I627551

(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 I627551 B

(45)公告日： 中華民國 107 (2018) 年 06 月 21 日

(21)申請案號：102131146　(22)申請日： 中華民國 102 (2013) 年 08 月 29 日

(51)Int. Cl.：　*G06F21/34　(2013.01)*　*G06K19/07　(2006.01)*

(71)申請人：徐一弘 (中華民國)　(TW)

新北市板橋區漢生東路 161 巷 5 號

(72)發明人：徐一弘 (TW)

(74)代理人：林文烽

(56)參考文獻：

TW　200816059A　TW　201013544A

US　4739328　US　5053774

審查人員：許人偉

申請專利範圍項數：12 項　圖式數：2　共 22 頁

(54)名稱

可驗證非接觸性感應標籤之系統及方法

(57)摘要

一種可驗證非接觸性感應標籤之系統及方法，該系統其具有：一讀取器，用以依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；一感應標籤，用以依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；以及一驗證裝置，用以接收該讀取器之所述授權請求，並對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以判斷該感應標籤是否為真。

指定代表圖：

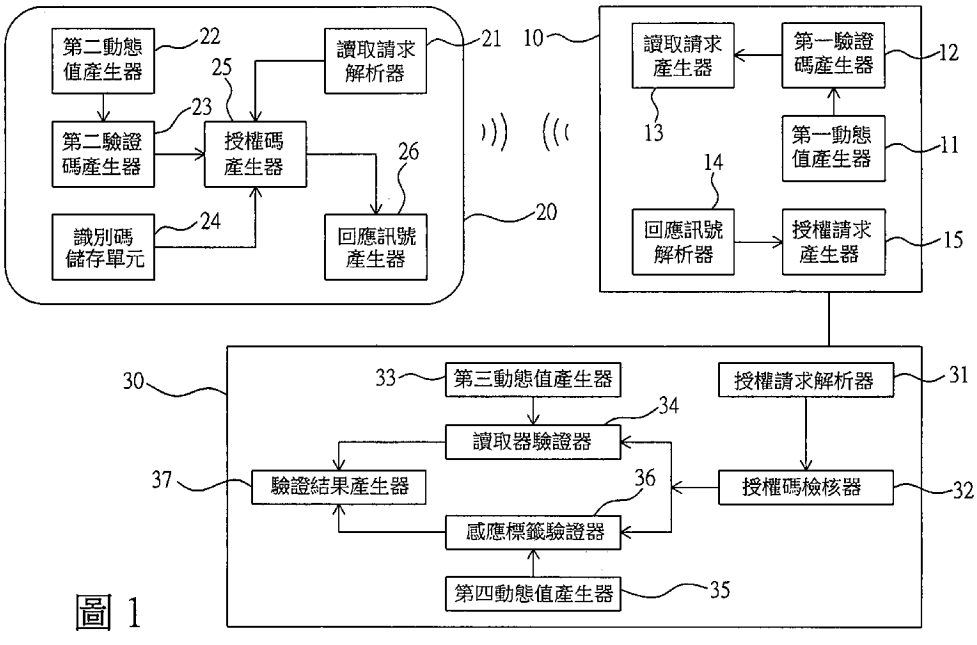

圖 1

符號簡單說明：

10・・・讀取器

11・・・第一動態值產生器

12・・・第一驗證碼產生器

13・・・讀取請求產生器

14・・・回應訊號解析器

15・・・授權請求產生器

20・・・感應標籤

21・・・讀取請求解析器

22・・・第二動態值產生器

23・・・第二驗證碼產生器

24・・・識別碼儲存單元

25・・・授權碼產生器

26・・・回應訊號產生器

30・・・驗證裝置

31・・・授權請求解析器

32・・・授權碼檢核器

33・・・第三動態值產生器

34・・・讀取器驗證器

35・・・第四動態值產生器

36・・・感應標籤驗證器

37・・・驗證結果產生器

【發明說明書】

【中文發明名稱】 可驗證非接觸性感應標籤之系統及方法

【技術領域】

【0001】 本發明係關於一種可驗證非接觸性感應標籤之系統及方法。

【先前技術】

【0002】 所謂非接觸性感應標籤，係指一種電子裝置可通過無線電訊號進行相關數據之辨識或讀寫，且讀取系統與感應標籤毋須進行任何機械或光學接觸，而是以無線電的訊號達成二者之間的聯絡，例如：以無線射頻辨識(RFID, Radio Frequency Identification)或近場通訊(Near Field Communication, NFC)等方式來交換資料之悠遊卡、感應式信用卡、門禁感應扣或NFC手機皆屬之，其在使用上具有極大的便利性。唯，習知感應標籤之識別碼為一固定數據或其加密後數據固定不變，易被側錄或破解，其安全性不佳。

