發明專利說明書200426582

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：92133335

※ 申請日期：92-11-27　　※IPC 分類：　60年11/16

壹、發明名稱：（中文/英文）

主動地偵測軟體竄改之系統與方法

A SYSTEM AND METHOD TO PROACTIVELY DETECT SOFTWARE TAMPERING

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商萬國商業機器公司

INTERNATIONAL BUSINESS MACHINES CORPORATION

代表人：（中文/英文）

傑拉德　羅森賽

ROSENTHAL, GERALD

住居所或營業所地址：（中文/英文）

美國紐約州阿蒙市新果園路

NEW ORCHARD ROAD, ARMONK, NY 10504, U.S.A.

國　籍：（中文/英文）

美國　　U.S.A.

參、發明人：(共 2 人)

姓　名：(中文/英文)

1.曾鴻霞

JIN, HONGXIA

2.傑佛瑞　布魯斯　羅斯皮奇

LOTSPIECH, JEFFREY BRUCE

住居所地址：(中文/英文)

1.美國加州古波帝諾市喬那森大道10600號

10600 JOHANSON DRIVE, CUPERTINO, CA 95014, U.S.A.

2.美國內華達州海德森市哈威克派斯大道2858號

2858 HARTWICK PINES DRIVE, HENDERSON, NEVADA 89052, U.S.A.

國　籍：(中文/英文)

1.中國　　PEOPLE'S REPUBLIC OF CHINA

2.美國　　U.S.A.

肆、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，其日期為： 年 月 日。

☑ **本案申請前已向下列國家（地區）申請專利：**

1.美國；2002年12月19日；10/248,130

2.

3.

4.

5.

☑ **主張國際優先權(專利法第二十四條)：**

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1.美國；2002年12月19日；10/248,130

2.

3.

4.

5.

☐ **主張國內優先權(專利法第二十五條之一)：**

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ **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】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明大致關於軟體安全的領域，更明確而言，本發明有關軟體竄改的偵測。

【先前技術】

隨著電影與音樂的數位技術的進步，未經認可複製的問題已變得較嚴格。數位副本是完美的複製，且可避免在網際網路廣泛重新分配，例如數位傳輸內容保護(DTCP)與可記錄媒體內容保護(CPRM)的許多內容保護技術已發展。這些技術在他們的許可具有"健全的術語"，其中在此許可中的術語能提供用於防止竄改的實施。特別是防止軟體竄改技術的防止竄改技術發展已變成一成長的工業。

在損害發生後，多數侵入偵測機構能使用，因此是敏感的。術語"主動安全"可視為在最後損害發生前，例如軟體執行的一處理期間發現的錯誤。先前技術系統不能提供一主動安全機構來反制軟體逆工程。這些先前技術系統在一逆工程嘗試期間不能識別電腦駭客留下的證據。需要的是在電腦駭客成功竄改及在他們獲得例如秘密鑰匙的重要資訊存取之前，能主動偵測(而且藉此當它仍然在它初期階段，透過阻止設法程式處理而避免實際損害的發生)一進行中的逆工程處理。

大體上，先前技術侵入偵測系統是敏感的，且使用既有知識來監視不正常。監視此不正常的方法是透過維持一"檢查記錄"。使用一檢查記錄的觀念已存在一段長時間。

然而，當它應用於一特殊"偵測"目的時，一"檢查記錄"方法能較佳工作且較實際。在此情況，一需要的是能識別需要放置在用於偵測目的記錄與應該遵從的確認處理的的資訊。在記錄中產生資訊能滿足某些屬性不僅能使方法更有效(從減少記錄大小與建立一更有效確認的觀點)，而且亦能保證確認處理及偵測目標異常。

另一相關的觀念是已在安全文獻中識別及出現的正式屬性的"前向安全"，前向安全包括在竄改發生後避免過去的碼或記錄破壞的方法。未來的動作可能是無法信賴，但是先前既有的信賴項目依然是不妥協。

下列參考文件是提供敏感侵入偵測機構的一般描述。

德雷克美國專利(6,006,328)揭示用於電腦軟體認證、保護、與安全的一方法。該方法包括使用直接與硬體溝通的等效程式碼(具移除易受影響)來取代易受影響的碼(例如，易受竊聽)，且它能使允許惡作劇軟體偷聽的系統中斷或其他功能失效。竄改發現技術能使用在軟體內，或由軟體存取，以便如果發現竄改，不允許ID資料隨後登入輸入常式。揭示的本發明提供：RAM或其他影像的碼核對加總執行；記憶體與可執行碼的其他儲存副本的比較及/或登錄處理的解密；可執行環境的檢查；執行大小與預期值的比較；一第三者或處理的認證失敗細節的通知及/或傳輸；及記錄有關(輸入常式或安全登錄處理)使用者的使用及/或細節的一記錄。

奧亞巴哈等人的美國專利(5,673,316)能提供米碼包封

的建立與分配。揭示的是具資訊部份集合的包封，其中每個部份係使用一部份加密鑰匙與一公眾鑰匙加密。清單然後使用一秘密鑰匙來簽署以產生一簽字，此簽字亦包含在包封內。

皮爾森的歐洲專利案號(EP1076279-A1)揭示使用與簽署版本與公眾鑰匙認證有關完整檢查的許可相關程式碼的一電腦平台。電腦平台或信賴模組能形成一防止竄改的元件，其中許可檢查能在使用者預期的信賴環境中發生。一相關的記錄處理單元機構允許資料的註冊與付款。系統亦允許一本地使用者或一遠端實體的一平台完整性確認。

