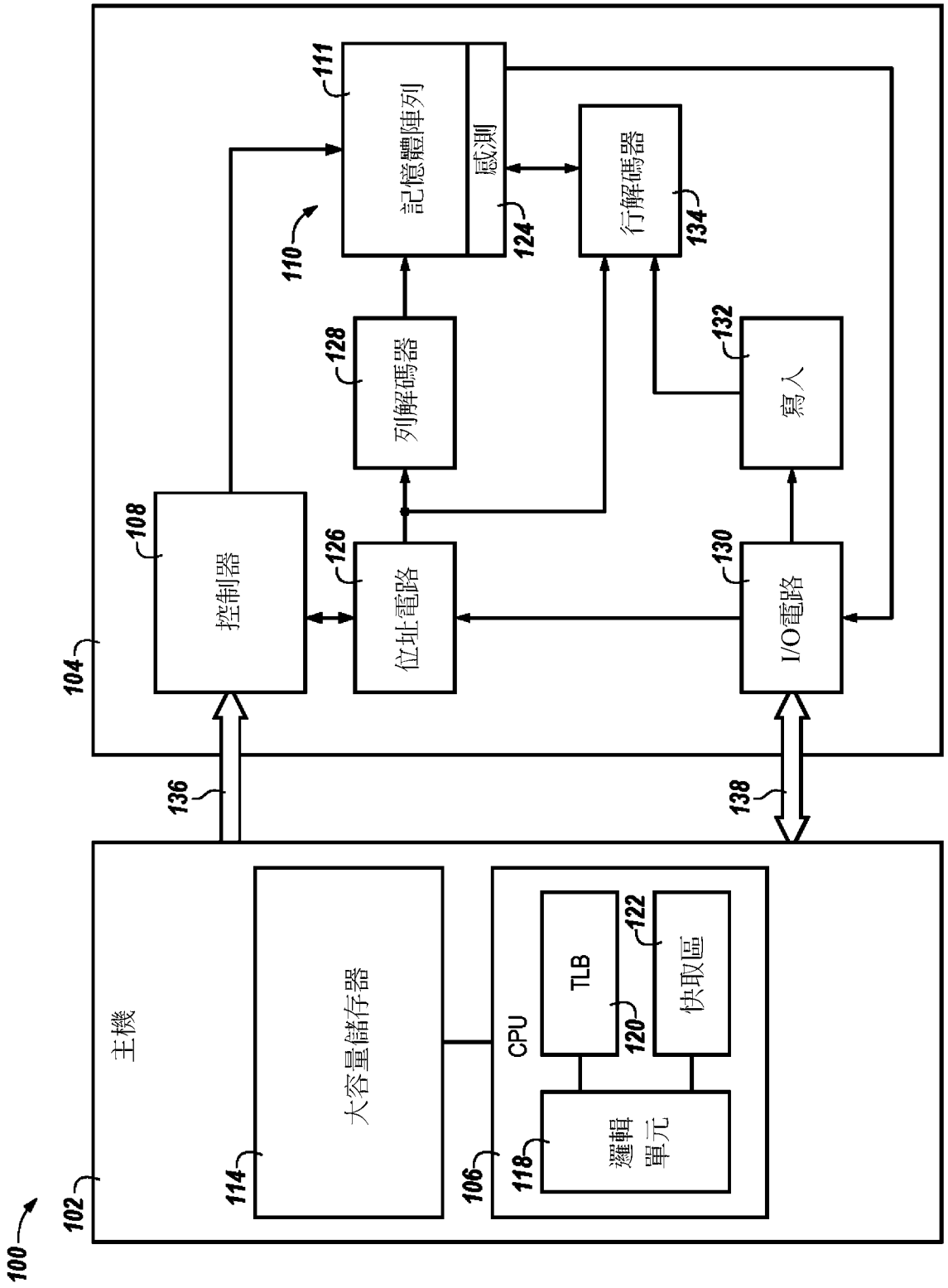
556・・・大小欄位

563・・・第三表項目

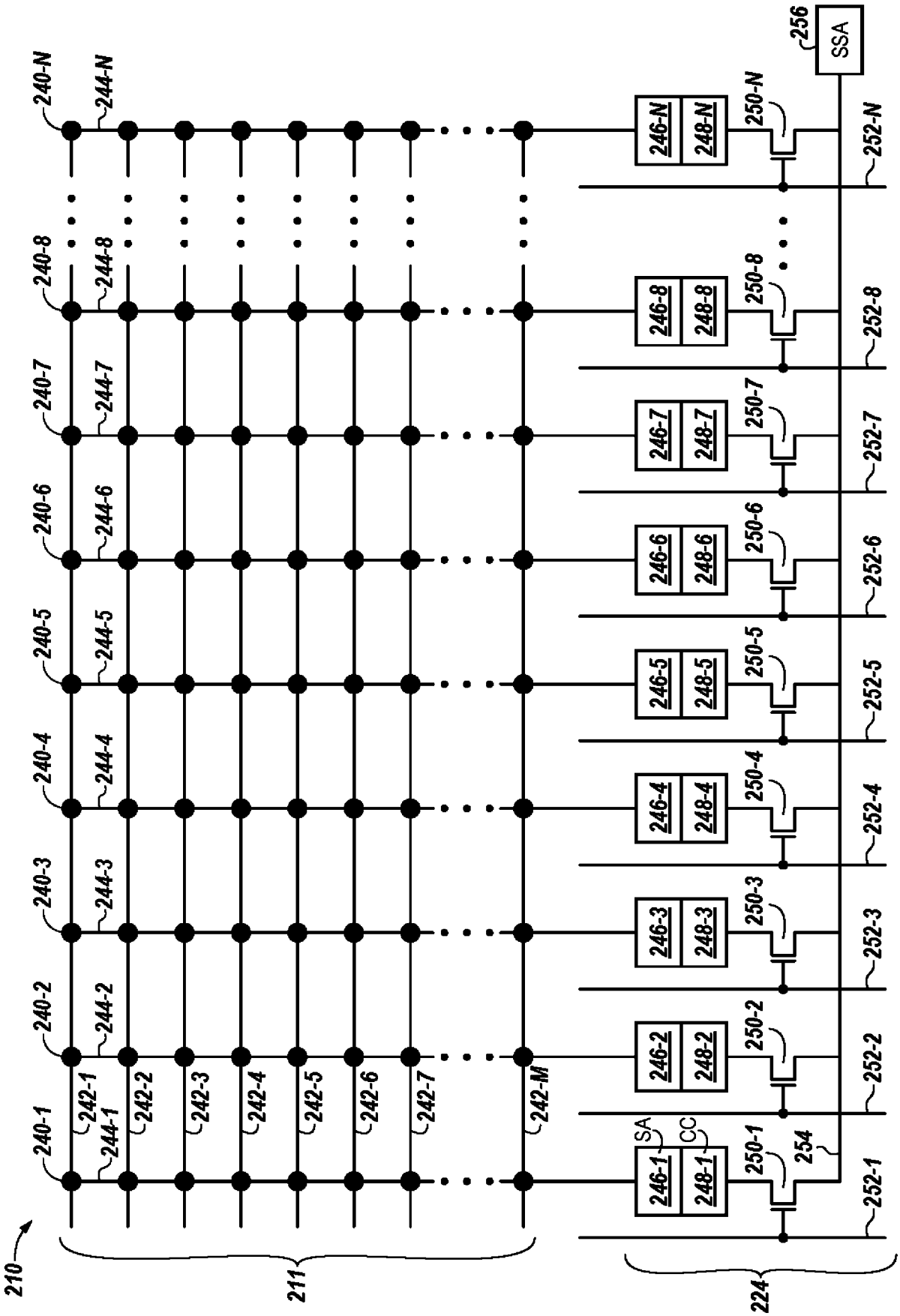
564・・・密文可執行指令

566・・・純文字可執行指令

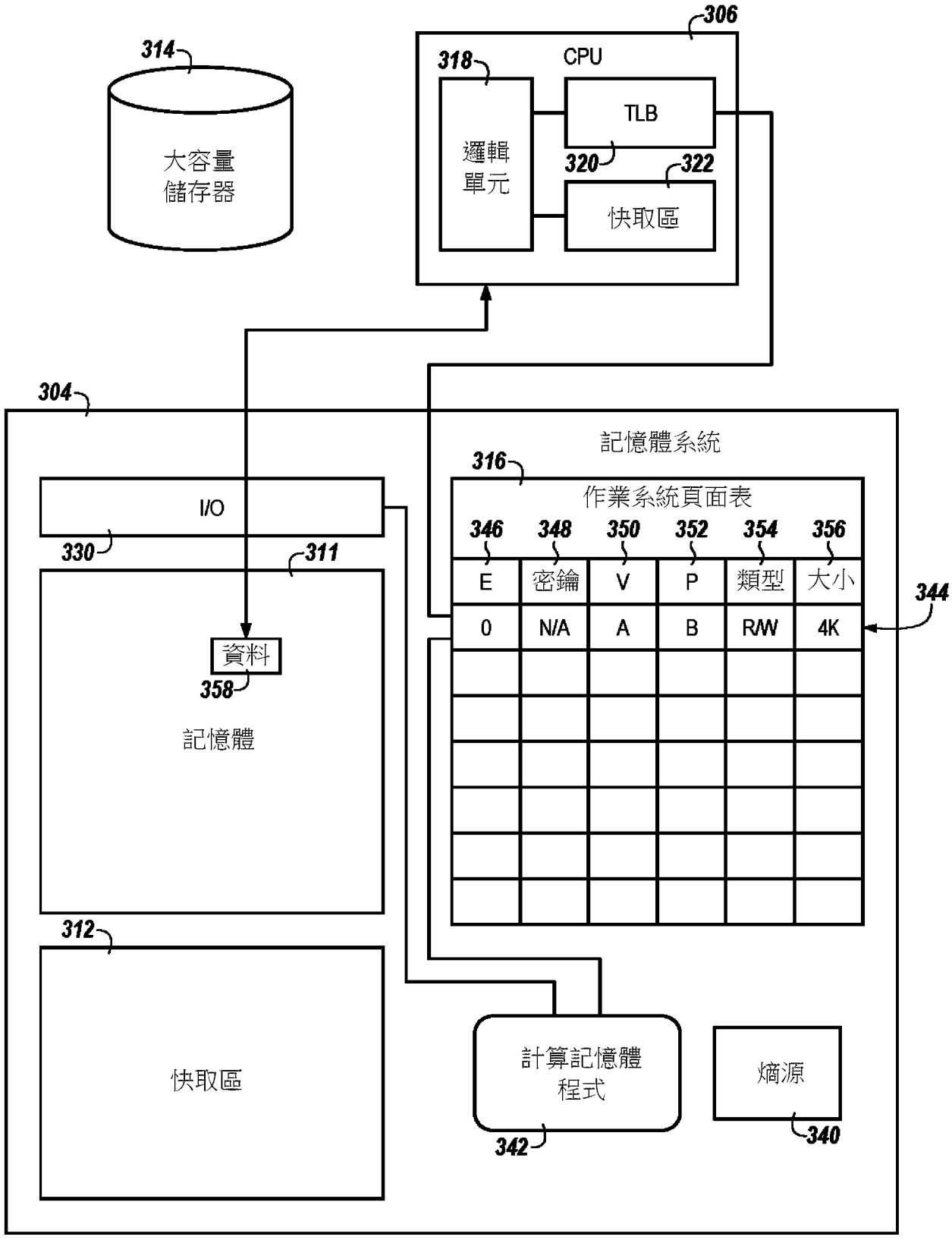
【發明圖式】


100
102
主機
114
大容量儲存器
106
CPU
118
邏輯單元
TLB
120
122
快取區
136
138
104
108
控制器
126
位址電路
128
列解碼器
110
111
記憶體陣列
感測
124
行解碼器
134
132
寫入
130
I/O電路

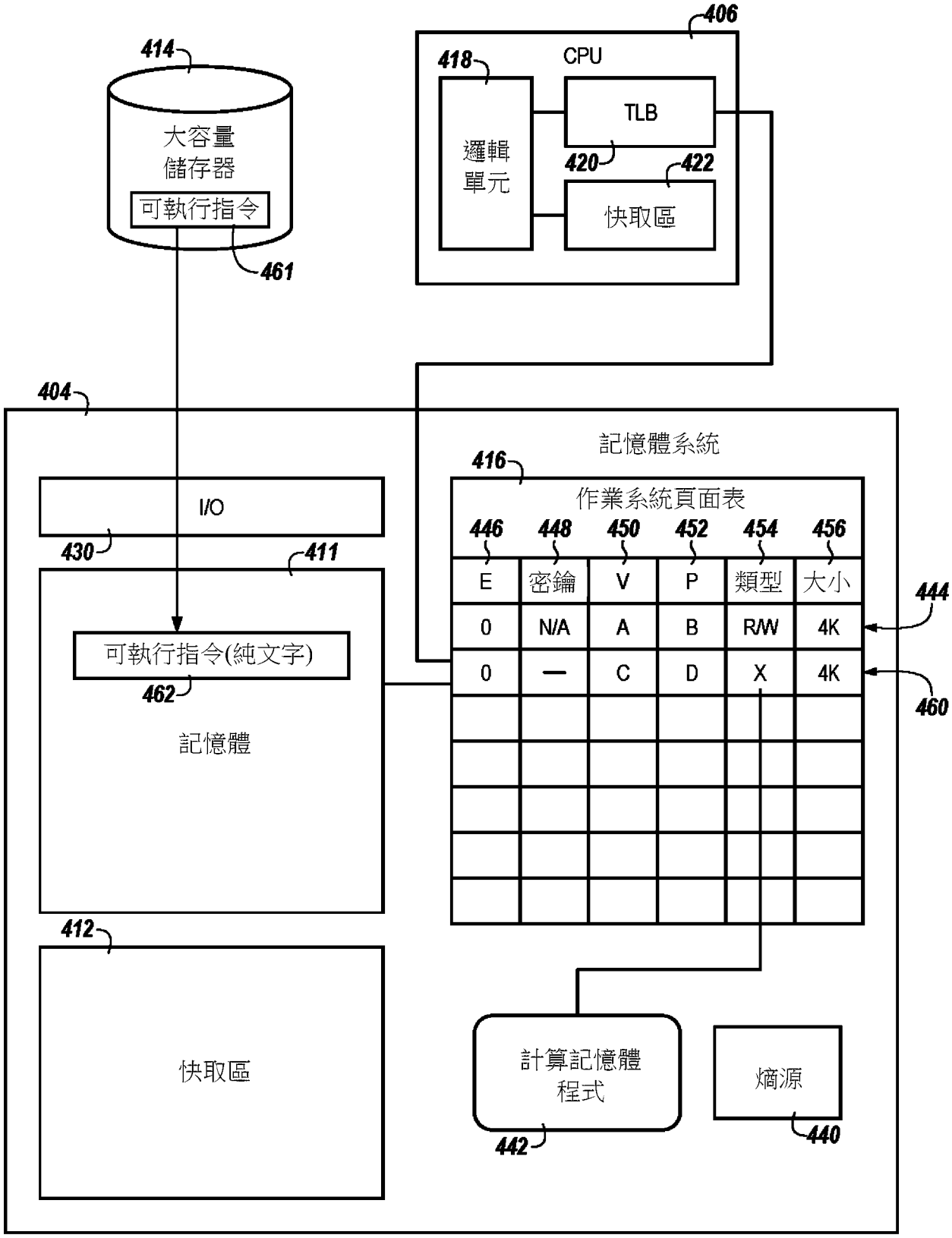
【圖 1】


210
211
224
240-1
240-2
240-3
240-4
240-5
240-6
240-7
240-8
240-N
242-1
242-2
242-3
242-4
242-5
242-6
242-7
242-M
244-1
244-2