【0003】 故專利字號發明第I384405號中提出一驗證方法，其利用一讀取器發送一第一驗證碼給一應答器，再從應答器所回應之信號解析出該第一驗證碼，並與該讀取器接收時產生之一第二驗證碼進行差異比較。由於該第一驗證碼與第二驗證碼為有相關之動態值，故具有防偽功效。但該習知驗證方法由於其應答器及讀取器皆屬於容易取得之裝置，較可能被偽造或破解，因而不適用於金融交易等安全性需求較高之應用環境。

【0004】 另外，美國專利申請公開號20050071231提出一種包含一授權裝置(authorizing entity)之系統，該系統以一感應標籤產生之一亂數及從一資料庫中取出一與該亂數相關之驗證碼，該授權裝置則從該亂數及該驗證碼之相關性驗證該標籤之真偽。又，專利字號發明第I325566號提出一改良之驗證方法，其係以一可變密鑰取代上述從資料庫中取出亂數、驗證碼之方式，以提高破解的難度。雖然上述二習知之驗證系統皆導入一驗證裝置，而非經由讀取器進行驗證，但由於該驗證裝置信任讀取器，僅依驗證資訊內之矛盾來判別真、偽，故當有心人士藉由側錄該驗證資訊並偽造讀取器而發出驗證請求時，上述習知之驗證系統就會被欺瞞。

【0005】 為解決上述之問題，吾人亟需一種更可靠的非接觸性感應標籤驗證機制。

【發明內容】

【0006】 本發明之一目的在於揭露一種可提高非接觸性感應標籤之真、偽辨識可靠度之驗證系統及方法。

【0007】 本發明之另一目的在於揭露一種非接觸性感應標籤之驗證系統及方法，其可同時驗證感應標籤及讀取器之真、偽以提高感應標籤之真、偽辨識可靠度。

【0008】 為達到上述目的，本發明提出一種可驗證非接觸性感應標籤之系統，其具有：

【0009】 一讀取器，用以依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；

【0010】 一感應標籤，用以依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；以及

【0011】 一驗證裝置，用以接收該讀取器之所述授權請求，對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以一第三動態值和所述第一動態值進行一第一比較運算以產生一第一差異值，以一第四動態值和所述第二動態值進行一第二比較運算以產生一第二差異值，以及依所述第一差異值判斷該讀取器是否為真和依所述第二差異值判斷該感應標籤是否為真，其中該解密運算係和該加密運算相對應。

【0012】 在一實施例中，該讀取器具有一第一動態值產生器以依一第一運算子模式產生所述的第一動態值、一第一驗證碼產生器以依一第一密文模式產生所述的第一驗證碼，該感應標籤具有一第二動態值產生器以依一第二運算子模式產生所述的第二動態值、一第二驗證碼產生器以依一第二密文模式產生所述的第二驗證碼，以及該驗證裝置具有一第三動態值產生器以依所述第一運算

子模式產生所述的第三動態值及一第四動態值產生器以依所述第二運算子模式產生所述的第四動態值。

【0013】 在一實施例中，所述的第一運算子模式和第二運算子模式均係由一時間戳模式、一計次模式、和一口令模式所組成的群組所選擇的一種模式。

【0014】 在一實施例中，所述的第一密文模式和第二密文模式均係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式。

【0015】 在一實施例中，所述的加密運算係以所述識別碼、所述第一驗證碼、和所述第二驗證碼做為來源運算元，而其目的運算元之內容則為所述的授權碼；所述的解密運算係以所述的授權碼作為來源運算元，而其目的運算元之內容則分別為所述識別碼、所述第一驗證碼、和所述第二驗證碼。

【0016】 在一實施例中，所述的非接觸方式係一無線射頻通訊方式。

【0017】 為達到上述目的，本發明進一步提出一種可驗證非接觸性感應標籤之方法，其包含以下步驟：

【0018】 第一步驟：使一讀取器依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；

【0019】 第二步驟：使一感應標籤依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；

【0020】 第三步驟：使一驗證裝置接收該讀取器之所述授權請求，對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以一第三動態值和所述第一動態值進行一第一比較運算以產生一第一差異值，以一第四動態值和所述第二動態值進行一第二比較運算以產生一第二差異值，以及依所述第一差異值判斷該讀取器是否為真和依所述第二差異值判斷該感應標籤是否為真，其中該解密運算係和該加密運算相對應；以及