艾倫等人的美國專利(4,757,533)係揭示將硬體與軟體組合以提供使用者與檔案存取防止竄改保護的一個人微電腦的安全系統。其中一揭示晶片能提供一檢查嘗試記錄、保護與加密系統旗號、與使用者存取權利，其中晶片能確保存取只由有效的使用者獲得。

外國專利案號WO200077597 A1、WO200114953 A1與WO200077596 B1通常揭示一防止竄改方法，其包括轉換在電腦軟體碼中的資料流，以從原始軟體碼意圖分離轉換碼的可識別操作。方法是提供能使電腦軟體防止竄改與逆工程。

史坦敦等人的外國專利(WO9904530 A1)係揭示使用當作一資料加密鑰匙使用以避免竄改的交談鑰匙之一檔案加密方法。此方法係使用根據一共用秘密鑰匙或公眾-私人鑰匙加密的一強加密演算法，以透過合法權限而允許緊

急存取檔案。

貝拉爾等人的非專利文獻名稱"Forward Integrity For Secure Audit Logs"係提供用以維持檢查記錄安全的一方法。揭示應用包括：侵入偵測或說明、通信安全、與認證行動代理計算部份結果的安全檢查記錄(例如，syslogd資料)。

桑格的非專利文獻名稱"Practical Forward Secure Group Signature Schemes"能提供一前向安全方法，以減輕由鑰匙暴露所引起的損害。

不論上述引用參考的好處、特徵、與優點，他們之中無一能達成或實施本發明目的。

【發明內容】

一方法揭示用於主動偵測軟體竄改，其中偵測是根據動態展開檢查記錄與密鑰值而動作。密鑰值是根據因先前記錄登錄與先前密鑰值而定的一單向函數而展開。檢查記錄(具產生的記錄登錄)與最後密鑰值皆透過分析這些值而傳送給一記錄處理單元，以偵測軟體侵入。在一特殊具體實施例中，記錄登錄值是相同，藉此減少傳送的記錄大小。在此具體實施例中，在傳送給記錄處理單元期間，只有最後密鑰值與一記錄登錄值需要傳送。因此，本發明能在軟體執行期間透過將"完整檢查"記錄在記錄檔而使用一完整檢查來偵測一進行中的設法程式處理。揭示的方法是將"完整檢查"與"前向安全"組合成一工作方法，並以設法程式處理沒有不被查出的此一方式而將此方法應用到

主動偵測電腦駭客使用軟體竄改。

在一擴大的具體實施例中，本發明的方法係進一步包含反應偵測竄改的步驟，其中反應包含下列任一者、或組合：中斷軟體碼使用者、取消軟體碼使用者的裝置密鑰值、拒絕來自軟體碼使用者的額外內容請求、增加在傳送給使用者的軟體碼或內容中的完整檢查類型的數量與多樣性、增加該檢查記錄與最後密鑰值的週期性傳輸頻率、與建議有關該偵測竄改的一系統管理者。

在另一擴大的具體實施例中，竄改可透過是否超過一記錄登錄的預定臨界值而(在記錄處理單元)發現。只要超過預定臨界值，上述反應的任一者便能由記錄處理單元使用。

【實施方式】

雖然本發明是在一較佳具體實施例中舉證與描述，但是本發明能產生許多不同結構、形式與材料。在此將詳細描述在圖中的本發明較佳具體實施例，且能了解到本揭示認為是本發明原理的範例及其結構的相關功能規格，而不是將本發明侷限於描述的具體實施例。熟諳此技者能了解到許多其他可能變化是在本發明的範圍內。

注意，在此整個規格中使用的術語"使用者"可視為一不信賴電腦(例如，機上盒、個人電腦、PDA、視訊遊戲控制台等)的操作員，且此使用者會嘗試以軟體碼(例如有關網站瀏覽器程式；音效卡驅動程式；遊戲控制台程式；Java® applet；或在例如影像、音樂或視訊檔案的多媒內容

中嵌入的巨集的軟體碼)與記錄竄改。此外，術語"記錄"可視為透過使用描述與軟體碼執行有關發生的一組登錄的檢查。在一實施中，登錄係描述在軟體碼中嵌入及由軟體碼(例如，在碼區塊的一核對加總)所執行的完整檢查結果。

本發明提供使用一檢查嘗試來偵測異常之系統及方法。注意，一情況可想像軟體是在客戶端執行(例如，一懷敵意的使用者機器)。因此，威脅會是來自不信賴使用者本身。特別注意的是此類型的威脅，只是因為電腦駭客不能只存取及使用程式碼來竄改，但亦能以檢查嘗試來竄改。因此，在此情況，嘗試本身需要受到保護，使得電腦駭客沒有方法來嘗試無法探查刪除任何舊登錄。雖然，過了一會兒，電腦駭客將完全了解記錄機構是可能的，而且從那點上，在嘗試中的新登錄是不能信賴。但是，根據本發明，電腦駭客不能回來修改在記錄中的登錄。