244-3
244-4
244-5
244-6
244-7
244-8
244-N
246-1
246-2
246-3
246-4
246-5
246-6
246-7
246-8
246-N
248-1
248-2
248-3
248-4
248-5
248-6
248-7
248-8
248-N
250-1
250-2
250-3
250-4
250-5
250-6
250-7
250-8
250-N
252-1
252-2
252-3
252-4
252-5
252-6
252-7
252-8
252-N
254
256
SSA
SA
CC

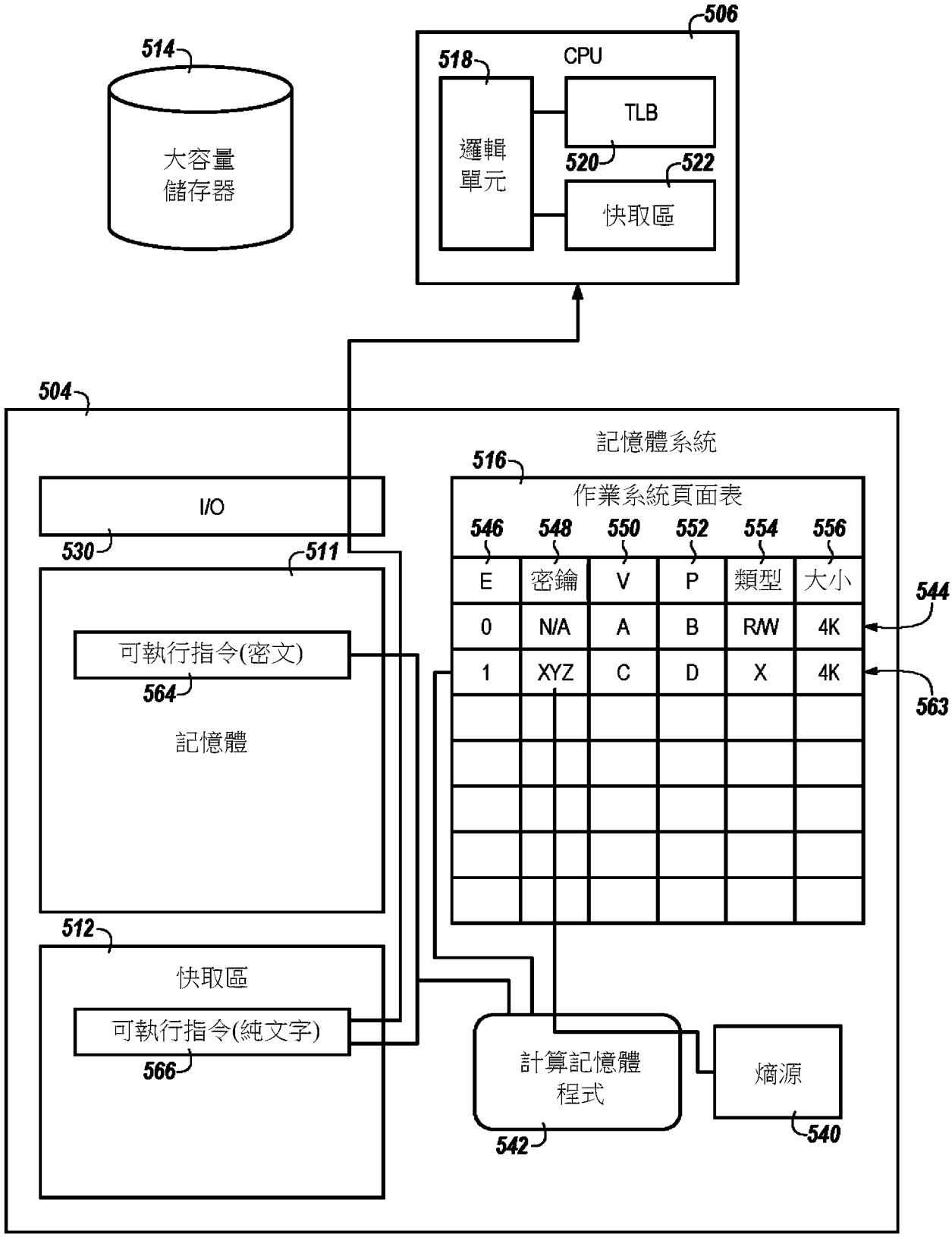
【圖 2】


306
314
318
CPU
大容量
儲存器
TLB
邏輯
單元
320
322
快取區
304
記憶體系統
316
作業系統頁面表
346
348
350
352
354
356
E
密鑰
V
P
類型
大小
344
0
N/A
A
B
R/W
4K
I/O
330
311
資料
358
記憶體
312
快取區
計算記憶體
程式
342
熵源
340