【0021】 第四步驟：該驗證裝置依該讀取器及該感應標籤之真、偽判斷，決定該識別碼之真、偽。

【0022】在一實施例中，該讀取器具有一第一動態值產生器以依一第一運算子模式產生所述的第一動態值、一第一驗證碼產生器以依一第一密文模式產生所述的第一驗證碼，該感應標籤具有一第二動態值產生器以依一第二運算子模式產生所述的第二動態值、一第二驗證碼產生器以依一第二密文模式產生所述的第二驗證碼，以及該驗證裝置具有一第三動態值產生器以依所述第一運算子模式產生所述的第三動態值及一第四動態值產生器以依所述第二運算子模式產生所述的第四動態值。

【0023】在一實施例中，所述之第一運算子模式和第二運算子模式均係由一時間戳模式、一計次模式、和一口令模式所組成的群組所選擇的一種模式。

【0024】在一實施例中，所述的第一密文模式和第二密文模式均係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式。

【0025】在一實施例中，所述的加密運算係以所述識別碼、所述第一驗證碼、和所述第二驗證碼做為來源運算元，而其目的運算元之內容則為所述的授權碼；所述的解密運算係以所述的授權碼作為來源運算元，而其目的運算元之內容則分別為所述識別碼、所述第一驗證碼、和所述第二驗證碼。

【0026】在一實施例中，所述的非接觸方式係一無線射頻通訊方式。

【0027】為使　貴審查委員能進一步瞭解本發明之結構、特徵及其目的，茲附以圖式及較佳具體實施例之詳細說明如后。

【圖式簡單說明】

【0028】

圖1繪示本發明可驗證非接觸性感應標籤之系統其一實施例之方塊圖。

圖2繪示本發明可驗證非接觸性感應標籤之方法其一實施例之流程圖。

【實施方式】

【0029】請參照圖1，其繪示本發明可驗證非接觸性感應標籤之系統其一實施例之方塊圖。如圖1所示，該系統包括一讀取器10、一感應標籤20、及一驗證裝置30。

【0030】 讀取器10係用以依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求。讀取器10具有一第一動態值產生器11、一第一驗證碼產生器12、一讀取請求產生器13、一回應訊號解析器14、以及一授權請求產生器15。

【0031】 第一動態值產生器11係依一第一運算子模式產生所述的第一動態值，而所述的第一運算子模式係由一時間戳模式、和一計次模式所組成的群組所選擇的一種模式。所述的時間戳模式係依一時鐘之目前時間產生所述的第一動態值；所述的計次模式係依一計數器之目前計數值產生所述的第一動態值。

【0032】 第一驗證碼產生器12以一第一密文模式處理所述第一動態值以產生所述的第一驗證碼，而所述的第一密文模式係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式，可使所述的第一驗證碼具有可逆性。

【0033】 讀取請求產生器13依一約定編碼標準產生包含所述第一驗證碼之一讀取請求，以供讀取器10傳送至感應標籤20。

【0034】 回應訊號解析器14依所述約定編碼標準對感應標籤20所送出之一回應訊號進行解析以獲得所述的授權碼。

【0035】 授權請求產生器15依一約定通訊協定產生包含所述的授權碼之所述的授權請求，以供讀取器10傳送至驗證裝置30。

【0036】 感應標籤20係用以依一非接觸方式獲得讀取器10之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼轉成所述的回應訊號以藉由所述的非接觸方式傳送至讀取器10，其中，所述的非接觸方式係一RF (radio frequency；無線射頻)通訊方式。感應標籤20具有一讀取請求解析器21、一第二動態值產生器22、一第二驗證碼產生器23、一識別碼儲存單元24、一授權碼產生器25、以及一回應訊號產生器26。

【0037】 讀取請求解析器21係用以依所述約定編碼標準對讀取器10所送出的所述讀取請求進行解析以獲得所述的第一驗證碼。

【0038】 第二動態值產生器22係依一第二運算子模式產生所述的第二動態值，而所述的第二運算子模式係由所述的時間戳模式、所述的計次模式所組

成的群組所選擇的一種模式。所述的第二運算子模式和所述的第一運算子模式係互相獨立，亦即二者可相同也可相異。

【0039】 第二驗證碼產生器23依所述第二動態值及一第二密文模式產生所述的第二驗證碼，而所述的第二密文模式係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式，可使所述的第二驗證碼具有可逆性。所述的第二密文模式和所述的第一密文模式係互相獨立，亦即二者可相同也可相異。

