I686072

(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 I686072 B**

(45)公告日： 中華民國 109 (2020) 年 02 月 21 日

(21)申請案號：106126380 (22)申請日： 中華民國 106 (2017) 年 08 月 04 日

(51)Int. Cl.： ***H04L9/28 (2006.01)***

(71)申請人：財團法人資訊工業策進會 (中華民國) INSTITUTE FOR INFORMATION INDUSTRY (TW)

臺北市大安區和平東路 2 段 106 號 11 樓

(72)發明人：林志達 LIN, CHIH TA (TW) ；高傳凱 KAO, CHUAN KAI (TW)

(74)代理人：陳翠華

(56)參考文獻：

TW	487851	TW	I248276
TW	I311433	TW	I326547
US	8850583B1	US	9043517B1

審查人員：施孝欣

申請專利範圍項數：17 項 圖式數：6 共 36 頁

(54)名稱

傳輸裝置及其傳輸資料保護方法

(57)摘要

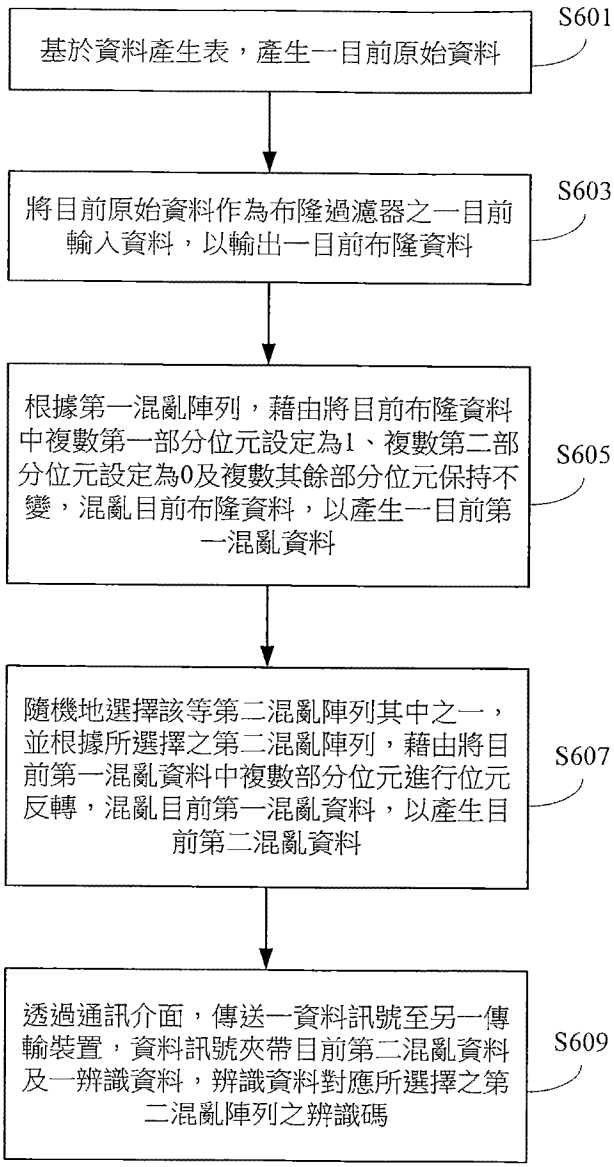
一種傳輸裝置及其傳輸資料保護方法。傳輸裝置儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列及各該第二混亂陣列之一辨識碼。布隆過濾器具有複數獨立雜湊函數。傳輸裝置基於資料產生表，產生一目前原始資料；將目前原始資料作為布隆過濾器之一目前輸入資料，以輸出一目前布隆資料；根據第一混亂陣列，混亂目前布隆資料，以產生一目前第一混亂資料；根據隨機選擇之第二混亂陣列，混亂目前第一混亂資料，以產生目前第二混亂資料；以及傳送夾帶目前第二混亂資料及一辨識資料之一資料訊號至另一傳輸裝置。

A transmission apparatus and transmission data protection method thereof are provided. The transmission apparatus stores a data table, a bloom filter, a first randomization array, a plurality of second randomization arrays and an identifier of each of the second randomized arrays. The bloom filter has a plurality of independent hash functions. The transmission apparatus generates a current original data according to the data table; inputs the current original data to the bloom filter as a current input data of the bloom filter to output a current bloom data; randomizes the current bloom data according to the first randomization array to generate a current first randomized data; randomizes the current first randomized data according to one of the second randomization arrays to generate a current second randomized data; and transmits a data signal carrying the current second randomized data and an identified data to another transmission apparatus.

指定代表圖：

符號簡單說明：

S601-S609・・・步驟



第 6 圖

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

傳輸裝置及其傳輸資料保護方法/ TRANSMISSION APPARATUS, AND TRANSMISSION DATA PROTECTION METHOD THEREOF

【技術領域】

【0001】 本發明係關於傳輸裝置及其傳輸資料保護方法。具體而言，本發明之傳輸裝置藉由輕量化運算方式達到對原始資料進行安全性加工處理。

【先前技術】

【0002】 近年無線通訊技術的快速成長，使得各種無線通訊產品充斥人們的日常生活中，以滿足各種通訊需求及應用。為保護傳輸資料的安全性，這些傳輸資料會先被加密處理後才傳送，例如透過資料加密標準（Data Encryption Standard；DES）演算法或進階加密標準（Advanced Encryption Standard；AES）演算法進行資料加密。然而，在某些具有低傳輸延遲要求的環境中，接收端裝置不但需要及時地接收資料，更需快速地將接收到的資料解密，才能使得使用者或自動化裝置得以及時地作出反應。舉例而言，車聯網中所需傳輸的緊急資訊（例如：危險逼近、交叉路口接近、方向指揮等），由這些緊急資訊具有時效性，若因加解密運算而造成無法及時地被接收端裝置所獲知，則將無法有效地避免交通事故的發生。

【0003】 有鑑於此，本技術領域亟需一種傳輸資料保護機制，縮減對欲傳送資料進行安全性加工處理的時間及對接收資料進行還原處理的時間，以讓具有時效性的資訊得以及時地被接收端裝置所獲知。