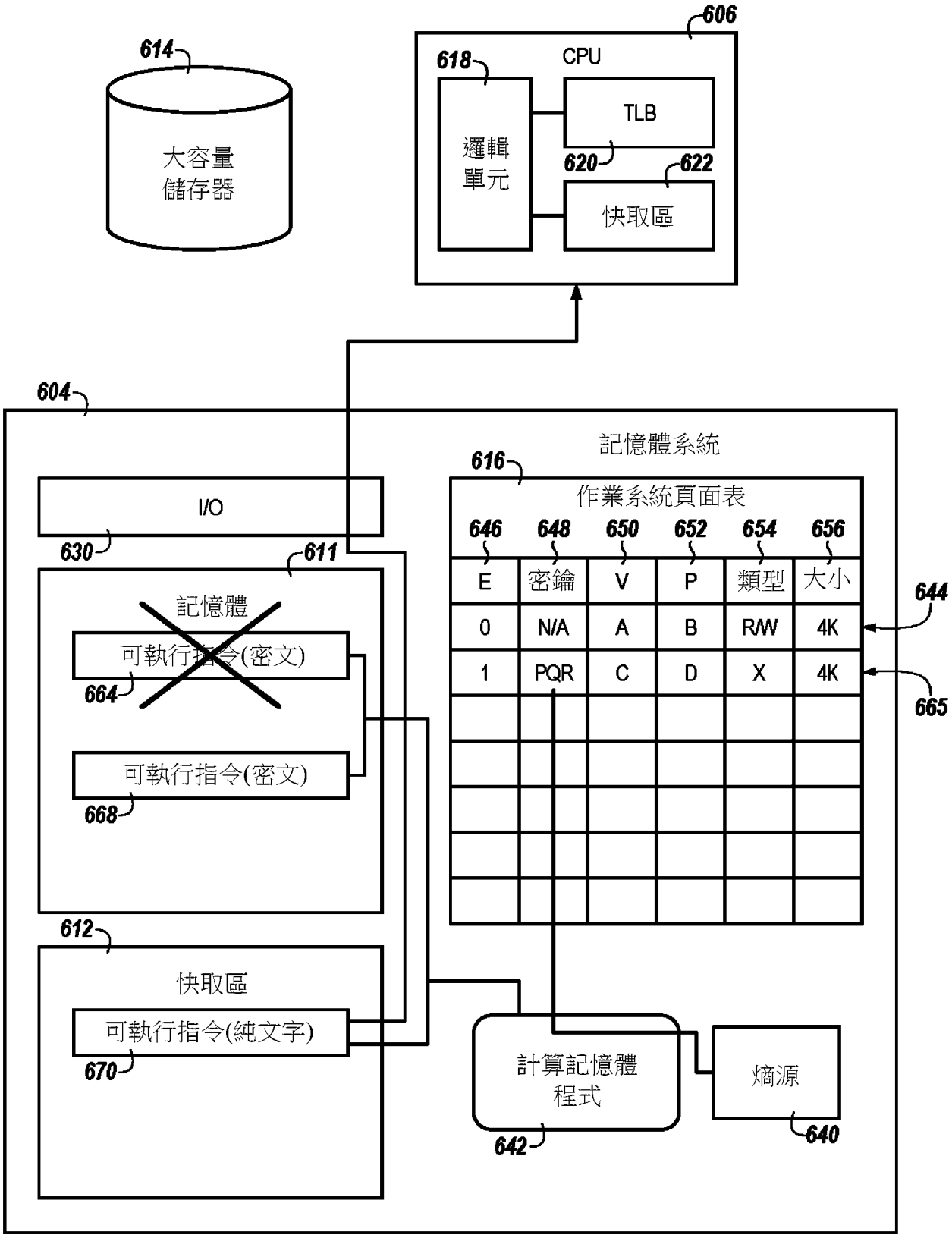
【圖 3】


406
CPU
418
TLB
邏輯
單元
420
422
快取區
414
大容量
儲存器
可執行指令
461
404
記憶體系統
416
作業系統頁面表
446
448
450
452
454
456
E
密鑰
V
P
類型
大小
444
0
N/A
A
B
R/W
4K
0
—
C
D
X
4K
460
I/O
430
411
可執行指令(純文字)
462
記憶體
412
快取區
計算記憶體
程式
442
熵源
440

【圖 4】


506
514
518
CPU
大容量
儲存器
TLB
邏輯
單元
520
522
快取區
504
記憶體系統
516
作業系統頁面表
I/O
546
548
550
552
554
556
530
511
E
密鑰
V
P
類型
大小
544
0
N/A
A
B
R/W
4K
可執行指令(密文)
1
XYZ
C
D
X
4K
564
563
記憶體
512
快取區
可執行指令(純文字)
566
計算記憶體
程式
熵源
542
540

【圖 5】


606
614
618
CPU
大容量
儲存器
TLB
邏輯
單元
620
622
快取區
604
記憶體系統
616
作業系統頁面表
I/O
646
648
650
652
654
656
630
611
E
密鑰
V
P
類型
大小
644
記憶體
0
N/A
A
B
R/W
4K
可執行指令(密文)
664
1
PQR
C
D
X
4K
665
可執行指令(密文)
668
612
快取區
可執行指令(純文字)
670
計算記憶體
程式
熵源
642
640

【圖 6】

【發明說明書】

【中文發明名稱】

計算記憶體中可執行指令之加密之方法及設備

【英文發明名稱】

METHOD AND APPARATUS OF ENCRYPTION OF EXECUTABLES IN COMPUTATIONAL MEMORY

【技術領域】

本發明大體上係關於半導體記憶體及方法，且更特定言之，本發明係關於計算記憶體中之可執行指令之加密。

【先前技術】

記憶體裝置通常提供為計算裝置或其它電子裝置中之內部、半導體、積體電路。存在諸多不同類型的記憶體，包含揮發性記憶體及非揮發性記憶體。揮發性記憶體可需要電力來維持其資料(例如，使用者資料、錯誤資料等)且包含隨機存取記憶體(RAM)、動態隨機存取記憶體(DRAM)及同步動態隨機存取記憶體(SDRAM)以及其它。非揮發性記憶體可藉由在未被供電時保持所儲存之資料而提供持久性資料且可包含NAND快閃記憶體、NOR快閃記憶體、唯讀記憶體(ROM)、電可擦除可程式化ROM (EEPROM)、可擦除可程式化ROM (EPROM)及電阻可變記憶體(諸如，相變隨機存取記憶體(PCRAM)、電阻性隨機存取記憶體(RRAM)及磁阻性隨機存取記憶體(MRAM)，諸如自旋力矩轉移隨機存取記憶體(STT RAM))以及其它。

運算系統通常包含若干處理資源(例如，一或多個處理器)，其等可擷取並執行指令且將所執行指令之結果儲存至一適合位置。一處理器可包括

若干功能單元(例如，在本文中稱為功能單元電路(FUC))，諸如算術邏輯單元(ALU)電路、浮點單元(FPU)電路及/或一組合邏輯區塊，例如，其等可執行指令以對資料(例如，一或多個運算元)執行邏輯運算(諸如「及」、「或」、「非」、「反及」、「反或」及「互斥或」邏輯運算)。

在提供指令至功能單元電路以供執行時可涉及一運算系統中之若干組件。指令可由(例如)諸如一控制器及/或主機處理器之一處理資源產生。可將資料(例如，將對其執行指令以執行邏輯運算之運算元)儲存於可由FUC存取之一記憶體陣列中。指令及/或資料可自記憶體陣列擷取且可在FUC開始對資料執行指令之前序列化及/或緩衝。此外，因為可透過FUC而在一或多個時脈週期中執行不同類型的運算，所以亦可序列化及/或緩衝運算及/或資料之中間結果。在諸多例項中，處理資源(例如，處理器及/或相關聯的FUC)可位於記憶體陣列之外部，且可(例如經由處理資源與記憶體陣列之間的一匯流排)存取資料以執行指令。資料可經由一匯流排從記憶體陣列移動到該記憶體陣列外部的暫存器。

【發明內容】

【圖式簡單說明】

圖1為根據本發明之若干實施例之呈包含至少一個計算記憶體系統之一運算系統之形式之一設備之一方塊圖。

圖2為根據本發明之若干實施例之一計算記憶體裝置之一部分之一示意圖。

圖3為繪示根據本發明之若干實施例之一讀取或寫入存取之一方塊流程圖。

圖4為繪示根據本發明之若干實施例之一新頁面分配之一方塊流程圖。

圖5為繪示根據本發明之若干實施例之可執行指令之加密之一方塊流程圖。

圖6為繪示根據本發明之若干實施例之對一已加密可執行指令之一隨後存取之一方塊流程圖。

【實施方式】

多數現代電腦架構使用一暫存器-記憶體技術，其中在兩個個別域中執行運算。通常對若干暫存器檔案執行邏輯運算(例如，算術、流程控制及組合運算)。通常對記憶體裝置執行記憶體操作(例如，加載、儲存等)。暫存器-記憶體架構中之指令利用暫存器索引或記憶體位址來指示如何/在何處執行一運算。

計算記憶體，諸如記憶體中處理(PIM)或記憶體裝置附近處理可分類為計算架構分類法中之記憶體間裝置。在計算記憶體中，對記憶體裝置就地執行邏輯運算及記憶體操作兩者。記憶體間架構中之指令使用實體位址指示如何/在何處執行一運算。