【0040】 授權碼產生器25係用以依一識別碼儲存單元24所儲存之識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，其中所述的識別碼係代表感應標籤20之身分相關數據，而所述的加密運算係以所述識別碼、所述第一驗證碼、和所述第二驗證碼作為來源運算元，而其目的運算元之內容則為所述的授權碼。

【0041】 回應訊號產生器26係用以依所述的約定編碼標準產生包含所述的授權碼之所述的回應訊號。

【0042】 驗證裝置30係用以接收讀取器10之所述授權請求，對所述授權請求進行一解密運算以獲得所述的識別碼、所述的第一動態值和所述的第二動態值，以一第三動態值和所述第一動態值進行一第一比較運算以產生一第一差異值，以一第四動態值和所述第二動態值進行一第二比較運算以產生一第二差異值，以及依所述第一差異值判斷讀取器10是否為真和依所述第二差異值判斷感應標籤20是否為真，其中該解密運算係和所述的加密運算相對應，亦即，所述的解密運算係以所述的授權碼作為來源運算元，而其目的運算元之內容則分別為所述識別碼、所述第一驗證碼、和所述第二驗證碼。驗證裝置30具有一授權請求解析器31、一授權碼檢核器32、一第三動態值產生器33、一讀取器驗證器34、一第四動態值產生器35、一感應標籤驗證器36、以及一驗證結果產生器37。

【0043】 授權請求解析器31係用以依所述的約定通訊協定對讀取器10所送出的所述的授權請求進行解析以獲得所述的授權碼。

【0044】 授權碼檢核器32係用以依所述的授權碼進行所述的解密運算，以獲得所述的識別碼、所述的第一驗證碼、及所述的第二驗證碼。

【0045】 第三動態值產生器33係用以依所述第一運算子模式產生所述的第三動態值。

【0046】 讀取器驗證器34係用以依所述第一密文模式及所述的第一驗證碼獲得所述第一動態值，及依所述第三動態值和所述第一動態值進行所述的第一比較運算以產生所述的第一差異值，並依所述第一差異值是否在一第一預定範圍內，以決定讀取器10是否為真。

【0047】 第四動態值產生器35係用以依所述第二運算子模式產生所述的第四動態值。

【0048】 感應標籤驗證器36係用以依所述第二密文模式及所述的第二驗證碼獲得所述第二動態值，及依所述第四動態值和所述第二動態值進行所述的第二比較運算以產生所述的第二差異值，並依所述第二差異值是否在一第二預定範圍內，以決定感應標籤20是否為真。

【0049】 驗證結果產生器37係用以依讀取器驗證器34和感應標籤驗證器36的判斷結果產生對感應標籤20的最終真、偽判斷。

【0050】 另外，本發明的可驗證非接觸性感應標籤之系統亦可採用一種口令模式以產生所述的第一動態值、第二動態值、第三動態值及第四動態值。在所述的口令模式下，驗證裝置30會產生一第一動態口令資料及一第二動態口令資料，二者互相獨立，可相同或相異，其中該第一動態口令資料被指定為所述的第三動態值，該第二動態口令資料被指定為所述的第四動態值。驗證裝置30會將該第一動態口令資料及該第二動態口令資料傳送至讀取器10。讀取器10會以該第一動態口令資料做為所述的第一動態值並將該第二動態口令資料傳送至感應標籤20。感應標籤20會以該第二動態口令資料做為所述的第二動態值。後續的驗證程序同於上述之說明，故在此不擬贅述。

【0051】 依上述之原理，本發明進一步提出一種可驗證非接觸性感應標籤之方法，其包含以下步驟：

【0052】 第一步驟：使一讀取器依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；

【0053】 第二步驟：使一感應標籤依一非接觸方式接收該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；

【0054】 第三步驟：使一驗證裝置接收該讀取器之所述授權請求，對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以一第三動態值和所述第一動態值進行一第一比較運算以產生一第一差異值，以一第四動態值和所述第二動態值進行一第二比較運算以產生一第二差異值，以及依所述第一差異值判斷該讀取器是否為真和依所述第二差異值判斷該感應標籤是否為真，其中該解密運算係和該加密運算相對應；以及