在此描述的本發明是在軟體執行來期間將"前向安全"性質應用到完整性檢查以偵測軟體竄改處理的一方法。當使用者連接到以獲得新內容時，記錄的任何截斷、記錄刪除、或一舊有效記錄的替換可容易偵測。假設在電腦駭客完全了解一特殊軟體程式之前，他將會觸發已記錄的許多"完整檢查"。因此，根據本發明，一電腦駭客在沒有偵測是不能做軟體逆工程。

前向安全可透過動態發展包含記錄的資訊而達成。例如，一亂數能當作執行開始中的一密鑰值來選取；然後，

此密鑰值能用來將一登錄記錄在記錄內。此密鑰值能使用單向函數來發展一新密鑰值，舊密鑰值然後可抹除(重寫)。其次，新密鑰值可用來將資訊記錄在記錄內。密鑰值能用來產生資訊，以決定要記錄什麼資訊、以將記錄加密或供任何其他使用。因此，包含記錄的登錄是使用單向函數發展的密鑰值功能。例如，在時間t，電腦駭客能發現他/她的行為記錄在記錄，但是他/她沒有方法回來找到先前密鑰值(在時間t前)，為了要使已記錄在記錄的資訊能嘗試使記錄保持正確性。

記錄將週期性連接及傳回給記錄處理單元(記錄處理單元是週期性接收記錄、檢查記錄以判斷竄改是否發生，透過將記錄內容與適當記錄內容相比較的實體)。同時，當軟體記錄程式碼執行發生時，相同的初始亂數(密鑰值)便會在記錄處理單元中以一同步方式展開。記錄處理單元知道應該包含記錄的資訊。在記錄處理單元中發生的確認/偵測處理然後能會是在傳回的記錄與記錄處理單元使用持續展開不同連接的相同展開密鑰值所計算正確資訊之間的簡單比較。如果不信賴的使用者替換一舊的有效記錄，密鑰值便不會是正確的。如果使用者提出一截除的記錄，那麼下次記錄便會傳送，密鑰值將不會是正確的。第一次，一異常會在記錄發現，記錄處理單元能送出警示給管理者。管理者下次能注意相同的使用者，或選擇將警示提供給使用者。當"充足"竄改證據累積(例如，超過一臨界值)時，使用者能從網路中斷，且不允許未來接受新的

內容分配。

在本方法中相關的基本步驟：

(1) 決定何處執行一完整檢查，並需要何類型的完整檢查。所有類型的完整檢查是在本發明的範圍內。例如，測試在一區塊碼的核對加總可以是完整檢查之一。

(2) 決定單向函數，例如C2_G、MD5、或RSA。C2_G(Cryptomeria)單向函數是使用在稱為CPRM的眾所週知內容保護方法的單向函數。MD5(訊息文摘#5）是普遍當作在數位簽字操作中的一密碼雜湊使用的單向函數。RSA是類別公眾鑰匙加密演算法。RSA加密演算法能充當不包含相關私人鍵匙任何一者的單向函數。

(3) 將完整檢查資訊嵌入受保護的程式碼，使得記錄登錄能在步驟(1)決定的點上產生，且當此發生時，密鑰值能使用單向函數來展開。

(4) 將記錄傳回給記錄處理單元，且記錄處理單元將查證記錄，並偵測竄改處理或判斷是否沒有竄改發生。

圖1描述密鑰值等差級數是與記錄登錄值無關的一般方法。記錄的大小是無限的。單向函數f1是用來發展與完整檢查值v_i無關的密鑰值f1(k_i)->k_i+1。另一f2函數係使用在完整檢查值v_i上的密鑰值來產生記錄登錄。函數f2能例如使用值v_i將密鑰值k_i加密，但是其他f2函數可被置換。因為密鑰值能使用單向函數發展，所以在時間t，當一電腦駭客成功竄改，且獲得目前密鑰值k_i時，電腦駭客仍然沒有方法知道先前密鑰值k_0....k_(i-1)。因此，

電腦駭客不能回來產生任何已記錄的記錄登錄。當記錄登錄傳回給記錄處理單元時，記錄處理單元可重複f2計算，並檢查記錄登錄在下列兩情況是否正確：他們是正確加密，且完整檢查值表示沒有竄改發生。因為設法處理在一些完整檢查值v_i失敗，所以記錄登錄會不正確，且能由記錄處理單元偵測到。

在本發明的基本方法(如前述)中，有與步驟(3)-(4)有關的兩個不同具體實施例。兩個具體實施例每一者的簡短描述可提供如下。

具體實施例A：圖2描述密鑰值等差級數使用記錄登錄值的本發明方法。在此綱要中，單向函數係使用目前密鑰值k_i與目前完整檢查值v_i來產生一新密鑰值k_(i+1)。在記錄中，只輸入目前完整檢查值v_i。記錄登錄與獲得的最後密鑰值k_n會傳向給記錄處理單元。當軟體設法處理程式、且電腦駭客使用一些完整檢查值v_i來竄改時，密鑰值展開便會錯誤。因此，記錄處理單元能使用k_0與記錄登錄值v_0...v_n來發展密鑰值，並偵測竄改處理。首先，它會檢查傳回的k_n能的確使用觀察的記錄登錄v-i來獲得。此是要判斷電腦駭客是否未使用在記錄中任何v_i值來竄改。然後，記錄處理單元能檢查實際v_i值來判斷在軟體執行期間是否有任何竄改的證據。