【發明內容】

【0004】 本發明之目的在於提供一種傳輸資料保護機制，其藉由布隆過濾器，針對有限範圍之輸入資料或較固定的輸入資料產生具有一對一之輸出資料，並透過兩階段的資料混亂程序，以達到對原始資料進行安全性加工處理之目的，並使得接收端裝置得以完全地將接收資料還原成原始資料。如此一來，本發明之傳輸資料保護機制可有效地縮減對欲傳送資料進行安全性加工處理的時間及對接收資料進行還原處理的時間，以讓具有時效性的資訊得以及時地被接收端裝置所獲知。

【0005】 為達上述目的，本發明揭露一種傳輸裝置，其包含一儲存器、一通訊介面及一處理器。該儲存器用以儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列以及各該第二混亂陣列之一辨識碼。該布隆過濾器具有複數獨立雜湊函數。該處理器，電性連接至該儲存器及該通訊介面，用以執行以下操作：基於該資料產生表，產生一目前原始資料；將該目前原始資料作為該布隆過濾器之一目前輸入資料，以輸出一目前布隆資料；根據該第一混亂陣列，藉由將該目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂該目前布隆資料，以產生一目前第一混亂資料；隨機地選擇該等第二混亂陣列其中之一，並根據所選擇之該第二混亂陣列，藉由將該目前第一混亂資料中複數部分位元進行位元反轉，混亂該目前第一混亂資料，以產生該目前第二混亂資料；以及透過該通訊介面，傳送一資料訊號至另一傳輸裝置，該資料訊號夾帶該目前第二混亂資料及一辨識資料，該辨識資料對應所選擇之該第二混亂陣列之該辨識碼。

【0006】 此外，本發明更揭露一種用於一傳輸裝置之傳輸資料保護方法。該傳輸裝置包含一儲存器、一通訊介面及一處理器。該儲存器儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列以及各該第二混亂陣列之一辨識碼。該布隆過濾器具有複數獨立雜湊函數。該傳輸資料保護方法由該處理器執行且包含下列步驟：基於該資料產生表，產生一目前原始資料；將該目前原始資料作為該布隆過濾器之一目前輸入資料，以輸出一目前布隆資料；根據該第一混亂陣列，藉由將該目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂該目前布隆資料，以產生一目前第一混亂資料；隨機地選擇該等第二混亂陣列其中之一，並根據所選擇之該第二混亂陣列，藉由將該目前第一混亂資料中複數部分位元進行位元反轉，混亂該目前第一混亂資料，以產生該目前第二混亂資料；以及透過該通訊介面，傳送一資料訊號至另一傳輸裝置，該資料訊號夾帶該目前第二混亂資料及一辨識資料，該辨識資料對應所選擇之該第二混亂陣列之該辨識碼。

【0007】 此外，本發明更揭露一種傳輸裝置，其包含一儲存器、一通訊介面及一處理器。該儲存器用以儲存一資料產生表、一布隆過濾器之一輸入輸出表、一第一混亂陣列、一第二混亂陣列及各該第二混亂陣列之一辨識碼。該輸入輸出表紀錄基於該資料產生表所產生之複數原始資料與該布隆過濾器輸出之複數布隆資料，及該等原始資料與該等布隆資料間之一對一關係。該處理器電性連接至該儲存器及該通訊介面，用以執行以下操作：透過該通訊介面自另一傳輸裝置接收一資料訊號，該資料訊號夾帶一目前第二混亂資料及一辨識資料；根據該辨識資料，獲得該等第二混亂陣列其中之

一之該辨識碼；根據所獲得之該辨識碼所對應之該第二混亂陣列，將該第二混亂資料中複數部分位元進行位元反轉，以還原一目前第一混亂資料；根據該第一混亂陣列，比對該目前第一混亂資料與該等布隆資料，以獲得一目前布隆資料，其中該目前第一混亂資料係根據該第一混亂陣列，藉由將該目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂該目前布隆資料而產生；根據該布隆過濾器輸入輸出表，獲得對應至該目前布隆資料之該目前原始資料。

【0008】 在參閱圖式及隨後描述之實施方式後，此技術領域具有通常知識者便可瞭解本發明之其他目的，以及本發明之技術手段及實施態樣。

【圖式簡單說明】

【0009】

第1圖係描繪本發明之傳輸裝置1與傳輸裝置3間之資料傳輸之示意圖；

第2A圖係描繪傳輸裝置1進行資料加工處理之示意圖；

第2B圖係描繪傳輸裝置3進行資料復原處理之示意圖；

第3A圖係本發明之布隆過濾器之循環訓練之示意圖；

第3B圖係本發明之第一混亂陣列之循環訓練之示意圖；

第3C圖係本發明之該等第二混亂陣列之循環訓練之示意圖；

第4圖係為本發明之傳輸裝置1之示意圖；

第5圖係為本發明之傳輸裝置3之示意圖；以及

第6圖係為本發明之傳輸資料保護方法之流程圖。

【實施方式】

【0010】 以下將透過實施例來解釋本發明內容，本發明的實施例並非

用以限制本發明須在如實施例所述之任何特定的環境、應用或特殊方式方能實施。因此，關於實施例之說明僅為闡釋本發明之目的，而非用以限制本發明。需說明者，以下實施例及圖式中，與本發明非直接相關之元件已省略而未繪示，且圖式中各元件間之尺寸關係僅為求容易瞭解，並非用以限制實際比例。

【0011】 本發明第一實施例如第1、2圖所示。第1圖係描繪傳輸裝置1與傳輸裝置3間之資料傳輸。第2A圖係描繪傳輸裝置1進行資料加工處理之示意圖以及第2B圖係描繪傳輸裝置3進行資料復原處理之示意圖。傳輸裝置1及傳輸裝置3可為一伺服器、一基地台、一使用者裝置或任一具有資料產生及傳輸功能之裝置。於本實施例中，假設傳輸裝置1為一基地台以及傳輸裝置3為裝載在一車輛上之使用者裝置。

【0012】 傳輸裝置1係用以根據目前傳輸裝置3所處位置之路況，傳送各種資訊（特別是即時資訊）給傳輸裝置3。舉例而言，即時資訊可為緊急資訊（例如：危險警示、交叉路口接近警示）、導航指示（例如：左轉指示、右轉指示）或操作命令（例如：停止命令、右轉命令、左轉命令）等，但不限於此。傳輸裝置1儲存一資料產生表DT、一布隆過濾器BF、一第一混亂陣列FRA、複數第二混亂陣列SRA1~SRAm（m為一正整數，例如：10）以及各第二混亂陣列SRA1~SRAm之辨識碼ID1~IDm。資料產生表DT係用以產生分別對應前述多種即時資訊之複數原始資料S1~Sn（n為一正整數，例如：30）。