【0055】 第四步驟：該驗證裝置依該讀取器及該感應標籤之真、偽判斷，決定該識別碼之真、偽。

【0056】 其中，該讀取器具有一第一動態值產生器以依一第一運算子模式產生所述的第一動態值、一第一驗證碼產生器以依一第一密文模式產生所述的第一驗證碼，該感應標籤具有一第二動態值產生器以依一第二運算子模式產生所述的第二動態值、一第二驗證碼產生器以依一第二密文模式產生所述的第二驗證碼，以及該驗證裝置具有一第三動態值產生器以依所述第一運算子模式產生所述的第三動態值及一第四動態值產生器以依所述第二運算子模式產生所述的第四動態值。

【0057】 其中所述之第一運算子模式和第二運算子模式均係由一時間戳模式、一計次模式、和一口令模式所組成的群組所選擇的一種模式。

【0058】 其中所述的第一密文模式和第二密文模式均係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式。

【0059】 其中所述的加密運算係以所述識別碼、所述第一驗證碼、和所述第二驗證碼做為來源運算元，而其目的運算元之內容則為所述的授權碼；所述的解密運算係以所述的授權碼作為來源運算元，而其目的運算元之內容則分別為所述識別碼、所述第一驗證碼、和所述第二驗證碼。

【0060】 其中所述的非接觸方式係一無線射頻通訊方式。

【0061】 請參照圖2，其繪示本發明可驗證非接觸性感應標籤之方法其一實施例之流程圖，其具體之實施步驟配合圖1之系統說明如后：

【0062】 步驟a：一讀取器依一第一動態值產生一第一驗證碼，並產生內含該第一驗證碼之一讀取請求。例如：一讀取器10發送一讀取請求時，若第一動態值產生器11以一計次模式為所述的第一運算子模式，在請求當時之計次值“123”為第一動態值，若第一驗證碼產生器12以一查表模式為所述的第一密文模式，則第一驗證碼產生器12會依指標位置“123”讀取一表格以產生一第一驗證碼“ABC”，再經讀取請求產生器13依一所述的約定之編碼標準(例如ISO/IEC 14443)產生一內含“ABC”之讀取請求。

【0063】 步驟b：一感應標籤接收該讀取請求以獲得該第一驗證碼，並依一第二動態值產生一第二驗證碼。例如：感應標籤20之讀取請求解析器21依所述的編碼標準(ISO/IEC 14443)，從接收之該讀取請求中，解析出第一驗證碼“ABC”，且若第二動態值產生器22以一時間戳模式為所述的第二運算子模式，在回應當時之值“201307041259”為第二動態值，若第二驗證碼產生器23以一預定公式模式為所述的第二密文模式，則第二驗證碼產生器23會依所述預定公式模式依該第二動態值產生一第二驗證碼“952140703102”。

【0064】 步驟c：該感應標籤依一加密運算產生內含一識別碼、該第一驗證碼、以及該第二驗證碼資訊之一授權碼。例如：感應標籤20之識別碼儲存單元24儲存一識別碼“甲乙丙”，授權碼產生器25產生一授權碼“ABC952140703102A甲952140B乙703102C丙”，則該加密運算即以最前端之英文字母“ABC”為該第一驗證碼、最前端之數字“952140703102”為該第二驗證碼、餘下之“A甲952140B乙703102C丙”為內含該識別碼之對稱式加密密文(ciphertext)，該第一驗證碼及該第二驗證碼為其密鑰(secret key)，該識別碼“甲乙丙”為其明文(plaintext)。

【0065】 再例如，另一加密運算產生一另一授權碼“ABC952140703102甲乙丙abcxyz”，即以最前端之大寫英文字母“ABC”為該第一驗證碼、最前端之

數字“952140703102”為該第二驗證碼、最前端之中文字“甲乙丙”為該識別碼、餘下之“abcxyz”為第一驗證碼、第二驗證碼及識別碼的雜湊值，用以確認授權碼的正確性。

【0066】步驟d：該感應標籤產生內含該授權碼之一回應訊號。例如：一感應標籤20之回應訊號產生器26，依所述的編碼標準(ISO/IEC 14443)產生內含授權碼“ABC952140703102A甲952140B乙703102C丙”或另一例“ABC952140703102甲乙丙abcxyz”之一回應訊號。