電腦駭客稍後能學習已儲存的正確完整檢查值v_i ；不幸地，對於電腦駭客而言，它是沒有幫忙的。首先，函數f是在k與v。當電腦駭客先摸索時，它是因為他/她不能成

功完整檢查及獲得錯誤的完整檢查值v。當在他/她設法程式處理期間處理，電腦駭客最後成功設法程式處理及找出正確完整檢查值v時，電腦駭客只知道目前密鑰值k_n，且不知道先前密鑰值k_0...k_(n-1)，而且電腦駭客仍然沒有方法知道正確k_n值是什麼。因此，記錄處理單元能始終偵測設法程式處理。其次，如果電腦駭客嘗試使所有正確的完整檢查值v_i在記錄中復原，那麼因為值k_n不符合觀察的v_i，所以記錄處理單元便應知道電腦駭客是否正嘗試產生記錄。

因此，具體實施例A允許用於清楚的實際記錄(只輸入目前完整檢查值v_i)。此觀點對於在某些應用能有利使用。

具體實施例B：圖3描述本發明的單密鑰值具體實施例。先前具體實施例需要將整個記錄傳回給記錄處理單元。記錄本身能隨時間而變得非常大。此具體實施例B是圖1的一般方法變化，且目標在於減少記錄的大小。在完整檢查期間，每當檢查成功時，完整檢查值便能產生一固定預設值值v。換句話說，只有當完整檢查失敗時，檢查值將會是除了v之外的一不同值。在此情況，因為一正確記錄只是一連串N值v，所以最後k_n與記錄長度N只是需要儲存及傳回給記錄處理單元的一些值。記錄處理單元能透過使用函數f來執行密鑰值計算，並檢查k_n是否正確。如果在軟體執行期間所有完整檢查是成功，最後的k_n必須是正確。如果在執行期間的任何完整檢查是失敗，完整檢查值會是不同於v，且密鑰值展開處理是錯誤的(即是，當f是

單向函數時，正確值從來不會重新產生)。

為了減少記錄處理單元中發生的確認計算處理，單向函數f的選擇使得任何有效密鑰值k_i能共用一共同性質，且不同於無效的密鑰值。然後，記錄處理單元需要確認此性質是否保存。它不再需要執行密鑰值展開處理。例如，如果一方法函數是一類似RSA的計算且v = 1：

$k_i = (v\ k_{i+1})^3 \bmod pq$　　(p與q是大質數)

然後，記錄處理單元能確認

$k_n = k_0^{3n} \bmod pq$

不知道因素p與q的電腦駭客或任何人不能在密鑰值發展中使用第(3n)根mod pq來向後移動，所以前向安全性質能維護。

密鑰值k_i需要儲存在一非揮發性記憶體，所以k展開不能讓使用者將電力關閉而重新設定。不容易讓末端使用者將一先前值復原亦是重要的，如此只將k_i儲存在一檔案通常是不足夠的。注意，本發明能想像使用在具有儲存內容密鑰值與使用計數正確相同問題的一內容保護應用。

當記錄具有一固定大小時，本發明的另一延伸包括迴繞的使用，且當超過固定大小時，一情況便會發生。具體實施例B是此的極端(具體實施例B可想像是大小1的記錄)。在圖1的一般方法中，如果一記錄具有一固定長度N，只要記錄處理單元知道已記錄的記錄登錄總數，每件事仍然可良好工作，即使由於迴繞而一些已遺失。透過使用總數，記錄處理單元能計算密鑰值展開，並讀取最後N個登

錄。注意，先前登錄已被重寫，但是當有一固定長度記錄時，此便無法避免。然而，具體實施例A略微需要更多幫忙來判斷記錄是否為固定長度。如果因為記錄處理單元已被重寫而使它遺失一些記錄登錄，記錄處理單元便不能計算密鑰值展開，且會讀取最後N個值。

因此，本發明能透過將"完整檢查"記錄在記錄檔而在軟體執行期間使用完整檢查來偵測一進行中的設法程式處理。揭示的方法是將"完整檢查"與"前向安全"組合在一工作方法，並將此方法應用來偵測電腦駭客是否以設法程式處理不能被發現的方式而使用軟體來竄改。

圖4描述實施本發明前述具體實施例(A與B)的系統400之概述。方塊402表示具嵌入完整檢查的一區塊軟體程式碼。如前述，各種不同完整檢查能想像。例如，一完整檢查可以在測試在一區塊軟體程式碼402上的一核對加總。方塊404與406分別表示檢查記錄與展開密鑰值。單向函數408是用來展開密鑰值406，其中單向函數是因先前記錄登錄(在檢查記錄404)與先前密鑰值而定。在一特殊具體實施例中，密鑰值是儲存在非揮發性記憶體405。在檢查記錄的值與最後密鑰值是傳送給記錄處理單元410，然後分析這些值(透過在404使用單向函數產生一連串密鑰值，並將一連串密鑰值與在記錄登錄的密鑰值相比較)來偵測軟體侵入。最後，如果記錄處理單元偵測到軟體侵入，一反應412便會傳送給例如一系統管理者的適當人員414。注意，密鑰值展開發生的位置不能用來限制本發明的範圍。