試圖攻擊或將惡意軟體插入至一運算系統中通常包含改變由主機處理器執行之指令流程或指令之一病毒或惡意軟體。本發明之一些實施例使用計算記憶體來加密可執行指令(可執行指令，諸如主機處理器指令)。加密可多態隨機化可執行指令，使得一攻擊者將必須瞭解加密狀態以注入將對此一系統有一負面影響之惡意軟體。可執行指令之隨機化可混淆及/或改變可執行指令以產生二進位分集之一生態系統，此可減少及/或消除惡意軟體及/或系統洩露之一來源。試圖注入程式碼之任何惡意軟體(例如，

二進位注入、緩衝區溢位攻擊、莫里斯(Morris)蠕蟲、紅色警戒(Code Red)、疾風(Blaster)病毒、統一資源定位器(URL)堆積漏洞利用等)將必須理解底層指令集架構以便運行程式碼。

本發明係關於計算記憶體中之可執行指令之加密。計算記憶體可周遊計算記憶體中之一作業系統頁面表以尋找針對標記為可執行指令之一頁面。回應於尋找到標記為可執行指令之一頁面，計算記憶體可判定標記為可執行指令之該頁面是否已加密。回應於判定標記為可執行指令之該頁面未加密，計算記憶體可針對標記為可執行指令之該頁面產生一密鑰。計算記憶體可使用該密鑰加密標記為可執行指令之該頁面。本發明之一些實施例為可執行指令而非資料提供加密，此有利地允許在無一加密及/或解密程序之情況下改變、讀取、寫入資料等，同時為可作為特定攻擊者之目標之可執行指令提供保護。可執行指令(executable instructions)在本文中通常稱為可執行指令(executables)。

在本發明之下文詳細描述中，參考隨附圖式(其等形成本發明之一部分，且其中以圖解之方式展示可如何實踐本發明之若干實施例)。此等實施例被足夠詳細地描述以使一般技術者能夠實踐本發明之該等實施例，且應瞭解可利用其它實施例，且可在不脫離本發明之範疇之情況下作出程序、電及/或結構變化。如本文中所用，標示符「M」及「N」(尤其針對圖式中之元件符號)指示：可包含如此標示之若干特定特徵。如本文中所用，「若干」特定事物可指代一或多個此等事物(例如，若干記憶體裝置可指代一或多個記憶體裝置)。如本文中所用，術語「第一」及「第二」用於區分一特徵與另一特徵，且未必暗指如此標示之特徵之間之一順序。

本文中之圖遵循一編號慣例，其中第一數字對應於圖式圖號且其餘

數字識別圖式中之一元件或組件。可藉由使用類似數字而識別不同圖之間之類似元件或組件。例如，110可指涉圖1中之元件「10」，且一類似元件可在圖2中指涉為210。可用其後有一連字符及另一數字或字母之一元件符號指涉一圖內之多個類似元件。例如，240-1可指涉圖2中之元件20-1且240-N可指涉可類似於元件240-1之元件40-N。通常可在無連字符及額外數字或字母之情況下指涉此等類似元件。例如，元件240-1、…、240-N可統稱為240。如應瞭解，可添加、交換及/或剔除本文中在各種實施例中所展示之元件以便提供本發明之若干額外實施例。另外，如應瞭解，圖中所提供元件之比例及相對尺度意欲繪示本發明之某些實施例，且不應被理解為限制意義。

圖1為根據本發明之若干實施例之呈包含至少一個計算記憶體系統104之一運算系統100之形式之一設備之一方塊圖。如本文中所用，一主機102、一計算記憶體系統104、一計算記憶體裝置110、一記憶體陣列111及/或感測電路124 (包含感測放大器及計算電路)可各自亦被單獨視為一「設備」。

運算系統100可包含耦合至計算記憶體系統104之一主機102，該計算記憶體系統104包含一計算記憶體裝置110 (例如，包含一記憶體陣列111及/或感測電路124)。計算記憶體系統104可充當一習知記憶體及/或一計算記憶體。主機102可為一主機系統，諸如一個人膝上型電腦、一桌上型電腦、一數位相機、一行動電話或一記憶體卡讀取器，以及各種其它類型的主機。主機102可包含一系統主機板及/或背板且可包含若干處理資源(例如一或多個處理器、微處理器或一些其它類型的控制電路)，諸如中央處理單元(CPU) 106。CPU 106可耦合至大容量儲存器114。大容量儲存

器114可為不可由CPU 106直接存取之一儲存裝置或其它媒體，諸如硬碟機、固態磁碟、光碟機且可為非揮發性記憶體。在一些實施例中，大容量儲存器114可位於主機102之外部。主機102可組態有一作業系統。作業系統為管理硬體資源且為在作業系統上運行之其它可執行指令(應用程式)提供服務之可執行指令(軟體)。作業系統可實施一虛擬記憶體系統。

CPU 106可包含耦合至一轉譯後備緩衝器(TLB) 120及CPU快取區122之一邏輯單元118。一邏輯單元118之一實例為一算術邏輯單元(ALU)，其為可對整數型二進位數執行算術及按位元邏輯運算之一電路。若干ALU可用於充當一浮點單元(FPU)及/或圖形處理單元(GPU)，該浮點單元為運算浮點數目之一電路，該圖形處理單元為加速旨在用於輸出至一顯示器之一圖框緩衝器中之影像之產生之一電路。TLB 120為記憶體管理硬體可使用其來改良虛擬位址轉譯速度之一快取區。TLB 120可為一內容可定址記憶體，其中搜尋索引鍵為一虛擬位址且搜尋結果為一實體位址。如關於圖3至圖5更詳細地描述，TLB 120可包含作業系統頁面表項目，該等作業系統頁面表項目將虛擬位址映射至實體位址且作業系統頁面表可儲存於記憶體(例如，記憶體陣列111)中。CPU快取區122可為相對較快速暫存器與相對較緩慢主記憶體之間之一中間階段(未具體繪示)。待由CPU 106運算之該資料可在被放置於一暫存器中之前複製至CPU快取區122，其中運算可受邏輯單元118影響。儘管未具體繪示，但CPU快取區122可為一多層級階層式快取區。

運算系統100可包含個別積體電路，或主機102及計算記憶體系統104兩者可在相同積體電路上。運算系統100可為(例如)一伺服器系統及/或一高效能運算系統及/或該高效能運算系統之一部分。儘管圖1中展示之實例

繪示具有一范紐曼(Von Neumann)架構之一系統，但本發明之實施例可在非范紐曼架構(例如，一杜林機(Turing machine))中實施，該等非范紐曼架構可不包含通常與一范紐曼架構相關聯之一或多個組件(例如，CPU、ALU等)。

為清楚起見，運算系統100已經簡化以集中在與本發明特定相關之特徵。記憶體陣列111可為一混合記憶體立方體(HMC)、計算記憶體，諸如一記憶體處理隨機存取記憶體體(processing in memory random access memory (PIMRAM))陣列，其可包含例如一DRAM陣列、SRAM陣列、STT RAM陣列、PCRAM陣列、TRAM陣列、RRAM陣列、NAND快閃陣列及/或NOR快閃陣列之一或多者。記憶體陣列111可包括配置成由存取線(其在本文中可稱為字線或選擇線)耦合之列及由感測線(其在本文中可稱為數位線或資料線)耦合之行的記憶體胞。儘管圖1中展示一單一計算記憶體裝置110，但實施例不受限於此。例如，計算記憶體系統104可包含若干計算記憶體裝置110 (例如，DRAM胞之若干記憶體庫)。

計算記憶體系統104可包含位址電路126，用以鎖存經由一輸入/輸出「I/O」匯流排138 (例如，資料匯流排及/或位址匯流排)透過I/O電路130提供之位址信號(例如，經由局域I/O線及全域I/O線提供至外部ALU電路及DRAM DQ)。可由一列解碼器128及一行解碼器134接收並解碼位址信號以存取計算記憶體裝置110。可藉由使用感測電路124感測感測線上之電壓及/或電流變化而自記憶體陣列111讀取資料。感測電路124可自記憶體陣列111讀取一頁(例如一列)資料且鎖存該頁資料。I/O電路130可用於經由I/O匯流排138與主機102雙向資料通信。寫入電路132可用於將資料寫入至計算記憶體裝置110。

控制器108可解碼由控制匯流排136自主機102提供之信號。此等信號可包含用於控制對計算記憶體裝置110執行之記憶體操作(包含資料讀取、資料寫入及資料抹除操作)之晶片啟用信號、寫入啟用信號及位址鎖存信號。信號亦可用於控制對計算記憶體裝置110執行之邏輯運算，包含算術、流程控制及組合運算以及其它。在各種實施例中，控制器108負責執行來自主機102之指令。控制器108可為一狀態機、一定序器、一處理器及/或其它控制電路。

在一些先前方法中，與(例如)一邏輯運算相關聯之資料將經由感測電路而自記憶體讀取且經由I/O線(例如，經由局域I/O線及/或全域I/O線)而提供至外部ALU電路。外部ALU電路可包含若干暫存器且將使用該資料(其可稱為運算元或輸入)執行邏輯運算，且結果將經由I/O線傳送回至陣列。相比之下，在本發明之若干實施例中，感測電路124經組態以對儲存於記憶體陣列111中之資料執行邏輯運算且將結果儲存回至記憶體陣列111，而不啟用耦合至感測電路124之一I/O線(例如，一局域I/O線)。啟用一I/O線可包含：啟用(例如，接通)具有耦合至一解碼信號(例如，一行解碼信號)之一閘極及耦合至該I/O線之一源極/汲極的一電晶體。然而，實施例不限於不啟用一I/O線。例如，在若干實施例中，感測電路124可用於執行邏輯運算而不啟用陣列之行解碼線；然而，除傳送回至陣列111之外，可啟用(若干)局域I/O線以將一結果傳送至一適合位置(例如，至一外部暫存器)。