【0067】步驟e：該讀取器接收該回應訊號並傳送內含該授權碼之一授權請求至一驗證裝置。例如：一讀取器10之回應訊號解析器14可依所述的編碼標準(ISO/IEC 14443)解析該回應訊號中內含之授權碼，並由授權請求產生器15依一所述的約定之通訊協定(例如HTTPS或UART)產生內含該授權碼“ABC952140703102A甲952140B乙703102C丙”或另一例“ABC952140703102甲乙丙abcxyz”之一授權請求，再由一網路連線或電性連接傳送至驗證裝置30。

【0068】步驟f：該驗證裝置接收該授權請求並獲得該授權碼，依一解密運算獲得該識別碼、該第一驗證碼、及該第二驗證碼。例如：驗證裝置30之授權請求解析器31依所述的通訊協定(例如HTTPS或UART)取得該授權請求內含之該授權碼“ABC952140703102A甲952140B乙703102C丙”，授權碼檢核器32依所述之解密運算，即以最前端之英文字母“ABC”為該第一驗證碼、最前端之數字“952140703102”為該第二驗證碼、餘下之“A甲952140B乙703102C丙”為內含該識別碼之對稱式加密密文，該第一驗證碼及該第二驗證碼為其密鑰，該識別碼“甲乙丙”為其明文。

【0069】再例如，另一解密運算依所述的另一授權碼“ABC952140703102甲乙丙abcxyz”，即以最前端之大寫英文字母“ABC”為該第一驗證碼、最前端之數字“952140703102”為該第二驗證碼、最前端之中文字“甲乙丙”為該識別碼，再以該第一驗證碼、該第二驗證碼及該識別碼的雜湊值比較是否為餘下之“abcxyz”，用以檢核加密資訊之正確性。

【0070】 步驟g：該驗證裝置依一第三動態值計算與該第一驗證碼內含該第一動態值之差異值，以判斷該讀取器是否為真；以及依一第四動態值計算與該第二驗證碼內含該第二動態值之差異值，以判斷該感應標籤是否為真。例如：驗證裝置30之讀取器驗證器34驗證讀取器10是否為真，係以此時第三動態值產生器33依所述的第一運算子模式所產生之計次值，即前次驗證成功之第一動態值“108”為第三動態值。讀取器驗證器34依所述的第一密文模式，以該第一驗證碼“ABC”查表取得該第一動態值“123”，並經所述第一比較運算將該第一動態值減去該第三動態值以獲得一第一差異值(=123-108=15)。在此例中，我們設定當所述第一差異值為正時，讀取器10為真。因該第一差異值為15，故讀取器10為真。

【0071】 驗證裝置30之感應標籤驗證器36驗證感應標籤20是否為真，係以此時第四動態值產生器35依所述的第二運算子模式所產生之時間戳，即當時之值“201307041302”為該第四動態值，感應標籤驗證器36依所述的第二密文模式，以該第二驗證碼“952140703102”依所述之預定公式模式獲得該第二動態值“201307041259”，並經所述的第二比較運算將該第四動態值減去該第二動態值以獲得一第二差異值(=3)。在此例中，我們設定當所述第二差異值大於等於0且小於等於5(5分鐘)時，感應標籤20為真。因該第二差值等於3，故感應標籤20為真。

【0072】 步驟h：該驗證裝置依該讀取器及該感應標籤之真、偽判斷，決定該識別碼之真、偽。例如：當讀取器驗證器34驗證該讀取器10為真，且感應標籤驗證器36驗證感應標籤20為真時，驗證結果產生器37則判定從感應標籤20內所讀取之該識別碼“甲乙丙”為真。

【0073】 另外，本發明的可驗證非接觸性感應標籤之方法亦可採用一種口令模式以產生所述的第一動態值、第二動態值、第三動態值及第四動態值。在所述的口令模式下，驗證裝置30會產生一第一動態口令資料及一第二動態口令資料，二者互相獨立，可相同或相異，其中該第一動態口令資料被指定為所述的第三動態值，該第二動態口令資料被指定為所述的第四動態值。驗證裝置30會將該第一動態口令資料及該第二動態口令資料傳送至讀取器10。讀取器10會以

該第一動態口令資料做為所述的第一動態值並將該第二動態口令資料傳送至感應標籤20。感應標籤20會以該第二動態口令資料做為所述的第二動態值。後續的驗證程序同於上述之說明，故在此不擬贅述。

【0074】 本案所揭示者，乃較佳實施例，舉凡局部之變更或修飾而源於本案之技術思想而為熟習該項技藝之人所易於推知者，俱不脫本案之專利權範疇。

【0075】 綜上所陳，本案無論就目的、手段與功效，在在顯示其迥異於習知之技術特徵，且其首先發明合於實用，亦在在符合發明之專利要件，懇請 貴審查委員明察，並祈早日賜予專利，俾嘉惠社會，實感德便。