例如，前述密鑰值展開方法能在記錄處理單元410中實施。

此外，本發明能提供用於一產品物件，其包含在實施健全最佳化的一或多個模組中包含的電腦可讀程式碼。而且，本發明包括一以電腦程式碼為主之產品，此產品具有儲存程式碼的一儲存媒體，且這些程式碼能用來使電腦執行與本發明有關的任何方法。電腦儲存媒體包括(但是未侷限於)下列任一者：CD-ROM、DVD、磁帶、光碟、硬碟、軟碟、鐵電記憶體、快閃記憶體、強磁記憶體、光學儲存，電耦合裝置、磁或光學卡、智慧型卡、EEPROM、EPROM、隨機存取記憶體、ROM、DRAM、SRAM、SDRAM、或任何其他適當靜態或動態記憶體或資料儲存裝置。

在以電腦程式碼為主之產品實施是下列軟體模組：(a)在檢查記錄中產生記錄登錄；(b)根據單向函數而展開密鑰值，其中單向函數是因先前記錄登錄與先前密鑰值而定；及(c)透過分析該等記錄登錄與該等最後密鑰值來幫助將具產生的記錄登錄與一最後密鑰值的檢查記錄傳送給偵測軟體侵入的記錄處理單元。

結論

在前述具體實施例中顯示的一系統及方法能有效實施偵測軟體竄改的一系統及方法。雖然顯示及描述各種不同較佳具體實施例，但是可了解到並未以此揭示來限制本發明，而是涵蓋在如文後申請專利所定義本發明的精神與範圍內的所有修改與其他結構。例如，本發明並未受到軟體

碼類型、完整檢查類型、單向函數類型、或計算環境的限制。

上述增強是在各種不同計算環境實施。例如，本發明能在一傳統IBM個人電腦或類似、多樣式系統(例如，區域網路)或網路系統(例如，網際網路、WWW、無線網路)實施。有關此的所有程式規劃與資料是儲存在電腦記憶體、靜態或動態、並能在下列任一者由使用者取回：傳統電腦儲存裝置、顯示器(即是，CRT)及/或硬拷貝(即是，列印)格式。本發明的程式規劃能在技術安全/加密程式規劃中由熟諳此技者實施。

【圖式簡單說明】

圖1描述密鑰值等差級數是與記錄登錄值無關的一般方法。

圖2描述密鑰值等差級數使用記錄登錄值的本發明方法的一具體實施例。

圖3描述本發明的單一密鑰值具體實施例。

圖4描述實施在圖2與3揭示的具體實施例的一系統概述。

【圖式代表符號說明】

400	系統	405	非揮發性記憶體
402	軟體碼	406	鑰匙
404	記錄	408	單向函數
410	記錄處理單元		

伍、中文發明摘要：

本發明揭示軟體侵入能使用一動態展開檢查記錄而主動偵測，其中該等記錄登錄能在該檢查記錄中產生，且該等密鑰值能根據一單向函數而展開，此是因該先前記錄登錄與該先前密鑰值而定。具該等產生記錄登錄與該最後密鑰值的檢查記錄是傳送給一記錄處理單元，其能透過分析這些值而偵測軟體侵入。在致力於減少傳送的記錄大小中，該等記錄登錄是指定相同的值，藉此只需要將一記錄登錄與該最後密鑰值傳送給該記錄處理單元。

陸、英文發明摘要：

Software intrusion is proactively detected using a dynamically evolving audit log wherein log entries are generated in the audit log and key values are evolved based upon a one-way function depending on both the previous log entry and the previous key. The audit log with the generated log entries and the final key value is transmitted to a clearinghouse that detects software intrusion by analyzing these values. In an effort to reduce the size of the log to be transmitted, the log entries are assigned identical values, thereby only needing to transmit one log entry and the last key value to the clearinghouse.