【0013】 須說明者，本發明之資料產生表DT係用以產生有限範圍之原始資料S1~Sn。換言之，資料產生表DT係用以記錄各種資訊所對應之資料

內容（例如：以二進位方式表示）。因此，傳輸裝置1可根據目前傳輸裝置3所處位置之路況，基於資料產生表DT，產生一目前原始資料Sp。

【0014】 為保護目前原始資料Sp傳輸中的安全性，避免被截取、竄改或假造，傳輸裝置1係進一步地對目前原始資料Sp進行資料加工處理，如第2A圖所示。首先，傳輸裝置1將目前原始資料Sp作為布隆過濾器BF之一目前輸入資料，以輸出一目前布隆資料Bp。

【0015】 舉例而言，布隆過濾器BF具有4個獨立雜湊函數H1、H3、H7、H11，以產生256位元之目前布隆資料Bp。換言之，本發明藉由將目前原始資料Sp輸入至布隆過濾器BF，藉由其4個獨立雜湊函數H1、H3、H7、H11分別產生雜湊值h1、h3、h7、h11。隨後，本發明將這4個雜湊值h1、h3、h7、h11（例如：雜湊值h1為3、h3為89、h7為176及h11為211）分別對應至初始值為0之256位元資料中的第3、89、176及211個位元，並將此4個位元設定為1，其餘位元保持為0，以產生目前布隆資料Bp。由於所屬技術領域中具有通常知識者可基於前述說明瞭解本發明之布隆過濾器BF之運作，故在此不再加以贅述。

【0016】 於產生目前布隆資料Bp後，傳輸裝置1根據第一混亂陣列FRA，藉由將目前布隆資料Bp中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂目前布隆資料Bp，以產生一目前第一混亂資料FRSp。舉例而言，第一混亂陣列FRA具有256個欄位FRA(1)~FRA(256)，其分別一對一地對應至256個位元。各欄位FRA(1)~FRA(256)之數值表示所對應之目前布隆資料Bp之位元所對應之位元需設定為1、0或保持不變。假設FRA(i)欄位為1係代表目前布隆資料Bp之

第i個位元將設定為1，FRA(i)欄位為0係代表目前布隆資料Bp之第i個位元將設定為0，FRA(i)欄位為x係代表目前布隆資料Bp之第i個位元將保持不變，其中i=1~256。

【0017】 接著，傳輸裝置1隨機地選擇第二混亂陣列SRA1~SRAm其中之一，並根據所選擇之第二混亂陣列（例如：SRA9），藉由將目前第一混亂資料FRSp中複數部分位元進行位元反轉，混亂目前第一混亂資料FRSp，以產生目前第二混亂資料SRSp。舉例而言，各第二混亂陣列SRA1~SRAm具有256個欄位，其分別一對一地對應至256個位元。以第二混亂陣列SRA9作為說明，各欄位SRA9(1)~SRA9(256)之數值表示所對應之目前第一混亂資料FRSp之位元所對應之位元需進行位元反轉。假設SRA9(i)欄位為1係代表目前第一混亂資料FRSp之第i個位元將反轉以及SRA9(i)欄位為0係代表目前第一混亂資料FRSp之第i個位元將不反轉（即保持不變），i=1~256。

【0018】 需說明者，在一實際運作上，傳輸裝置1可直接將目前第一混亂資料FRSp與第二混亂陣列SRA9進行互斥或（XOR）運算，而獲得目前第二混亂資料SRSp。最後，傳輸裝置1將目前第二混亂資料SRSp及一辨識資料IDD封裝成一資料訊號102，並將資料訊號102傳送至傳輸裝置3。換言之，資料訊號102夾帶該目前第二混亂資料SRSp及一辨識資料IDD。辨識資料IDD對應所選擇之第二混亂陣列SRA9之辨識碼ID9。進一步言，辨識資料IDD可以一明文方式記載所選擇之第二混亂陣列SRA9之辨識碼ID9，或者經由將所選擇之第二混亂陣列SRA9之辨識碼ID9以一雜湊函數計算所產生。

【0019】 傳輸裝置3儲存資料產生表DT、布隆過濾器BF之一輸入輸出表、第一混亂陣列FRA、第二混亂陣列SRA1~SRAm及各第二混亂陣列

SRA1~SRAm之辨識碼ID1~IDm。布隆過濾器BF之輸入輸出表紀錄基於資料產生表DT所產生之原始資料S1~Sn與布隆過濾器BF輸出之布隆資料B1~Bn，及原始資料S1~Sn與布隆資料B1~Bn間之一對一關係。

【0020】 傳輸裝置3自傳輸裝置1接收資料訊號102後，根據辨識資料IDD，獲得第二混亂陣列SRA1~SRAm其中之一之辨識碼（在此，即為第二混亂陣列SRA9之辨識碼ID9）。接著，傳輸裝置3根據所獲得之辨識碼ID9所對應之第二混亂陣列SRA9，將目前第二混亂資料SRSp中複數部分位元進行位元反轉，以還原目前第一混亂資料FRSp。類似地，在一實際運作上，傳輸裝置3可直接將目前第二混亂資料SRSp與第二混亂陣列SRA9進行互斥或（XOR）運算，以還原目前第一混亂資料FRSp。

【0021】 隨後，傳輸裝置3根據第一混亂陣列FRA，比對目前第一混亂資料FRSp與該等布隆資料B1~Bn，以獲得目前布隆資料Bp。舉例而言，傳輸裝置3可基於第一混亂陣列FRA中FRA(i)欄位為x所對應之該等位元（即不會經由第一混亂陣列FRA而改變的該等位元），比對目前第一混亂資料FRSp與該等布隆資料B1~Bn，以獲得複數目前候選布隆資料。接著，傳輸裝置3可將該等目前候選布隆資料經由第一混亂陣列FRA混亂，以獲得複數目前候選第一混亂資料。據此，傳輸裝置3可藉由比對目前第一混亂資料FRSp與該等目前候選第一混亂資料，以自該等目前候選布隆資料中獲得目前布隆資料Bp。

【0022】 再舉例而言，傳輸裝置3亦可儲存第一混亂陣列FRA之一混亂映射表。混亂映射表紀錄布隆過濾器BF之布隆資料B1~Bn與其經第一混亂陣列FRA混亂後之第一混亂資料FRS1~FRSn，及布隆資料B1~Bn與第一