【符號說明】

【0076】

讀取器 10

第一動態值產生器 11

第一驗證碼產生器 12

讀取請求產生器 13

回應訊號解析器 14

授權請求產生器 15

感應標籤 20

讀取請求解析器 21

第二動態值產生器 22

第二驗證碼產生器 23

識別碼儲存單元 24

授權碼產生器 25

回應訊號產生器 26

驗證裝置 30

授權請求解析器 31

授權碼檢核器 32

第三動態值產生器 33

讀取器驗證器 34

第四動態值產生器 35

感應標籤驗證器 36

驗證結果產生器 37

步驟a：在此步驟中，一讀取器依一第一動態值產生一第一驗證碼，並產生內含該第一驗證碼之一讀取請求。

步驟b：在此步驟中，一感應標籤接收該讀取請求以獲得該第一驗證碼，並依一第二動態值產生一第二驗證碼。

步驟c：在此步驟中，該感應標籤依一加密運算產生內含一識別碼、該第一驗證碼、以及該第二驗證碼資訊之一授權碼。

步驟d：在此步驟中，該感應標籤產生內含該授權碼之一回應訊號。

步驟e：在此步驟中，該讀取器接收該回應訊號並傳送內含該授權碼之一授權請求至一驗證裝置。

步驟f：在此步驟中，該驗證裝置接收該授權請求並獲得該授權碼，且依一解密運算獲得該識別碼、該第一驗證碼、及該第二驗證碼。

步驟g：在此步驟中，該驗證裝置依一第三動態值計算與該第一驗證碼內含該第一動態值之差異值，以判斷該讀取器是否為真；以及依一第四動態值計算與該第二驗證碼內含該第二動態值之差異值，以判斷該感應標籤是否為真。

步驟h：在此步驟中，該驗證裝置依該讀取器及該感應標籤之真、偽判斷，決定該識別碼之真、偽。

I627511 專利案號：102131146

公告本

104年11月02日 修正

申請日：102/08/29

IPC分類：G06F 21/34 (2013.01)
G06K 19/07 (2006.01)

【發明摘要】

【中文發明名稱】可驗證非接觸性感應標籤之系統及方法

【中文】

一種可驗證非接觸性感應標籤之系統及方法，該系統其具有：一讀取器，用以依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；一感應標籤，用以依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；以及一驗證裝置，用以接收該讀取器之所述授權請求，並對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以判斷該感應標籤是否為真。

【指定代表圖】 第（1）圖。

【代表圖之符號簡單說明】

讀取器 10

第一動態值產生器 11

第一驗證碼產生器 12

讀取請求產生器 13

回應訊號解析器 14

授權請求產生器 15

感應標籤 20

讀取請求解析器 21

第二動態值產生器 22

第二驗證碼產生器 23

識別碼儲存單元 24

授權碼產生器 25

回應訊號產生器 26

【發明申請專利範圍】

【第1項】一種可驗證非接觸性感應標籤之系統，其具有：

一讀取器，用以依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；

一感應標籤，用以依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；以及

一驗證裝置，用以接收該讀取器之所述授權請求，對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以一第三動態值和所述第一動態值進行一第一比較運算以產生一第一差異值，以一第四動態值和所述第二動態值進行一第二比較運算以產生一第二差異值，以及依所述第一差異值判斷該讀取器是否為真和依所述第二差異值判斷該感應標籤是否為真，其中該解密運算係和該加密運算相對應。

【第2項】如申請專利範圍第1項所述之系統，其中該讀取器具有一第一動態值產生器以依一第一運算子模式產生所述的第一動態值、一第一驗證碼產生器以依一第一密文模式產生所述的第一驗證碼，該感應標籤具有一第二動態值產生器以依一第二運算子模式產生所述的第二動態值、一第二驗證碼產生器以依一第二密文模式產生所述的第二驗證碼，以及該驗證裝置具有一第三動態值產生器以依所述第一運算子模式產生所述的第三動態值及一第四動態值產生器以依所述第二運算子模式產生所述的第四動態值。

【第3項】如申請專利範圍第2項所述之系統，其中所述之第一運算子模式和第二運算子模式均係由一時間戳模式、一計次模式、和一口令模式所組成的群組所選擇的一種模式。

【第4項】如申請專利範圍第2項所述之系統，其中所述之第一密文模式和第二密文模式均係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式。