拾、申請專利範圍：

1. 一種使用一動態展開檢查記錄來主動偵測軟體侵入之方法，該方法包含下列步驟：

a. 在該檢查記錄中產生記錄登錄；

b. 根據單向函數而展開密鑰值，該單向函數是因一先前記錄登錄與一先前密鑰值而定；及

c. 將具該等產生記錄登錄與一最後密鑰值傳送給一記錄處理單元，以透過分析該等記錄登錄與該最後密鑰值來偵測軟體侵入。

2. 如申請專利範圍第1項之方法，其中該等記錄登錄是根據軟體執行的完整檢查結果。

3. 如申請專利範圍第2項之方法，其中該完整檢查包括在一區段軟體碼上的一核對加總計算。

4. 如申請專利範圍第1項之方法，其中該等記錄登錄是相同值。

5. 如申請專利範圍第1項之方法，其中該檢查記錄有大小限制，藉使該等記錄登錄能形成迴繞的一檢查記錄。

6. 如申請專利範圍第1項之方法，其中該等先前密鑰值是在建立下一密鑰值之後刪除。

7. 如申請專利範圍第1項之方法，其中該展開密鑰值的步驟能獨立由該記錄處理單元執行。

8. 如申請專利範圍第1項之方法，其中該透過記錄處理單元的分析包括使用該單向函數而將一連串密鑰值再生，並將該等一連串密鑰值與在該等記錄登錄的密鑰值相比

較。

9. 如申請專利範圍第1項之方法，其中該等密鑰值的展開是在該產生步驟發生。

10. 如申請專利範圍第1項之方法，其中該等密鑰值的展開是在該傳送步驟發生。

11. 如申請專利範圍第1項之方法，其中該等密鑰值具有算術獨特性質。

12. 如申請專利範圍第1項之方法，其中該等密鑰值是儲存在非揮發性記憶體。

13. 如申請專利範圍第1項之方法，其中該傳輸是週期性發生。

14. 如申請專利範圍第1項之方法，其中該傳輸是在經由第三者的軟體碼執行期間發生。

15. 如申請專利範圍第1項之方法，其中如果記錄登錄異常的一臨界值已超過，該記錄處理單元便偵測到軟體竄改。

16. 一種包含一電腦可用媒體之產品物件，其中該電腦可用媒體具有在此儲存的電腦可讀程式碼，以使用一動態展開的檢查記錄來幫助主動偵測軟體侵入，該媒體包含：

a. 電腦可讀程式碼，以在該檢查記錄中產生記錄登錄；

b. 電腦可讀程式碼，以根據單向函數將密鑰值展開，該單向函數是因先前記錄登錄與先前密鑰值而定；及

c. 電腦可讀程式碼，以幫助將具該等產生的記錄登錄與一最後密鑰值傳送給一記錄處理單元，以透過分析該等記錄登錄與該最後密鑰值來偵測軟體侵入。

17. 一種使用動態展開的檢查記錄來主動偵測軟體侵入之方法，該方法包含下列步驟：

a. 將完整檢查嵌入在軟體碼；

b. 在該檢查記錄中產生具一相同記錄登錄值的記錄登錄；

c. 根據一單向函數將密鑰值展開，該單向函數是因該相同記錄登錄值與和先前密鑰值而定；及

d. 將該相同記錄登錄值與最後密鑰值傳送給一記錄處理單元，以透過分析該相同記錄登錄值與最後密鑰值來偵測軟體侵入。

18. 如申請專利範圍第17項之方法，其中該軟體碼包括：網站瀏覽器、音效卡驅動程式、遊戲控制台程式、Java applet、在其他數位內容嵌入的巨集。

19. 如申請專利範圍第18項之方法，其中該數位內容包含下列任一者：影像、音樂、視訊或資料庫檔案。

20. 如申請專利範圍第17項之方法，其中該方法進一步包含該反應偵測竄改的步驟，該反應包含下列任一者、或組合：中斷軟體碼使用者、使軟體碼使用者的裝置密鑰值失效、拒絕來自軟體碼使用者的額外內容請求、增加在傳送給使用者的軟體碼或內容中完整檢查類型的數量與多樣性、增加該檢查記錄與最後密鑰值的週期傳輸的頻率、與建議系統管理者有關該偵測竄改。

21. 如申請專利範圍第17項之方法，其中該檢查記錄有大小限制，藉使該記錄登錄形成迴繞的一檢查記錄。

22. 如申請專利範圍第17項之方法，其中該等完整檢查包括在該軟體碼區段上的一核對加總計算。

23. 如申請專利範圍第17項之方法，其中該等先前密鑰值是在下一密鑰值建立之後刪除。

24. 如申請專利範圍第17項之方法，其中該展開密鑰值的步驟是由該記錄處理單元獨立執行。

25. 如申請專利範圍第17項之方法，其中透過該記錄處理單元的分析包括使用該單向函數而將一連串密鑰值再生，並將該等一連串密鑰值與分解成該等記錄登錄的密鑰值相比較。