因而，在若干實施例中，無需陣列111及感測電路124外部之電路來執行邏輯運算，此係因為感測電路124可操作以使用記憶體陣列111之位址空間來執行邏輯運算，而不使用一外部處理資源。因此，感測電路124

可用於至少在某種程度上補充及/或取代此一外部處理資源(或至少此一外部處理資源之頻寬消耗)。

感測電路124可形成於與陣列之記憶體胞之間距上。儘管未具體繪示，但在一些實施例中額外周邊感測放大器及/或邏輯(例如，各自儲存用於一邏輯功能之執行之指令之功能組件)可耦合至感測電路124。感測電路124及周邊感測放大器及邏輯可根據本文中所述之實施例協作執行邏輯運算。

然而，在若干實施例中，感測電路124除可用於執行由一外部處理資源(例如，主機102)執行之邏輯運算之外，亦可用於執行其它邏輯運算(例如，執行指令)。例如，主機102及/或感測電路124可受限於僅執行特定邏輯運算及/或特定數目個邏輯運算。

下文結合圖2進一步描述感測電路124之一實例。例如，在若干實施例中，感測電路124可包括若干感測放大器及若干計算組件，其等可包括用作一累加器之一鎖存器且可用於(例如，對與互補感測線相關聯之資料)執行邏輯運算。邏輯運算可包含布林運算(Boolean operation) (例如，「AND」、「OR」、「NOR」、「XOR」等)、用以執行其它數學運算之布林運算之組合以及非布林運算。在若干實施例中，感測電路124可用於使用儲存於記憶體陣列111中之資料作為輸入而執行邏輯運算，且將邏輯運算之結果儲存回至記憶體陣列111而不經由一感測線位址存取傳送(例如，不觸發一行解碼信號)。因而，取代藉由感測電路124外部之處理資源(例如，藉由主機CPU 106及/或位於計算記憶體系統104上(諸如控制器108上)或別處之其它處理電路(諸如，ALU電路)而執行一邏輯運算及/或除其之外，可使用感測電路124來執行一邏輯運算。

圖2為根據本發明之若干實施例之一計算記憶體裝置210之一部分之一示意圖。計算記憶體裝置210類似於圖1中繪示之計算記憶體裝置110。計算記憶體裝置210可包含一記憶體陣列211，該記憶體陣列211包含耦合至諸列存取線242-1、242-2、242-3、242-4、242-5、242-6、242-7、…、242-M及諸行感測線244-1、244-2、244-3、244-4、244-5、244-6、244-7、244-8、…、244-N之記憶體胞240-1、240-2、240-3、240-4、240-5、240-6、240-7、240-8、…、240-N。記憶體陣列211不受限於特定數目個存取線及/或感測線，且術語「列」及「行」之使用不意指存取線及/或感測線之一特定實體結構及/或定向。雖未圖示，但記憶體胞之各行可與一對對應的互補感測線相關聯。

記憶體胞之各行可耦合至可類似於圖1中繪示之感測電路124之感測電路224。在此實例中，感測電路包含耦合至各自感測線244之若干感測放大器246-1、246-2、246-3、246-4、246-5、246-6、246-7、246-8、…、246-N。感測放大器246經由存取裝置(例如，電晶體)250-1、250-2、250-3、250-4、250-5、250-6、250-7、250-8、…、250-N耦合至輸入/輸出(I/O)線254 (例如，一局域I/O線)。在此實例中，感測電路亦包含耦合至各自感測線244之若干計算組件248-1、248-2、248-3、248-4、248-5、248-6、248-7、248-8、…、248-N。行解碼線252-1、252-2、252-3、252-4、252-5、252-6、252-7、252-8、…、252-N分別耦合至存取裝置250之閘極，且可經選擇性地啟動以將由各自感測放大器246感測及/或儲存於各自計算組件248中之資料傳送至一次級感測放大器256。在若干實施例中，計算組件248可形成於與其等對應行之記憶體胞及/或與對應感測放大器246之間距上。

在若干實施例中，感測電路(例如，計算組件248及感測放大器246)經組態以對儲存於記憶體陣列211中之元素執行若干邏輯運算。作為一實例，可將第一複數個元素儲存於耦合至一特定存取線(例如，存取線242-1)及若干感測線244之一第一群組之記憶體胞中，且可將第二複數個元素儲存於耦合至一不同存取線(例如，存取線242-2)及各自若干感測線244之一第二群組之記憶體胞中。可用該第二複數個元素之一各自者對該第一複數個元素之各元素執行一邏輯運算，且可將邏輯運算之結果(例如，作為一位元向量)儲存於耦合至一特定存取線(例如，存取線242-3)及若干感測線244之一第三群組之記憶體胞中。

圖3為繪示根據本發明之若干實施例之一讀取或寫入存取之一方塊流程圖。圖3至圖6繪示表示類似架構之操作之不同流程圖。圖3包含類似於關於圖1描述之大容量儲存器114之一大容量儲存裝置314之一圖解。關於圖4更詳細地描述大容量儲存裝置314之功能。圖3包含類似於圖1中繪示之CPU 106之一CPU 306。將CPU 306繪示為包含一邏輯單元318、TLB 320及CPU快取區322。圖3包含一計算記憶體系統304，該計算記憶體系統304包含I/O電路330、記憶體陣列311及計算記憶體系統快取區312。關於圖5至圖6更詳細地描述計算記憶體系統快取區312。記憶體系統304類似於圖1中繪示之記憶體系統104。將記憶體系統304繪示為包含一作業系統頁面表316。儘管作業系統頁面表316可儲存於記憶體陣列311中，但為了易於圖解及解釋而單獨繪示作業系統頁面表316。同樣地，計算記憶體程式342可儲存於記憶體陣列311中，但單獨繪示以突顯關於圖3至圖6描述之功能流程。記憶體系統304可包含如在下文更詳細地描述之一熵源340。

本發明之一些實施例可使CPU 306及底層架構保持與CPU之習知情況不變。然而，計算記憶體系統304可不同地操作，及/或一主機之一作業系統可與習知情況不同地操作。習知地，作業系統可維持一作業系統頁面表，然而根據本發明，計算記憶體系統304可維持一作業系統頁面表316，此係因為計算記憶體系統304可加密及/或解密儲存於記憶體中之頁面，且在作業系統頁面表中指示該頁面且可針對已加密頁面產生密鑰並將密鑰儲存於作業系統頁面表中。計算記憶體系統304可針對一已加密頁面產生一新密鑰且即時重新加密該頁面。主機CPU 306可包含其記憶體階層中之一TLB 320，但作業系統頁面表316儲存於記憶體陣列311中。一旦一頁面缺失(例如，當將可執行指令加載至記憶體陣列311時)，可需要將頁面自大容量儲存器314加載且加載並放置於實體及虛擬記憶體之保留區域中。保留可由作業系統管理且維持於作業系統頁面表316中。作業系統頁面表316可定位於記憶體陣列311之一保留區域中。例如，在一ARM架構中，ARM記憶體管理單元(MMU)可使用暫存器TTB0及TTB1指向作業系統頁面表以允許一頁面錯失情況下之表之硬體查詢(walking)。

由於作業系統頁面表316定位於記憶體陣列311中，故計算記憶體系統304具有對作業系統頁面表316結構之程式化存取，意指計算記憶體系統304可對作業系統頁面表316作出改變。作業系統頁面表316可包含指示關於由作業系統頁面表316指涉之頁面之資訊之若干欄位。此等欄位可包含一加密指示欄位346，一密鑰欄位348、一虛擬位址欄位350、一實體位址欄位352、一頁面類型欄位354及/或一大小欄位356。加密指示欄位346可指示對應頁面是否已加密(例如，藉由針對是之一位元值1，或針對否之一位元值0)。若對應頁面已加密，則密鑰欄位348可儲存對應頁面之一密

鑰。若對應頁面未加密，則可能不針對對應頁面，將一密鑰儲存於密鑰欄位348中，此係因為其將為不必要的。虛擬位址欄位350可儲存對應於頁面之一虛擬位址。實體位址欄位352可儲存對應於頁面之一實體位址。頁面類型欄位354可標記對應頁面之類型(例如，讀取「R」、寫入「W」、讀取/寫入「R/W」或可執行「X」)。頁面之類型指示頁面是否儲存資料或可執行指令以及其它。大小欄位356可指示對應頁面之一大小(例如，4k)。表1中展示一表之一實例。

表1：

加密	密鑰	虛擬	實體	類型	頁面大小
1	0xA8F01...	0x80010000	0x01000000	X	4k
0	NA	0x40A00000	0x01100000	R	1MB
1	0xBB16B...	0x80080000	0x01080000	X	4k
0	NA	0x60A08000	0x00001000	R/W	4k

在一些實施例中，可不快取作業系統頁面表316以便保存作業系統頁面表316、CPU 306及記憶體陣列311中之資訊之間之相干性。計算記憶體系統304可經組態(例如，經程式化)以周遊記憶體陣列311中之作業系統頁面表316例如以尋找標記為可執行指令之一頁面。例如，計算記憶體系統304可包含可處置周遊作業系統頁面表316之一計算記憶體程式342。作業系統頁面表316中指涉之頁面可儲存資料或可執行指令。因此，可藉由頁面類型欄位354中之一標記而將作業系統頁面表316中指涉之一頁面標記為可執行指令。頁面類型讀取、寫入及讀取/寫入可標記資料頁面(儲存資料之一頁面)且頁面類型可執行指令可標記可執行指令之一頁面(儲存可執行指令之一頁面)。