混亂資料FRS1~FRSn間之一對一關係。據此，傳輸裝置3可直接根據第一混亂陣列FRA之混亂映射表，比對目前第一混亂資料FRSp與第一混亂資料FRS1~FRSn，以獲得目前布隆資料Bp。

【0023】 最後，傳輸裝置3根據布隆過濾器輸入輸出表，獲得對應至目前布隆資料Bp之目前原始資料Sp。如此一來，傳輸裝置3可即時因應目前原始資料Sp所表示之資訊作出反應，例如：透過螢幕或揚聲器告知使用者，或自動控制車輛的動作。由上述說明可知，本發明針對有限範圍之輸入資料或較固定的輸入資料產生具有一對一之輸出資料，並透過兩階段的資料混亂程序（第一階段採用固定的混亂序列以及第二階段採用動態選擇的混亂序列），以達到對原始資料進行安全性加工處理之目的，進而讓竊聽者無法利用規律性以破解傳輸資料。此外，透過傳收端裝置與接收端裝置事先交換約定的參數資料（即，布隆過濾器、第一混亂陣列FRA、第二混亂陣列SRA1~SRAm及各第二混亂陣列SRA1~SRAm之辨識碼ID1~IDm），使得接收端裝置得以完全地將接收資料還原成原始資料。

【0024】 本發明第二實施例如第3A-3C圖所示。第3A圖係本發明之布隆過濾器BF之循環訓練之示意圖。第3B圖係本發明之第一混亂陣列FRA之循環訓練之示意圖。第3C圖係本發明之該等第二混亂陣列SRA1~SRAm之循環訓練之示意圖。須說明者，這些循環訓練可事先由具有高運算能力之電腦執行（例如：行動網路業者後端網路之伺服器），再將結果提供給傳輸裝置1及傳輸裝置3，或者當傳輸裝置1本身係具有高處理能力時，可於初始設定階段中執行這些循環訓練，再將結果提供給傳輸裝置3。

【0025】 首先，如第3A圖所示，透過隨機地自複數獨立雜湊函數

H1~Ht（例如：50個雜湊函數，即t=50）中選擇4個獨立雜湊函數Hw、Hx、Hy、Hz（{Hw, Hx, Hy, Hz} ∈ {H1~Ht}）作為布隆過濾器BF的雜湊函數，並將原始資料S1~Sn依序輸入至布隆過濾器BF，以判斷目前所選擇之4個獨立雜湊函數Hw、Hx、Hy、Hz是否可使輸入至布隆過濾器BF之這些不同原始資料S1~Sn具有一對一之不同布隆資料B1~Bn。各布隆資料B1~Bn係為256位元之二進位資料。倘若所產生之布隆資料B1~Bn中有相同的資料，則代表目前所選擇之4個獨立雜湊函數Hw、Hx、Hy、Hz會使得布隆過濾器BF之輸出資料產生碰撞。因此，需在重新隨機地選擇4個獨立雜湊函數Hw、Hx、Hy、Hz作為布隆過濾器BF的雜湊函數，並將原始資料S1~Sn依序再次輸入至布隆過濾器BF及判斷重新所選擇之4個獨立雜湊函數Hw、Hx、Hy、Hz是否可使輸入至布隆過濾器BF之這些不同原始資料S1~Sn具有一對一之不同布隆資料B1~Bn。

【0026】 透過判斷是否發生碰撞而重新隨機地選擇4個獨立雜湊函數Hw、Hx、Hy、Hz並將原始資料S1~Sn依序輸入至布隆過濾器BF這樣的循環訓練，本發明可獲得一組4個獨立雜湊函數Hw、Hx、Hy、Hz（例如：雜湊函數Hw、Hx、Hy、Hz為雜湊函數H1、H3、H7、H11），其可使得輸入至布隆過濾器BF之這些不同原始資料S1~Sn具有一對一之不同布隆資料B1~Bn。換言之，本發明布隆過濾器BF中的4個獨立雜湊函數H1、H3、H7、H11係經前述循環訓練，將基於資料產生表DT所產生之不同原始資料S1~Sn作為布隆過濾器BF之輸入資料，而自t個獨立雜湊函數H1~Ht中選出，以使輸入至布隆過濾器BF之不同原始資料S1~Sn具有一對一之不同布隆資料B1~Bn。

【0027】 於訓練出布隆過濾器BF中的4個獨立雜湊函數而獲得布隆

資料B1~Bn後，本發明進一步地訓練出第一混亂陣列FRA。如第3B圖所示，第一混亂陣列FRA包含複數欄位FRA(1)~FRA(256)，該等欄位FRA(1)~FRA(256)係一對一地對應至各布隆資料B1~Bn之256位元。各欄位FRA(i)之數值表示所對應之位元需設定為1、0或保持不變且各欄位FRA(i)之數值係基於一機率函數獨立地產生。此機率函數使得對應之位元被設為1之一機率等於f1、被設為0之一機率等於f2以及保持不變之一機率等於1-f1-f2。因此，本發明透過經循環訓練，判斷目前所產生之第一混亂陣列FRA是否得以使布隆過濾器輸出之不同布隆資料B1~Bn分別被第一混亂陣列FRA混亂後，具有一對一之複數不同第一混亂資料FRS1~FRSn。

【0028】 類似地，倘若所產生之第一混亂資料FRS1~FRSn中有相同的資料，則代表目前所產生之第一混亂陣列FRA會產生碰撞的第一混亂資料FRS1~FRSn。因此，需在重新產生第一混亂陣列FRA或進一步地調整機率f1、f2，並重新基於新產生之第一混亂陣列FRA混亂布隆資料B1~Bn，來判斷布隆資料B1~Bn分別被新產生之第一混亂陣列FRA混亂後是否已具有一對一之不同第一混亂資料FRS1~FRSn。

【0029】 透過判斷是否發生碰撞而重新產生第一混亂陣列FRA並混亂布隆資料B1~Bn這樣的循環訓練，本發明可獲得一第一混亂陣列FRA，其可使得布隆過濾器輸出之不同布隆資料B1~Bn分別被此第一混亂陣列FRA混亂後，具有一對一之不同第一混亂資料FRS1~FRSn。

【0030】 最後，於訓練出第一混亂陣列FRA而獲得第一混亂資料FRS1~FRSn後，本發明進一步地訓練出複數第二混亂陣列SRA1~SRAm（m為一正整數，例如：10）。如第3C圖所示，各第二混亂陣列SRAj（j=1~m）