26. 如申請專利範圍第17項之方法，其中該密鑰值的展開是在該產生步驟發生。

27. 如申請專利範圍第17項之方法，其中該密鑰值的展開是在該傳輸步驟發生。

28. 如申請專利範圍第17項之方法，其中該等密鑰值具有算術特色的屬性。

29. 如申請專利範圍第17項之方法，其中該等密鑰值是儲存在非揮發性記憶體。

30. 如申請專利範圍第17項之方法，其中該傳輸是週期性發生。

31. 如申請專利範圍第17項之方法，其中該傳輸是經由第三者而在軟體碼執行期間發生。

32. 如申請專利範圍第17項之方法，其中如果超過記錄登錄異常的一臨界值，該記錄處理單元能偵測軟體竄改。

33. 一種包含一電腦可用媒體之產品物件，該電腦可用媒體具有在此具體實施的一電腦可讀程式碼，以透過使用一動態展開的檢查記錄來有利地幫助偵測軟體侵入，該媒體包含：

a. 電腦可讀程式碼，以將完整檢查嵌入軟體碼；

b. 電腦可讀程式碼，以產生在該檢查記錄中具一相同記錄登錄的記錄登錄；

c. 電腦可讀程式碼，其能根據一單向函數而展開密鑰值，該單向函數是因該相同記錄登錄值與先前密鑰值而定；及

d. 電腦可讀程式碼，以幫助將該相同記錄登錄值與最後密鑰值傳送給一記錄處理單元，以透過分析該相同記錄登錄值與最後密鑰值來偵測軟體侵入。

拾壹、圖式：

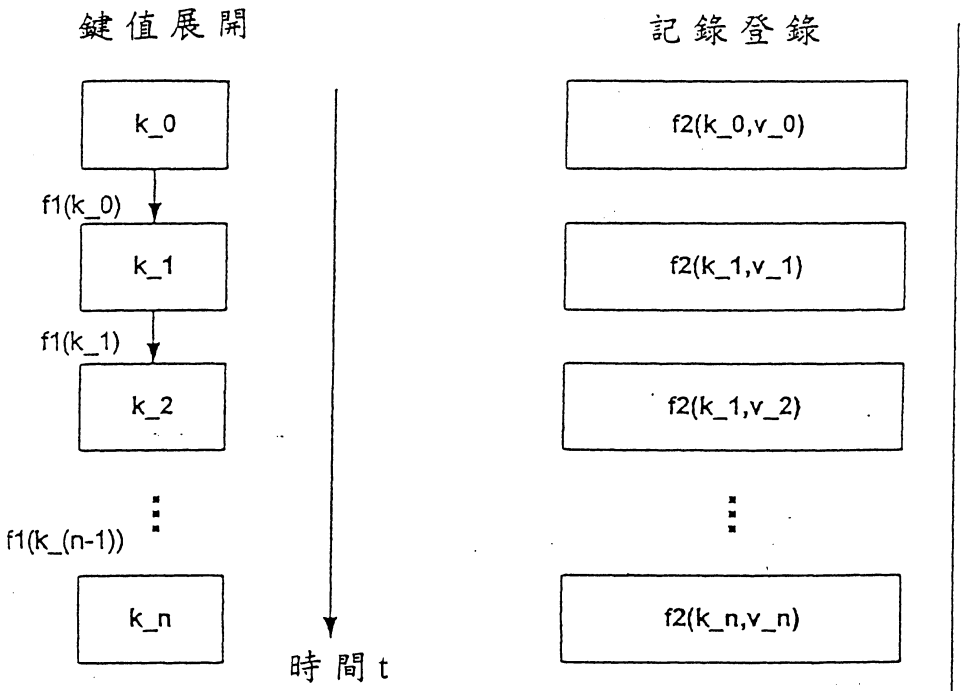
鍵值展開
記錄登錄
k_0
f2(k_0,v_0)
f1(k_0)
k_1
f2(k_1,v_1)
f1(k_1)
k_2
f2(k_1,v_2)
f1(k_(n-1))
k_n
f2(k_n,v_n)
時間 t

圖 1

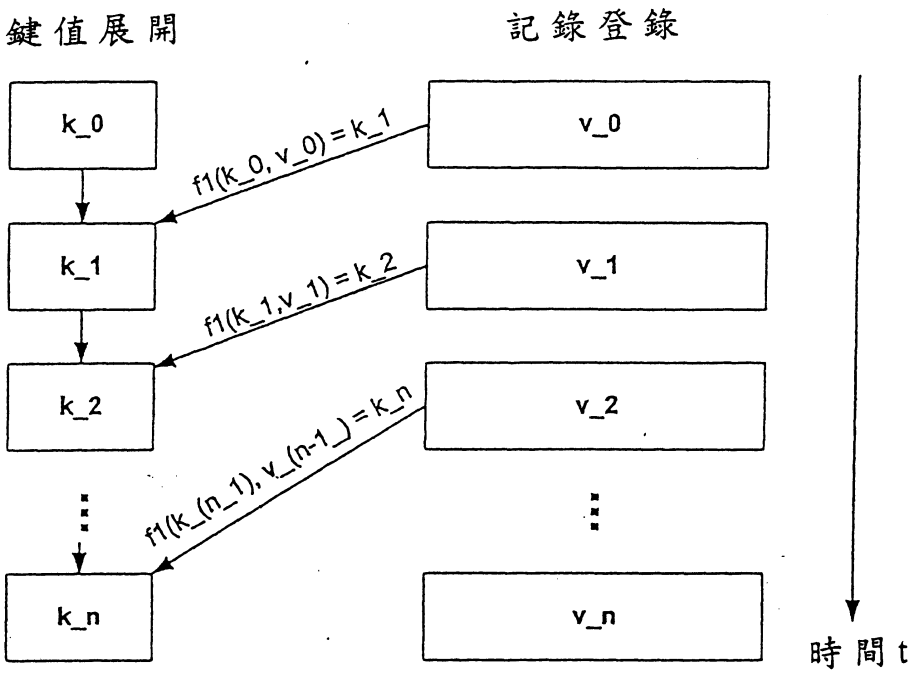
鍵值展開
記錄登錄
k_0
k_1
k_2
k_n
v_0
v_1
v_2
v_n
f1(k_0, v_0) = k_1
f1(k_1,v_1) = k_2
f1(k_(n_1), v_(n-1_) = k_n
時間 t