計算記憶體系統304可經組態以加密及/或解密可執行指令。例如，計算記憶體系統304可包含可處置可執行指令之加密及/或解密之一計算記

憶體程式342。在一些實施例中，計算記憶體程式342可於可執行指令在一頁面錯失期間填充於計算記憶體系統304中時，及/或(例如，在自CPU 306進行一快取線再填充期間)自計算記憶體系統304讀取可執行指令時處置可執行指令之加密及/或解密。一頁面是否加密之一指示可儲存於加密指示欄位346中。在一些實施例中，主機作業系統可如I/O電路330與計算記憶體程式342之間之線所指示而(例如，在起動時)啟動計算記憶體系統304中之計算記憶體程式342。在計算記憶體程式342運行之後，主機作業系統之責任可關於加密而結束。

計算記憶體系統304可包含一熵源340，該熵源340可產生一密鑰及/或用於針對標記為可執行指令之一頁面產生一密鑰以用該密鑰加密該頁面。可基於由熵源340產生之一隨機數字或接近隨機數字產生密鑰。熵源340之一實例為一鎖相迴路(PLL)頻率(例如，一PLL時脈)，其可經取樣以產生將用作一密鑰之數字。熵源340之一實例為與計算記憶體系統304相關聯之一序號，該序號可經取樣以產生將用作一密鑰及/或用作至產生另一值之一演算法之輸入之一數字，該另一值可經取樣(或使用)以產生將用作一密鑰之一數字。熵源340之一實例為一計時器，其可經取樣以產生將用作一密鑰之一數字。在一些實施例中，一密鑰可由一經取樣PLL頻率，互斥或(XOR)由一經取樣序號，XOR由一經取樣計時器產生。計算記憶體系統304可經組態以使用由熵源340產生之唯一密鑰加密或重新加密記憶體陣列311中之頁面。其它熵源及/或熵源之組合可用於產生一隨機或接近隨機數字。

如上文所述，根據本發明，針對資料讀取或寫入操作，加密並非必要的。計算記憶體程式442可授予存取作業系統頁面表316中之一資料頁

面(標記為讀取、寫入及/或讀取/寫入之一頁面)，而無關於加密。因此，一資料頁面358可透過記憶體陣列311與CPU 306之間之I/O電路330傳送(例如，經由CPU快取區322)且儲存於記憶體陣列311中或自記憶體陣列311讀取。例如，在一讀取/寫入操作中，來自TLB 320之一虛擬記憶體位址(例如，「A」)可來往於計算記憶體系統304傳輸且擷取自及/或儲存於對應於寫入之資料頁面358之第一表項目344之虛擬位址欄位350。對應於虛擬位址之一實體位址(例如，「B」)可擷取自及/或儲存於第一表項目344之實體位址欄位352中。此由延伸於第一表項目344與TLB 320之間之線指示。因為傳送的係一資料頁面358，而非可執行指令，故計算記憶體程式342可如計算記憶體程式342與第一表項目344之間之線所指示而在第一表項目344之加密指示欄位346中將頁面標記為未加密(例如，「0」)。計算記憶體程式可不將一密鑰儲存於第一表項目344之密鑰欄位348中(例如，「N/A」)，此係因為其對應於未加密之一資料頁面358。計算記憶體程式342可將資料頁面358係讀取/寫入之一指示(例如，「R/W」)儲存於頁面類型欄位354中且將頁面大小之一指示(例如，「4k」)儲存於大小欄位356中。在圖4至6中，第一表項目分別標示為444、544及644。

圖4為繪示根據本發明之若干實施例之一新頁面分配之一方塊流程圖。圖4包含一大容量儲存裝置414之一圖解，該大容量儲存裝置414包含可執行指令461。圖4包含一CPU 406，該CPU 406包含一邏輯單元418、TLB 420及CPU快取區422。圖4包含一計算記憶體系統404，該計算記憶體系統404包含I/O電路430、記憶體陣列411、計算記憶體系統快取區412、作業系統頁面表416、計算記憶體程式442及熵源440。

大容量儲存器414可儲存用於CPU 406之可執行指令461。可如從大

容量儲存裝置414穿過I/O電路430至記憶體陣列411之箭頭所指示，藉由自大容量儲存裝置414之直接記憶體存取(DMA)而將可執行指令461加載至記憶體陣列411中。最初，將來自大容量儲存裝置414之可執行指令461作為一純文字可執行指令頁面462儲存於記憶體陣列411中，此係因為其等未在大容量儲存裝置414中加密。計算記憶體程式442可在作業系統頁面表416中產生一第二表項目460以對應於記憶體陣列411中之純文字可執行指令頁面462。

因為純文字可執行指令頁面462尚未加密，故計算記憶體程式442可在第二表項目460之加密指示欄位446中將純文字可執行指令頁面462標記為未加密(例如，「0」)。同樣地，不在第二表項目460之密鑰欄位448中儲存一密鑰(例如，「—」)。可將來自TLB 420之一虛擬記憶體位址(例如，「C」)傳輸至計算記憶體系統404且儲存於第二表項目460之虛擬位址欄位450中。可將對應於虛擬位址之一實體位址(例如，「D」)儲存於第二表項目460之實體位址欄位452中。此由延伸於第二表項目460與TLB 420之間之線指示。如計算記憶體程式442與第二表項目460之間之線所指示，計算記憶體程式可在第二表項目460之類型欄位454中將純文字可執行指令頁面462標記為可執行指令(例如，「X」)。未加密之純文字可執行指令頁面462與此指示之間之對應性由記憶體陣列411與第二表項目460之間之線繪示。計算記憶體程式442可將頁面大小之一指示(例如，「4k」)儲存於大小欄位456中。

圖5為繪示根據本發明之若干實施例之可執行指令之加密之一方塊流程圖。圖5包含一大容量儲存裝置514之一圖解。圖5包含一CPU 506，該CPU 506包含一邏輯單元518、TLB 520及CPU快取區522。圖5包含一計

算記憶體系統504，該計算記憶體系統504包含I/O電路530、記憶體陣列511、計算記憶體系統快取區512、作業系統頁面表516、計算記憶體程式542及熵源540。

在圖4中，最初將來自大容量儲存裝置414之可執行指令461作為一純文字可執行指令462儲存於記憶體陣列411中。然而在圖5中，計算記憶體程式542可使用熵源540產生純文字可執行指令462之一密鑰且將純文字可執行指令462加密成一密文可執行指令564，且將密文可執行指令564儲存回至記憶體陣列511。加密之一些實例包含高級加密標準(AES)(諸如AES 128位元加密、AES 256位元加密等)及資料加密標準(DES)以及其它。計算記憶體程式542可刪除純文字可執行指令462之第二表項目460且產生密文可執行指令564之一第三表項目563。

計算記憶體程式542可在第三表項目563之加密指示欄位546中將密文可執行指令頁面564標記為已加密(例如，「1」)。此由計算記憶體程式542與第三表項目563之間之線指示。產生用以加密頁面之密鑰可儲存於第三表項目563之密鑰欄位548中(例如，「XYZ」)。此由從熵源540穿過計算記憶體程式542至第三表項目563中之密鑰欄位548之線指示。第三表項目563之虛擬位址欄位550中之虛擬記憶體位址(例如，「C」)、實體位址欄位552中之實體位址(例如，「D」)、類型欄位554中之類型(例如，「X」)及大小欄位556中之大小(例如，「4k」)可保持與第二表項目460的相同，然而，實施例不受限於此，此係因為例如，實體位址可改變。

計算記憶體程式542可在將純文字可執行指令462加密成密文可執行指令564之前複製純文字可執行指令462 (如圖4中繪示)且將其儲存為記憶體系統快取區512中之純文字可執行指令566。此由計算記憶體程式542、

密文可執行指令564與純文字可執行指令566之間之線指示。計算記憶體系統快取區512可為(例如，計算記憶體系統504及/或記憶體陣列511之)計算記憶體之一非可定址(例如，安全)區域。非可(例如，由一主機或DMA裝置等)定址之計算記憶體系統快取區512可使純文字可執行指令566安全，此係因為一外部裝置(諸如一主機或DMA裝置)無法注入惡意軟體。計算記憶體系統快取區512中之純文字可執行指令566可用於滿足來自主機之額外指令請求且隱藏可由計算記憶體程式542之操作導致之一些延時。此由從純文字可執行指令566至CPU 506之線繪示。

計算記憶體程式542可周遊作業系統頁面表516 (例如，任何主機操作以外及/或在計算記憶體系統504及/或作業系統頁面表516之閒置時間期間)來查找標記為可執行指令之頁面。在一些實施例中，計算記憶體程式542可回應於自與(例如，針對一經請求頁面之)一頁面存取相關聯之一主機接收一指令而周遊作業系統頁面表516。回應於尋找到標記為可執行指令之一頁面，計算記憶體程式542可判定標記為可執行指令之頁面是否已加密。可藉由參考指示頁面是否已加密(例如，藉由加密指示欄位546)且頁面是否可執行(例如，藉由類型欄位554)之作業系統頁面表516而判定經請求頁面是否已加密。回應於判定標記為可執行指令之頁面未加密，計算記憶體程式542可針對標記為可執行指令之頁面產生一密鑰且使用該密鑰加密該頁面。可取代未加密頁面(取代其中加密操作係回應於來自一主機之一請求之經請求頁面)儲存已加密頁面。尋找到未加密之標記為可執行指令之一頁面可暗指在某一時刻計算記憶體系統504遭遇一頁面錯失及需要將一頁面加載至記憶體陣列511中。有利地，計算記憶體程式542可藉由用一唯一產生的密鑰加密頁面而補救此，使得對注入攻擊更有彈性。

回應於判定標記為可執行指令之頁面已加密，計算記憶體程式542可繼續周遊作業系統頁面表516以尋找標記為可執行指令之一額外頁面。回應於尋找到標記為可執行指令之一額外頁面，計算記憶體程式542可判定標記為可執行指令之額外頁面是否已加密。若標記為可執行指令之額外頁面尚未加密，則計算記憶體程式542可產生一不同的密鑰且使用該不同的密鑰加密標記為可執行指令之該額外頁面。計算記憶體程式542可繼續周遊作業系統頁面表516以尋找標記為可執行指令之任何頁面且加密未加密之該等可執行指令。可用一唯一的密鑰加密已加密之作業系統記憶體表516中指涉之各加密頁面，使得作業系統頁面表516之密鑰欄位548中之各密鑰係唯一的(沒有兩個密鑰係相同的)。