對應至辨識碼IDj，且包含複數欄位SRAj(1)~SRAj(256)，該等欄位SRAj(1)~SRAj(256)係一對一地對應至第一混亂資料FRS1~FRSn之256位元。各欄位SRAj(i)之數值表示所對應之位元是否需進行位元反轉且各欄位SRAj(i)之數值係基於一機率函數獨立地產生。此機率函數使得對應之該位元進行位元反轉之一機率等於f以及保持不變之一機率等於1-f。因此，本發明透過經循環訓練，判斷目前所產生之第二混亂陣列SRAj是否得以使第一混亂資料FRS1~FRSn分別被第二混亂陣列SRAj混亂後，具有一對一之複數不同第二混亂資料SRS1~SRSn。

【0031】 類似地，倘若所產生之第二混亂資料SRS1~SRSn中有相同的資料，則代表目前所產生之第二混亂陣列SRAj會產生碰撞的第二混亂資料SRS1~SRSn。因此，需在重新產生第二混亂陣列SRAj或進一步地調整機率f，並重新基於新產生之第二混亂陣列SRAj混亂第一混亂資料FRS1~FRSn，來判斷第一混亂資料FRS1~FRSn分別被新產生之第二混亂陣列SRAj混亂後是否已具有一對一之不同第二混亂資料SRS1~SRSn。

【0032】 透過判斷是否發生碰撞而重新產生第二混亂陣列SRAj並混亂第一混亂資料FRS1~FRSn這樣的循環訓練，本發明可獲得m個第二混亂陣列SRA1~SRAm，其每一者皆可使得第一混亂資料FRS1~FRSn分別被其混亂後，具有一對一之不同第二混亂資料SRS1~SRSn。

【0033】 須說明者，本實施例係以具有4個獨立雜湊函數及產生256位元之二進位資料的布隆過濾器BF作為說明。然而，於其他實施例中，基於實際系統操作的需求，亦可選擇其他數量的獨立雜湊函數及產生其他位元數之二進位資料的布隆過濾器BF。同時，因應布隆過濾器BF產生之不同位

元數之二進位資料，第一混亂陣列FRA及該等第二混亂陣列SRA1~SRAm之欄位數也會因應地改變。由於所屬技術領域中具有通常知識者可基於上述說明可瞭解，如何訓練具有其他數量獨立雜湊函數之布隆過濾器BF及如何相應地訓練第一混亂陣列FRA及第二混亂陣列SRA1~SRAm，故在此不加以贅述。

【0034】 本發明第三實施例請參考第4圖，其係為本發明之傳輸裝置1之示意圖。傳輸裝置1包含一儲存器11、一通訊介面13及一處理器15。通訊介面13可為一有線通訊介面或一無線通訊介面。處理器15電性連接至儲存器11及通訊介面13。須說明者，基於說明簡化之原則，傳輸裝置1之其它元件，例如：天線模組、供電模組等與本發明較不相關的元件，皆於圖中省略而未繪示。

【0035】 儲存器11用以儲存資料產生表DT、布隆過濾器BF、第一混亂陣列FRA、該等第二混亂陣列SRA1~SRAm以及各第二混亂陣列SRA1~SRAm之辨識碼ID1~IDm。如同先前所述，布隆過濾器BF具有多個獨立雜湊函數（例如：4個獨立雜湊函數H1、H3、H7、H11）。處理器15基於資料產生表DT，產生目前原始資料Sp。接著，處理器15將目前原始資料Sp作為布隆過濾器BF之目前輸入資料，以輸出目前布隆資料Bp。

【0036】 隨後，處理器15根據第一混亂陣列FRA，藉由將目前布隆資料Bp中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂目前布隆資料Bp，以產生目前第一混亂資料FRSp。之後，處理器15隨機地選擇該等第二混亂陣列SRA1~SRAm其中之一（例如：SRA9），並根據所選擇之第二混亂陣列SRA9，藉由將目前第一混亂資料

FRSp中複數部分位元進行位元反轉，混亂目前第一混亂資料FRSp，以產生目前第二混亂資料SRSp。

【0037】 最後，處理器15透過通訊介面13，傳送資料訊號102至傳輸裝置3。如同先前所述，資料訊號102夾帶目前第二混亂資料SRSp及辨識資料IDD。辨識資料IDD對應所選擇之第二混亂陣列SRA9之辨識碼ID9。此外，處理器15可以一明文方式將所選擇之第二混亂陣列SRA9之辨識碼ID9記錄於辨識資料IDD中，或者經由將所選擇之第二混亂陣列SRA9之辨識碼ID9以一雜湊函數計算，以將所產生之雜湊值記錄於辨識資料IDD。

【0038】 本發明第四實施例請參考第5圖，其係為本發明之傳輸裝置3之示意圖。傳輸裝置3包含一儲存器31、一通訊介面33及一處理器35。通訊介面33可為一有線通訊介面或一無線通訊介面。處理器35電性連接至儲存器31及通訊介面33。須說明者，基於說明簡化之原則，傳輸裝置3之其它元件，例如：天線模組、供電模組等與本發明較不相關的元件，皆於圖中省略而未繪示。

【0039】 儲存器31用以儲存資料產生表DT、布隆過濾器BF之輸入輸出表、第一混亂陣列FRA、第二混亂陣列SRA1~SRAm以及各第二混亂陣列SRA1~SRAm之辨識碼ID1~IDm。輸入輸出表紀錄基於資料產生表DT所產生之原始資料S1~Sn與布隆過濾器BF輸出之布隆資料B1~Bn，及記錄原始資料S1~Sn與布隆資料B1~Bn間之一對一關係。輸入輸出表可由處理器35自行將原始資料S1~Sn輸入產生布隆過濾器BF所產生，或者自傳輸裝置1或遠端伺服器所獲得，但不限於此。處理器35透過通訊介面33自傳輸裝置1接收資料訊號102。資料訊號102夾帶目前第二混亂資料SRSp及辨識資料IDD。

【0040】 隨後，處理器35根據辨識資料IDD，獲得該等第二混亂陣列SRA1~SRAm其中之一之辨識碼（例如：第二混亂陣列SRA9之辨識碼ID9）。接著，處理器35根據所獲得之辨識碼ID9所對應之第二混亂陣列SRA9，將第二混亂資料SRSp中複數部分位元進行位元反轉，以還原目前第一混亂資料FRSp。之後，處理器35根據第一混亂陣列FRA，比對目前第一混亂資料FRSp與該等布隆資料B1~Bn，以獲得目前布隆資料Bp。