【第5項】 如申請專利範圍第1項所述之系統，其中所述的加密運算係以所述識別碼、所述第一驗證碼、和所述第二驗證碼做為來源運算元，而其目的運算元之內容則為所述的授權碼；所述的解密運算係以所述的授權碼作為來源運算元，而其目的運算元之內容則分別為所述識別碼、所述第一驗證碼、和所述第二驗證碼。

【第6項】 如申請專利範圍第1項所述之系統，其中所述的非接觸方式係一無線射頻通訊方式。

【第7項】 一種可驗證非接觸性感應標籤之方法，包含以下步驟：

第一步驟：使一讀取器依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；

第二步驟：使一感應標籤依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；

第三步驟：使一驗證裝置接收該讀取器之所述授權請求，對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以一第三動態值和所述第一動態值進行一第一比較運算以產生一第一差異值，以一第四動態值和所述第二動態值進行一第二比較運算以產生一第二差異值，以及依所述第一差異值判斷該讀取器是否為真和依所述第二差異值判斷該感應標籤是否為真，其中該解密運算係和該加密運算相對應；以及

第四步驟：該驗證裝置依該讀取器及該感應標籤之真、偽判斷，決定該識別碼之真、偽。

【第8項】 如申請專利範圍第7項所述之方法，其中，該讀取器具有一第一動態值產生器以依一第一運算子模式產生所述的第一動態值、一第一驗證碼產生器以依一第一密文模式產生所述的第一驗證碼，該感應標籤具有一第二動態值產生器以依一第二運算子模式產生所述的第二動態值、一第二驗證碼產生器以依一第二密文模式產生所述的第二驗證碼，以及該驗證裝置具有一第三動態值

產生器以依所述第一運算子模式產生所述的第三動態值及一第四動態值產生器以依所述第二運算子模式產生所述的第四動態值。

【第9項】 如申請專利範圍第8項所述之方法，其中所述之第一運算子模式和第二運算子模式均係由一時間戳模式、一計次模式、和一口令模式所組成的群組所選擇的一種模式。

【第10項】 如申請專利範圍第8項所述之方法，其中所述之第一密文模式和第二密文模式均係由一預定公式模式、和一查表模式所組成的群組所選擇的一種模式。

【第11項】 如申請專利範圍第7項所述之方法，其中所述的加密運算係以所述識別碼、所述第一驗證碼、和所述第二驗證碼做為加密運算元，而其目的運算元之內容則為所述的授權碼；所述的解密運算係以所述的授權碼作為來源運算元，而其目的運算元之內容則分別為所述識別碼、所述第一驗證碼、和所述第二驗證碼。

【第12項】 如申請專利範圍第7項所述之方法，其中所述的非接觸方式係一無線射頻通訊方式。

I627511 專利案號：102131146

公告本

104年11月02日 修正

申請日：102/08/29

IPC分類：G06F 21/34 (2013.01)
G06K 19/07 (2006.01)

【發明摘要】

【中文發明名稱】可驗證非接觸性感應標籤之系統及方法

【中文】

一種可驗證非接觸性感應標籤之系統及方法，該系統其具有：一讀取器，用以依一第一動態值產生一第一驗證碼及依一授權碼產生一授權請求；一感應標籤，用以依一非接觸方式獲得該讀取器之所述第一驗證碼，依一第二動態值產生一第二驗證碼，以及依一識別碼、所述的第一驗證碼、及所述的第二驗證碼進行一加密運算以產生所述的授權碼，並將所述的授權碼以所述的非接觸方式傳送至該讀取器；以及一驗證裝置，用以接收該讀取器之所述授權請求，並對所述授權請求進行一解密運算以獲得所述的第一動態值和所述的第二動態值，以判斷該感應標籤是否為真。

【指定代表圖】 第（1）圖。

【代表圖之符號簡單說明】

讀取器 10

第一動態值產生器 11

第一驗證碼產生器 12

讀取請求產生器 13

回應訊號解析器 14

授權請求產生器 15

感應標籤 20

讀取請求解析器 21

第二動態值產生器 22

第二驗證碼產生器 23

識別碼儲存單元 24

授權碼產生器 25

回應訊號產生器 26

驗證裝置 30

授權請求解析器 31

授權碼檢核器 32

第三動態值產生器 33

讀取器驗證器 34

第四動態值產生器 35

感應標籤驗證器 36

驗證結果產生器 37