在一些實施例中，回應於判定標記為可執行指令之頁面已加密，計算記憶體程式542可產生一新密鑰，使用新密鑰重新加密經請求頁面，且取代經請求頁面，將重新加密之頁面儲存於記憶體陣列511中。可用新密鑰更新經請求頁面之密鑰欄位548。重新加密之頁面可經解密(使用密鑰)且作為純文字儲存於記憶體系統快取區512中。

圖6為繪示根據本發明之若干實施例之對一已加密可執行指令之一隨後存取之一方塊流程圖。圖6包含一大容量儲存裝置614之一圖解。圖6包含一CPU 606，該CPU 606包含一邏輯單元618、TLB 620及CPU快取區622。圖6包含一計算記憶體系統604，該計算記憶體系統604包含I/O電路630、記憶體陣列611、計算記憶體系統快取區612、作業系統頁面表616、計算記憶體程式642及熵源640。

記憶體陣列611被繪示為具有對應於圖5中繪示之密文可執行指令564之密文可執行指令664。回應於對標記為可執行指令之頁面(例如，密文頁

面664)之一請求，計算記憶體程式642可(用熵源640)產生一新密鑰、使用新密鑰重新加密標記為可執行指令之頁面且儲存經重新加密之可執行指令之頁面而取代標記為可執行指令之頁面。此由計算記憶體程式642與密文可執行指令664及密文可執行指令668之間之線繪示，密文可執行指令668表示標記為可執行指令之重新加密頁面。密文可執行指令664之x-out表示取代它而儲存之密文可執行指令668。計算記憶體程式642可刪除密文可執行指令564之第三表項目563且產生密文可執行指令668之一第四表項目665。

計算記憶體程式642可在第四表項目665之加密指示欄位646中將密文可執行指令頁面668標記為已加密(例如，「1」)。產生用以加密頁面之新密鑰可儲存於第四表項目665之密鑰欄位648中(例如，「PQR」)。此由從熵源640穿過計算記憶體程式642至第四表項目665中之密鑰欄位648之線指示。第四表項目665之虛擬位址欄位650中之虛擬記憶體位址(例如，「C」)、實體位址欄位652中之實體位址(例如，「D」)、類型欄位654中之類型(例如，「X」)及大小欄位656中之大小(例如，「4k」)可保持與第三表項目563的相同，然而，實施例不受限於此，此係因為例如實體位址可改變。

儘管未在圖6中具體繪示，但可(例如，自一主機或DMA裝置)接收可執行指令之一新頁面且計算記憶體程式642可針對新頁面(用熵源640)產生一新密鑰。新頁面可由新密鑰加密且儲存於記憶體陣列611中。計算記憶體程式642可針對新頁面而在作業系統頁面表616中產生一新項目，包含將新頁面標記為可執行指令及已加密。

在一些實施例中，計算記憶體程式642可解密已重新加密之頁面(例

如，密文可執行指令668)且將已解密之頁面(例如，作為純文字可執行指令670)儲存於計算記憶體系統快取區612中以供傳送(例如，至一主機或DMA裝置)以滿足(對一請求來源之)一請求。此由計算記憶體程式642、純文字可執行指令670及密文可執行指令668之間之線，以及純文字可執行指令670與CPU 606之間之線繪示。在一些實施例中，已解密可執行指令或未加密可執行指令透過I/O電路630自計算記憶體系統快取區612而非自記憶體陣列611傳送至一請求裝置以防止將任何已注入的程式碼隨可執行指令一起發送，此係因為無用於將程式碼注入至計算記憶體系統快取區612之機構。即使記憶體陣列611中之密文可執行指令注入有惡意程式碼，可執行指令之解密將使注入之程式碼無意義，此係因為其將非以使用用於加密可執行指令之相同密鑰之一加密形式注入。因此，解密程序將洩露惡意程式碼。具有洩露的惡意程式碼之可執行指令無法用於其預期目的(其可產生一錯誤)，而惡意程式碼將不執行(例如，其可導致一停止、預取中止或使管線急劇斷路)，而病毒不會擴散。

儘管未具體繪示成此，但用於儲存可執行指令之一非暫態計算裝置可讀媒體可包含全部形式的揮發性及非揮發性記憶體，包含(藉由實例方式)半導體記憶體裝置、DRAM、PIM、HMC、EPROM、EEPROM、快閃記憶體裝置、磁碟(諸如，固定磁碟、軟碟及可抽換式磁碟)、其它磁性媒體(包含磁帶)、光學媒體(諸如，光碟(CD)、數位多功能光碟(DVD)及藍光光碟(BD))。指令可由ASIC補充或併入至ASIC中。例如，圖1中繪示之大容量儲存器114、CPU快取區122及/或記憶體陣列111之任何一或多者可為一非暫態計算裝置可讀媒體。

儘管已在本文中圖解及描述特定實施例，但一般技術者將瞭解，經

計算以達成相同結果之一配置可取代展示之特定實施例。本發明意欲涵蓋本發明之一或多個實施例之調適或變動。應瞭解，已依一繪示性方式且非一限制性方式進行以上描述。熟習此項技術者在檢視上述描述時將明白上述實施例與未在本文中具體描述之其它實施例之組合。本發明之一或多個實施例之範疇包含其中使用上文結構及方法之其它應用。因此，應參考隨附申請專利範圍連同此等申請專利範圍所授權之等效物之全部範圍而判定本發明之一或多個實施例之範疇。

在前述實施方式中，為簡化本發明之目的將一些特徵一起集合於一單一實施例中。本發明之此方法不應解釋為反映以下意圖：本發明之所揭示實施例必須使用多於各請求項中所明確陳述之特徵。實情係，如以下申請專利範圍反映，發明標的物可能少於一單一所揭示實施例之全部特徵。因此，以下申請專利範圍以此方式併入實施方式中，其中各請求項單獨作為一獨立實施例。

【符號說明】

100	運算系統
102	主機
104	計算記憶體系統
106	中央處理單元(CPU)
108	控制器
110	計算記憶體裝置
111	記憶體陣列
114	大容量儲存器
118	邏輯單元

120	轉譯後備緩衝器(TLB)
122	CPU快取區
124	感測電路
126	位址電路
128	列解碼器
130	I/O電路
132	寫入電路
134	行解碼器
136	控制匯流排
138	I/O匯流排
210	計算記憶體裝置
211	記憶體陣列
224	感測電路
240-1至240-N	記憶體胞
242-1至242-M	存取線
244-1至244-N	感測線
246-1至246-N	感測放大器
248-1至248-N	計算組件
250-1至250-N	存取裝置
252-1至252-N	行解碼線
254	輸入/輸出線
256	次級感測放大器
304	計算記憶體系統

306	中央處理單元(CPU)
311	記憶體陣列
312	計算記憶體系統快取區
314	大容量儲存裝置
316	作業系統頁面表
318	邏輯單元
320	轉譯後備緩衝器(TLB)
322	CPU快取區
330	I/O電路
340	熵源
342	計算記憶體程式
344	第一表項目
346	加密指示欄位
348	密鑰欄位
350	虛擬位址欄位
352	實體位址欄位
354	頁面類型欄位
356	大小欄位
358	資料頁面
404	計算記憶體系統
406	中央處理單元(CPU)
411	記憶體陣列
412	計算記憶體系統快取區

414	大容量儲存裝置
416	作業系統頁面表
418	邏輯單元
420	轉譯後備緩衝器(TLB)
422	CPU快取區
430	I/O電路
440	熵源
442	計算記憶體程式
444	第一表項目
446	加密指示欄位
448	密鑰欄位
450	虛擬位址欄位
452	實體位址欄位
454	類型欄位
456	大小欄位
460	第二表項目
461	可執行指令
462	純文字可執行指令
504	計算記憶體系統
506	中央處理單元(CPU)
511	記憶體陣列
512	計算記憶體系統快取區
514	大容量儲存裝置

516	作業系統頁面表
518	邏輯單元
520	轉譯後備緩衝器(TLB)
522	CPU快取區
530	I/O電路
540	熵源
542	計算記憶體程式
544	第一表項目
546	加密指示欄位
548	密鑰欄位
550	虛擬位址欄位
552	實體位址欄位
554	類型欄位
556	大小欄位
563	第三表項目
564	密文可執行指令
566	純文字可執行指令
604	計算記憶體系統
606	中央處理單元(CPU)
611	記憶體陣列
612	計算記憶體系統快取區
614	大容量儲存裝置
616	作業系統頁面表

618	邏輯單元
620	轉譯後備緩衝器(TLB)
622	CPU快取區
630	I/O電路
640	熵源
642	計算記憶體程式
644	第一表項目
646	加密指示欄位
648	密鑰欄位
650	虛擬位址欄位
652	實體位址欄位
654	類型欄位
656	大小欄位
664	密文可執行指令
665	第四表項目
668	密文可執行指令
670	純文字可執行指令

專利案號：105125524

公告本 106年10月17日 修正

申請日： 105/08/10

IPC分類： G06F 21/71 (2013.01)
G11C 7/24 (2006.01)

I631482

【發明摘要】

【中文發明名稱】

計算記憶體中可執行指令之加密之方法及設備

【英文發明名稱】

METHOD AND APPARATUS OF ENCRYPTION OF EXECUTABLES IN COMPUTATIONAL MEMORY

【中文】

本發明係關於計算記憶體中之可執行指令之加密。計算記憶體可周遊該計算記憶體體中之一作業系統頁面表以尋找標記為可執行指令之一頁面。回應於尋找到標記為可執行指令之一頁面，該計算記憶體可判定標記為可執行指令之該頁面是否已加密。回應於判定標記為可執行指令之該頁面未加密，該計算記憶體可針對標記為可執行指令之該頁面產生一密鑰。該計算記憶體可使用該密鑰加密標記為可執行指令之該頁面。

【英文】

The present disclosure is related to encryption of executables in computational memory. Computational memory can traverse an operating system page table in the computational memory for a page marked as executable. In response to finding a page marked as executable, the computational memory can determine whether the page marked as executable has been encrypted. In response to determining that the page marked as executable is not encrypted, the computational memory can generate a key for the page marked as executable. The computational memory can encrypt the page marked as executable using

the key.