【0041】 在一實施態樣中，處理器35可基於第一混亂陣列FRA中FRA(i)欄位為x所對應之該等位元（即不會經由第一混亂陣列FRA而改變的該等位元），比對目前第一混亂資料FRSp與該等布隆資料B1~Bn，以獲得複數目前候選布隆資料。接著，處理器35可將該等目前候選布隆資料經由第一混亂陣列FRA混亂，以獲得複數目前候選第一混亂資料。據此，處理器35可藉由比對目前第一混亂資料FRSp與該等目前等候選第一混亂資料，以自該等目前候選布隆資料中獲得目前布隆資料Bp。

【0042】 在另一實施態樣中，處理器35可儲存第一混亂陣列FRA之一混亂映射表。混亂映射表紀錄布隆過濾器BF之布隆資料B1~Bn與其經第一混亂陣列FRA混亂後之第一混亂資料FRS1~FRSn，及布隆資料B1~Bn與第一混亂資料FRS1~FRSn間之一對一關係。類似地，混亂映射表可由處理器35自行將布隆資料B1~Bn經由第一混亂陣列FRA混亂後所產生，或者自傳輸裝置1或遠端伺服器所獲得，但不限於此。據此，處理器35可直接根據第一混亂陣列FRA之混亂映射表，比對目前第一混亂資料FRSp與第一混亂資料FRS1~FRSn，以獲得目前布隆資料Bp。

【0043】 於得到目前布隆資料Bp後，處理器35根據布隆過濾器輸入

輸出表，獲得對應至目前布隆資料Bp之目前原始資料Sp。如此一來，處理器35可即時因應目前原始資料Sp所表示之資訊作出反應，例如：致能螢幕或揚聲器告知使用者，或自動控制車輛的動作。

【0044】 本發明第五實施例請參考第6圖，其係為本發明之傳輸資料保護方法之流程圖。傳輸資料保護方法適用於一傳輸裝置，其包含一儲存器、一通訊介面及一處理器。儲存器儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列以及各該第二混亂陣列之一辨識碼。布隆過濾器具有複數獨立雜湊函數。傳輸資料保護方法由處理器執行。

【0045】 首先，於步驟S601中，基於資料產生表，產生一目前原始資料。接著，於步驟S603中，將目前原始資料作為布隆過濾器之一目前輸入資料，以輸出一目前布隆資料。於步驟S605中，根據第一混亂陣列，藉由將目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂目前布隆資料，以產生一目前第一混亂資料。之後，於步驟S607中，隨機地選擇該等第二混亂陣列其中之一，並根據所選擇之第二混亂陣列，藉由將目前第一混亂資料中複數部分位元進行位元反轉，混亂目前第一混亂資料，以產生目前第二混亂資料。最後，於步驟S609中，透過通訊介面，傳送一資料訊號至另一傳輸裝置，資料訊號夾帶目前第二混亂資料及一辨識資料，辨識資料對應所選擇之第二混亂陣列之辨識碼。

【0046】 於其他實施例中，布隆過濾器具有4個獨立雜湊函數，以產生256位元之目前布隆資料。4個獨立雜湊函數可經一循環訓練所產生（如第3A圖所示之布隆過濾器之循環訓練），將根據資料產生表所產生之複數不同

原始資料作為布隆過濾器之複數輸入資料，而自t個獨立雜湊函數中選出，以使輸入至布隆過濾器之該等不同原始資料具有一對一之複數不同布隆資料。

【0047】 此外，於其他實施例中，第一混亂陣列包含複數欄位，該等欄位一對一地對應至目前布隆資料之複數位元，各欄位之一數值表示所對應之目前布隆資料之位元需設定為1、0或保持不變。各欄位之數值係基於一機率函數獨立地產生。機率函數使得對應之位元被設為1之一機率等於f1、被設為0之一機率等於f2以及保持不變之一機率等於1-f1-f2。第一混亂陣列係經一循環訓練決定（如第3B圖所示之第一混亂陣列之循環訓練），以使布隆過濾器輸出之複數不同布隆資料分別被第一混亂陣列混亂後，具有一對一之複數不同第一混亂資料。

【0048】 另外，於其他實施例中，各第二混亂陣列包含複數欄位，該等欄位一對一地對應至目前第一混亂資料之複數位元，各欄位之一數值表示所對應之目前第一混亂資料之位元是否需進行位元反轉。各欄位之數值係基於一機率函數獨立地產生，機率函數使得對應之位元進行位元反轉之一機率等於f以及保持不變之一機率等於1-f。各第二混亂陣列係經一循環訓練決定（如第3C圖所示之第二混亂陣列之循環訓練），以使複數不同第一混亂資料分別被該等第二混亂陣列任一者混亂後，具有一對一之複數不同第二混亂資料。

【0049】 於一實施例中，辨識資料係以一明文方式記載所選擇之第二混亂陣列之辨識碼，或者係經由將所選擇之第二混亂陣列之辨識碼以一雜湊函數計算所產生。

【0050】 除了上述步驟，本實施例之傳輸資料保護方法亦能執行在前述實施例中所闡述之所有操作並具有所有對應之功能。所屬技術領域具有通常知識者可直接瞭解此實施例如何基於前述實施例執行此等操作及具有該等功能，故不贅述。

【0051】 綜上所述，本發明之傳輸資料保護機制藉由輕量化運算方式達到對原始資料進行安全性加工處理，並使得接收端裝置得以完全將接收資料還原成原始資料。如此一來，本發明之傳輸資料保護機制可有效地縮減對欲傳送資料進行安全性加工處理的時間及對接收資料進行還原處理的時間，以讓具有時效性的資訊得以及時地被接收端裝置所獲知。除此之外，本發明之傳輸資料保護機制亦可套用在物聯網（Internet of Things；IoT）資料傳輸，以解決目前IoT資料傳輸多以明文記載方式而缺法隱私保護的問題，同時解決IoT裝置通常不具有高效能處理器以進行複雜的資料加解密的困境。

【0052】 前述之實施例僅用來例舉本發明之實施態樣，以及闡釋本發明之技術特徵，並非用來限制本發明之保護範疇。任何熟悉此技術者可輕易完成之改變或均等性之安排均屬於本發明所主張之範圍，本發明之權利保護範圍應以申請專利範圍為準。