圖 2

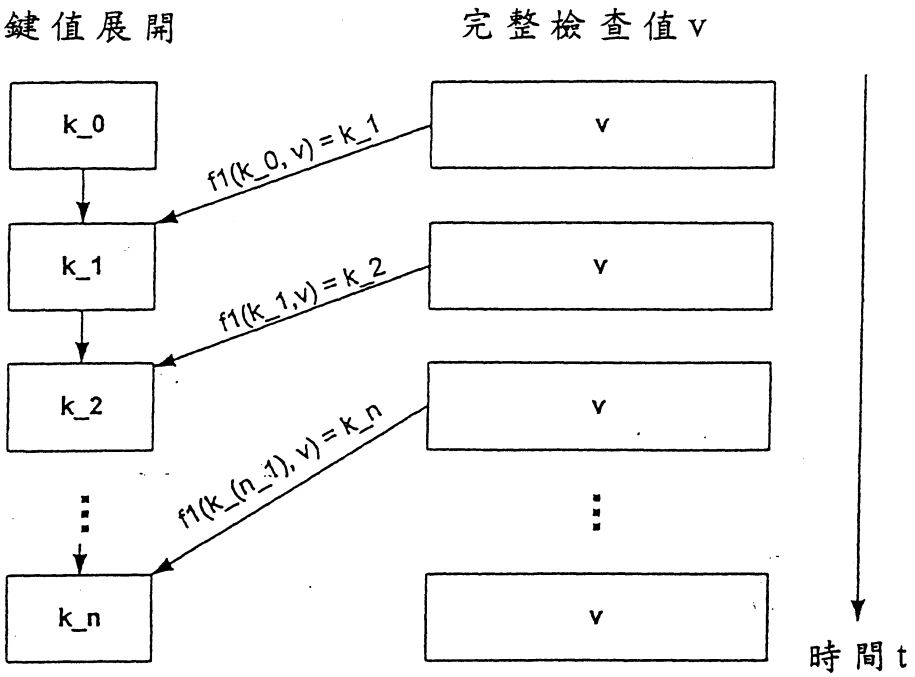

圖3

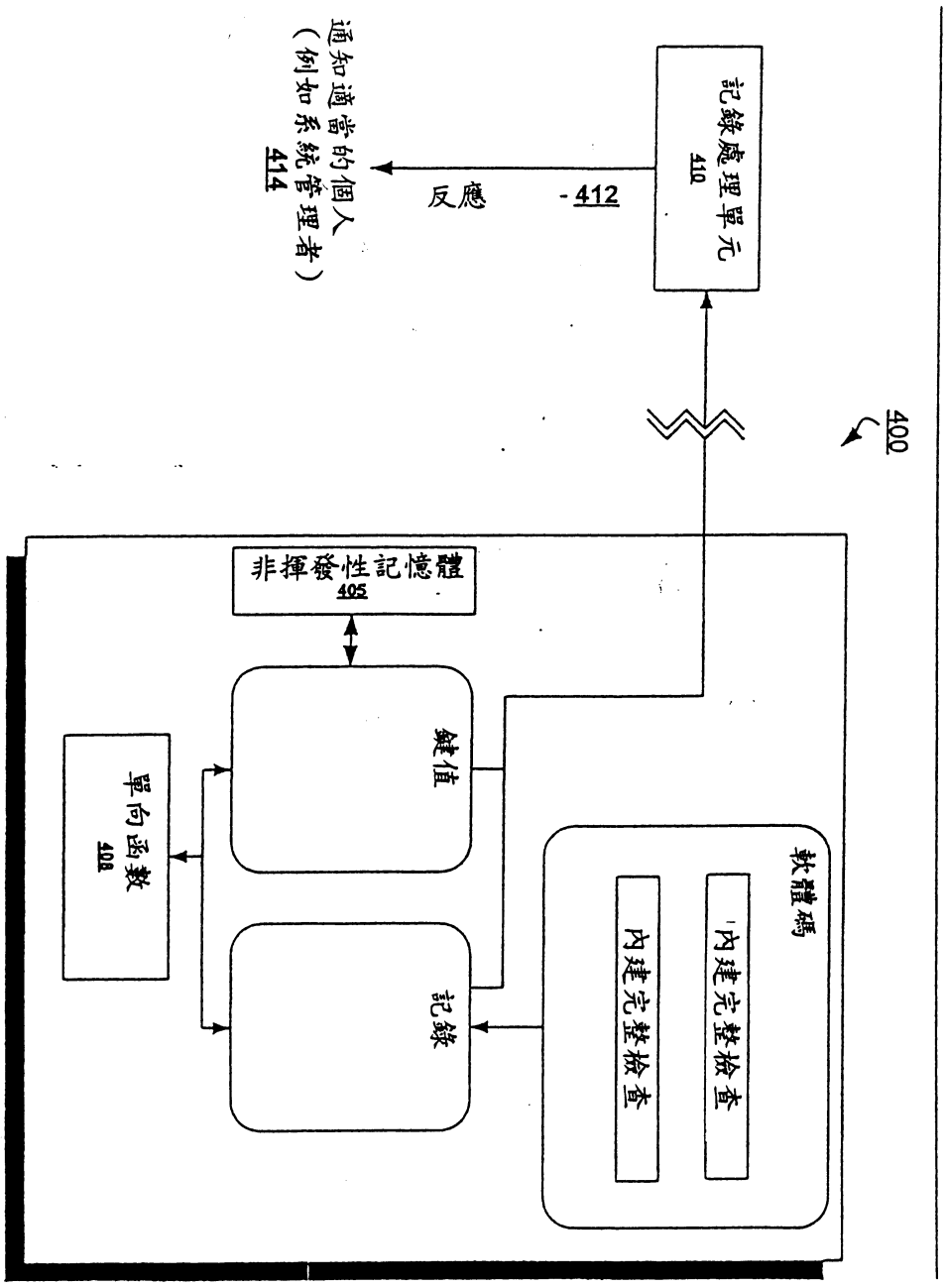
400
記錄處理單元
410
412
反應
通知適當的個人
（例如系統管理者）
414
軟體碼
內建完整檢查
內建完整檢查
鍵值
記錄
單向函數
408
非揮發性記憶體

圖 4

柒、指定代表圖：

(一)本案指定代表圖為：第（　2　）圖。

(二)本代表圖之元件代表符號簡單說明：

（無元件代表符號）

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（ 無 ）