【指定代表圖】

圖5

【代表圖之符號簡單說明】

504	計算記憶體系統
506	中央處理單元
511	記憶體陣列
512	計算記憶體系統快取區
514	大容量儲存裝置
516	作業系統頁面表
518	邏輯單元
520	轉譯後備緩衝器
522	CPU快取區
530	I/O電路
540	熵源
542	計算記憶體程式
546	加密指示欄位
548	密鑰欄位
550	虛擬位址欄位
552	實體位址欄位
554	類型欄位
556	大小欄位
563	第三表項目

【發明申請專利範圍】

【第1項】

一種計算記憶體中可執行指令之加密之方法，其包括：

藉由計算記憶體周遊該計算記憶體中之一作業系統頁面表以尋找儲存於該計算記憶體中且標記為可執行指令之任一頁面；

回應於尋找到標記為可執行指令之一頁面，判定標記為可執行指令之該頁面是否已加密；

回應於判定標記為可執行指令之該頁面未加密，針對標記為可執行指令之該頁面產生一密鑰；

使用該密鑰加密標記為可執行指令之該頁面；

回應於判定標記為可執行指令之該頁面已加密，周遊該作業系統頁面表以尋找標記為可執行指令之一額外頁面；

回應於尋找到標記為可執行指令之該額外頁面，判定標記為可執行指令之該額外頁面是否已加密；

回應於判定標記為可執行指令之該額外頁面未加密，針對標記為可執行指令之該額外頁面產生一不同的密鑰；及

使用該不同的密鑰加密標記為可執行指令之該額外頁面。

【第2項】

如請求項1之方法，其中周遊該作業系統頁面表包括：回應於自與一頁面存取相關聯之一主機接收一指令而周遊該作業系統頁面表。

【第3項】

如請求項1之方法，其中該方法包含，回應於對標記為可執行指令之該頁面之一請求而：

產生一新密鑰；及

使用該新密鑰重新加密標記為可執行指令之該頁面；及

儲存該重新加密之頁面以取代標記為可執行指令之該頁面。

【第4項】

如請求項3之方法，其中該方法包含，回應於對標記為可執行指令之該頁面之該請求：

解密該重新加密之頁面；及

將該已解密頁面儲存於該計算記憶體之快取區中以供傳送以滿足該請求。

【第5項】

如請求項1之方法，其中該方法包含：

接收一新頁面，該新頁面包括可執行指令；

針對該新頁面產生一新密鑰；

使用該新密鑰加密該新頁面；

將該新頁面儲存於該計算記憶體中；及

針對該新頁面在該作業系統頁面表中產生一項目，包含將該新頁面標記為可執行指令及已加密。

【第6項】

一種計算記憶體中可執行指令之加密之方法，其包括：

經由一計算記憶體之感測電路對儲存於該計算記憶體之記憶體胞中之資料執行一邏輯運算且將該結果儲存回至該計算記憶體，而不啟用耦合至該感測電路之一局域輸入/輸出線；

儲存一作業系統頁面表於該計算記憶體中其中該作業系統頁面表

包含：

一各自頁面是否已加密之一指示；

用於已加密之各頁面之一各自密鑰；

對應於該各自頁面之一虛擬位址；

對應於該各自頁面之一實體位址；及

該各自頁面之一類型之一標記；及

藉由該計算記憶體維持該作業系統頁面表。

【第7項】

如請求項6之方法，其中該方法包含：

周遊該作業系統頁面表以尋找標記為可執行指令且未指示為已加密之頁面；及

使用唯一產生的密鑰加密標記為可執行指令且未指示為已加密之該等頁面。

【第8項】

如請求項7之方法，其中該各自頁面之該類型之該標記包括包含可讀取、可寫入、可讀取/可寫入及可執行指令之類型群組之一者；及

其中該各自頁面之該類型指示該各自頁面是否儲存資料或可執行指令。

【第9項】

一種非暫態電腦可讀媒體，其儲存可由計算記憶體執行之指令以：

周遊該計算記憶體中之一作業系統頁面表以尋找儲存於該計算記憶體中且標記為可執行指令之任一頁面；

回應於尋找到標記為可執行指令之一頁面，判定標記為可執行指

令之該頁面是否已加密；

回應於判定標記為可執行指令之該頁面未加密，針對標記為可執行指令之該頁面產生一密鑰；

使用該密鑰加密標記為可執行指令之該頁面；

回應於判定標記為可執行指令之該頁面已加密，周遊該作業系統頁面表以尋找標記為可執行指令之一額外頁面；

回應於尋找到標記為可執行指令之該額外頁面，判定標記為可執行指令之該額外頁面是否已加密；

回應於判定標記為可執行指令之該額外頁面未加密，針對標記為可執行指令之該額外頁面產生一不同的密鑰；及

使用該不同的密鑰加密標記為可執行指令之該額外頁面。

【第10項】

如請求項9之媒體，其進一步包含授予存取該作業系統頁面表中標記為讀取、寫入或讀取/寫入之一頁面而無關於加密之指令。

【第11項】

如請求項9之媒體，其進一步包含回應於標記為可執行指令之該頁面之一請求之指令以：

產生一新密鑰；及

使用該新密鑰重新加密標記為可執行指令之該頁面；及

儲存該重新加密之頁面以取代標記為可執行指令之該頁面。

【第12項】

一種用於計算記憶體中可執行指令之加密之設備，其包括：

一計算記憶體，其中該計算記憶體包含感測電路，其經組態以對

儲存於該計算記憶體之記憶體胞中之資料執行一邏輯運算且將該結果儲存回至該計算記憶體，而不啟用耦合至該感測電路之一局域輸入/輸出線；及

一作業系統頁面表，其儲存於該計算記憶體中，其中該作業系統頁面表包含：

一各自頁面是否已加密之一指示；

用於已加密之各頁面之一各自密鑰；

對應於該各自頁面之一虛擬位址；

對應於該各自頁面之一實體位址；及

該各自頁面之一類型之一標記；及

其中該計算記憶體經組態以維持該作業系統頁面表。

【第13項】

如請求項12之設備，其中該設備包含經組態以產生該等各自密鑰之一熵源。

【第14項】

如請求項12之設備，其中該計算記憶體經組態以：

周遊該作業系統頁面表以尋找標記為可執行指令且未指示為已加密之頁面；及

使用唯一產生的密鑰加密標記為可執行指令且未指示為已加密之該等頁面。

【第15項】

如請求項14之設備，其中該各自頁面之該類型之該標記包括包含可讀取、可寫入、可讀取/可寫入及可執行指令之類型群組之一者；及

其中該各自頁面之該類型指示該各自頁面是否儲存資料或可執行指令。

【第16項】

一種用於計算記憶體中可執行指令之加密之設備，其包括：

一計算記憶體，其經組態以：

周遊該計算記憶體中之一作業系統頁面表以尋找儲存於該計算記憶體中且標記為可執行指令之任一頁面；

回應於尋找到標記為可執行指令之一頁面，判定標記為可執行指令之該頁面是否已加密；

回應於判定標記為可執行指令之該頁面未加密，針對標記為可執行指令之該頁面產生一密鑰；

使用該密鑰加密標記為可執行指令之該頁面；

回應於判定標記為可執行指令之該頁面已加密，周遊該作業系統頁面表以尋找標記為可執行指令之一額外頁面；

回應於尋找到標記為可執行指令之該額外頁面，判定標記為可執行指令之該額外頁面是否已加密；

回應於判定標記為可執行指令之該額外頁面未加密，針對標記為可執行指令之該額外頁面產生一不同的密鑰；及

使用該不同的密鑰加密標記為可執行指令之該額外頁面。

【第17項】

如請求項16之設備，其中該計算記憶體經組態以回應於自與一頁面存取相關聯之一主機接收一指令而周遊該作業系統頁面表。

【第18項】

如請求項16之設備，其中該計算記憶體經組態以授予存取該作業系統頁面表中標記為讀取、寫入或讀取/寫入之一頁面而無關於加密。

【第19項】

如請求項16之設備，其中該計算記憶體經組態以回應於標記為可執行指令之該頁面之一請求以：

產生一新密鑰；及

使用該新密鑰重新加密標記為可執行指令之該頁面；及

儲存該重新加密之頁面以取代標記為可執行指令之該頁面

【第20項】

如請求項22之設備，其中該計算記憶體經組態以回應於標記為可執行指令之該頁面之該請求以：

解密該重新加密之頁面；及

將該經解密頁面儲存於該計算記憶體之該快取區中用於傳送以滿足該請求。

【第21項】

如請求項16之設備，其中該計算記憶體經組態以：

接收一新頁面，該新頁面包括可執行指令；

針對該新頁面產生一新密鑰；

使用該新密鑰加密該新頁面；

將該新頁面儲存於該計算記憶體中；及

針對該新頁面在該作業系統頁面表中產生一項目，包含將該新頁面標記為可執行指令及已加密。

the key.

【指定代表圖】

圖5

【代表圖之符號簡單說明】

504	計算記憶體系統
506	中央處理單元
511	記憶體陣列
512	計算記憶體系統快取區
514	大容量儲存裝置
516	作業系統頁面表
518	邏輯單元
520	轉譯後備緩衝器
522	CPU快取區
530	I/O電路
540	熵源
542	計算記憶體程式
546	加密指示欄位
548	密鑰欄位
550	虛擬位址欄位
552	實體位址欄位
554	類型欄位
556	大小欄位
563	第三表項目

564 密文可執行指令

566 純文字可執行指令