【符號說明】

【0053】

1：傳輸裝置

11：儲存器

13：通訊介面

15：處理器

3：傳輸裝置

31：儲存器

33：通訊介面

35：處理器

102：資料訊號

DT：資料產生表

BF：布隆過濾器

FRA：第一混亂陣列

FRA(1)~ FRA(256)：第一混亂陣列之欄位

FRA(i)：第一混亂陣列之第i個欄位

SRA1~SRAm：第二混亂陣列

SRAj(1)~ SRAj(256)：第j個第二混亂陣列之欄位

SRAj(i)：具有辨識碼IDj之第二混亂陣列之第i個欄位

ID1~IDm：辨識碼

IDD：辨識資料

Sp：目前原始資料

Bp：布隆資料

FRSp：目前第一混亂資料

SRSp：目前第二混亂資料

H1~Ht、Hw、Hx、Hy、Hz：雜湊函數

S1~Sn：原始資料

B1~Bn：布隆資料

h1、h3、h7、h11：雜湊值

FRS1~ FRSn：第一混亂資料

SRS1~ SRSn：第二混亂資料

f、f1、f2：機率

S601-S609：步驟

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

【序列表】(請換頁單獨記載)

公告本

I686072

發明摘要

※ 申請案號：106126380

※ 申請日：106/08/04　　※IPC 分類：H04L 9/28 (2006.01)

【發明名稱】（中文/英文）

傳輸裝置及其傳輸資料保護方法/ TRANSMISSION APPARATUS, AND TRANSMISSION DATA PROTECTION METHOD THEREOF

【中文】

一種傳輸裝置及其傳輸資料保護方法。傳輸裝置儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列及各該第二混亂陣列之一辨識碼。布隆過濾器具有複數獨立雜湊函數。傳輸裝置基於資料產生表，產生一目前原始資料；將目前原始資料作為布隆過濾器之一目前輸入資料，以輸出一目前布隆資料；根據第一混亂陣列，混亂目前布隆資料，以產生一目前第一混亂資料；根據隨機選擇之第二混亂陣列，混亂目前第一混亂資料，以產生目前第二混亂資料；以及傳送夾帶目前第二混亂資料及一辨識資料之一資料訊號至另一傳輸裝置。

【英文】

A transmission apparatus and transmission data protection method thereof are provided. The transmission apparatus stores a data table, a bloom filter, a first randomization array, a plurality of second randomization arrays and an identifier of each of the second randomized arrays. The bloom filter has a plurality of independent hash functions. The transmission apparatus generates a current original data according to the data table; inputs the current original data to the

bloom filter as a current input data of the bloom filter to output a current bloom data; randomizes the current bloom data according to the first randomization array to generate a current first randomized data; randomizes the current first randomized data according to one of the second randomization arrays to generate a current second randomized data; and transmits a data signal carrying the current second randomized data and an identified data to another transmission apparatus.

【代表圖】

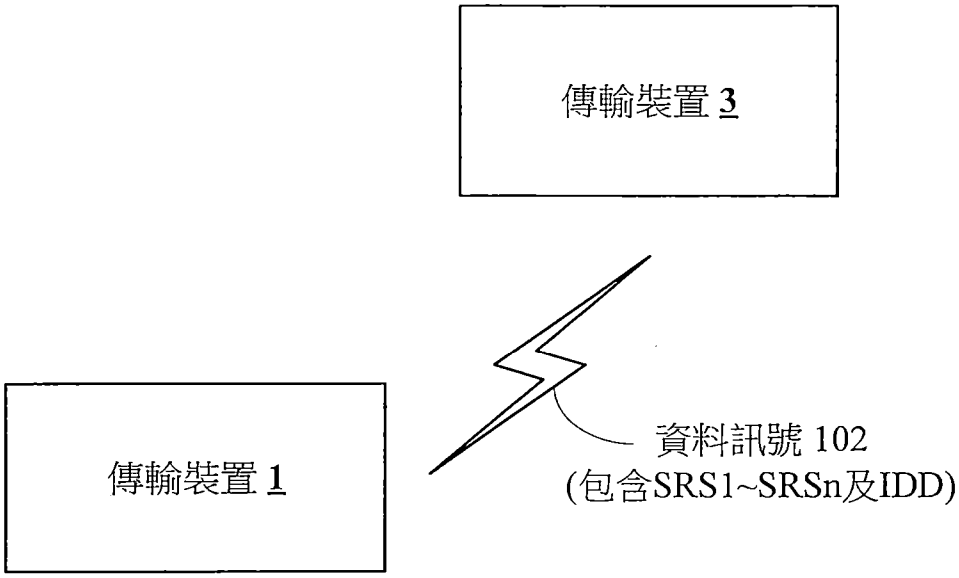
【本案指定代表圖】：第（6）圖。

【本代表圖之符號簡單說明】：

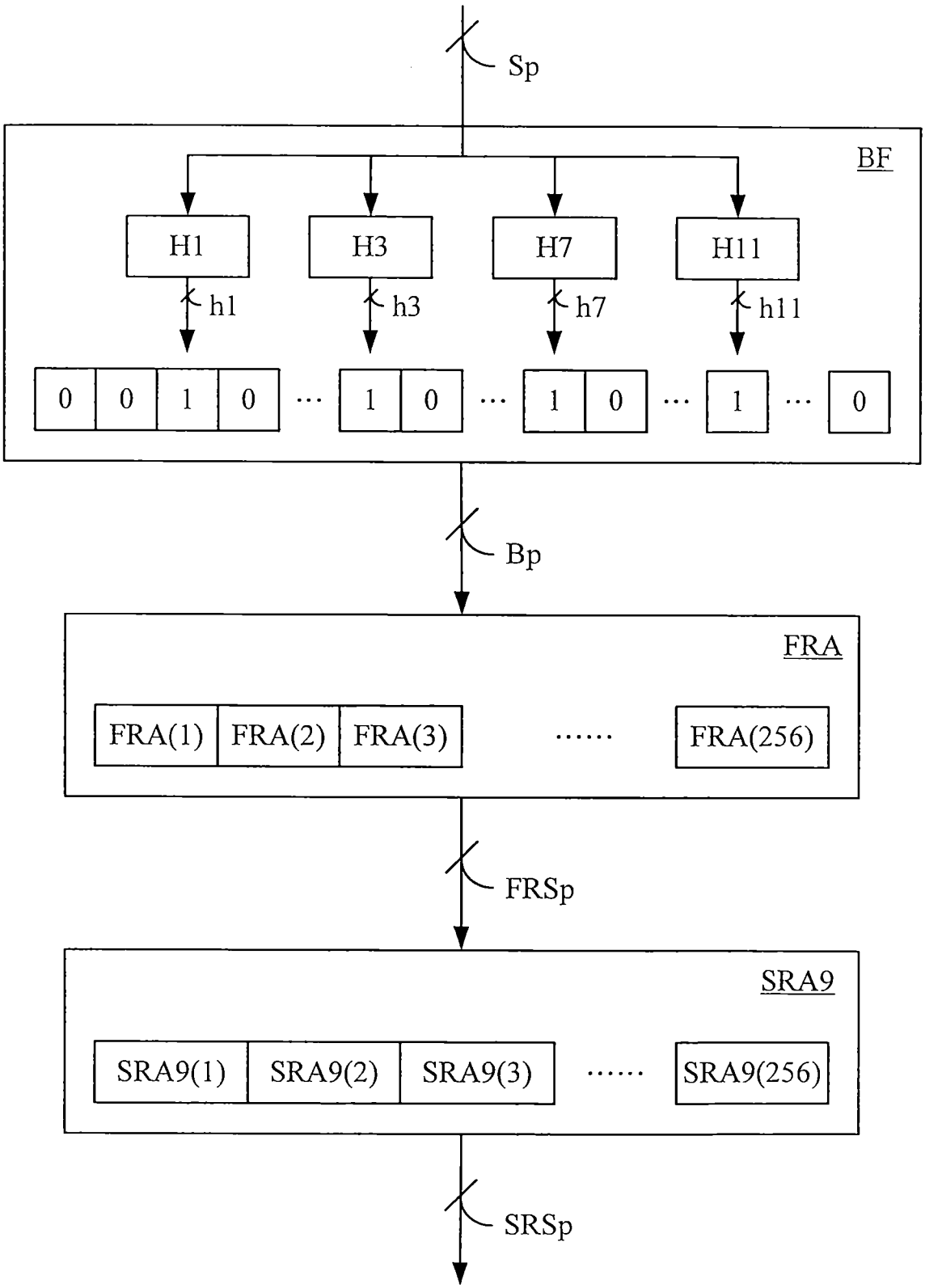
S601-S609：步驟

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

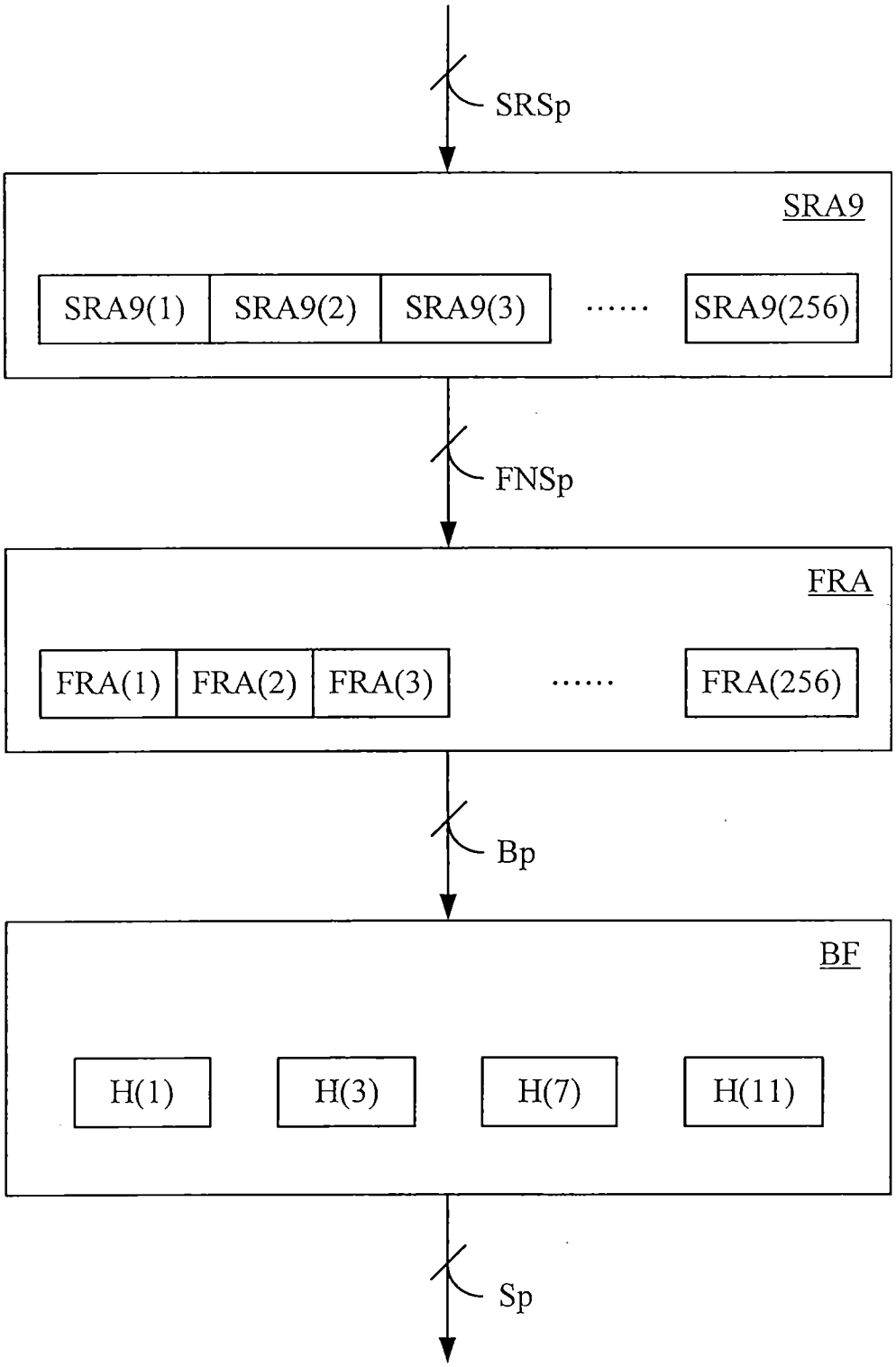
圖式



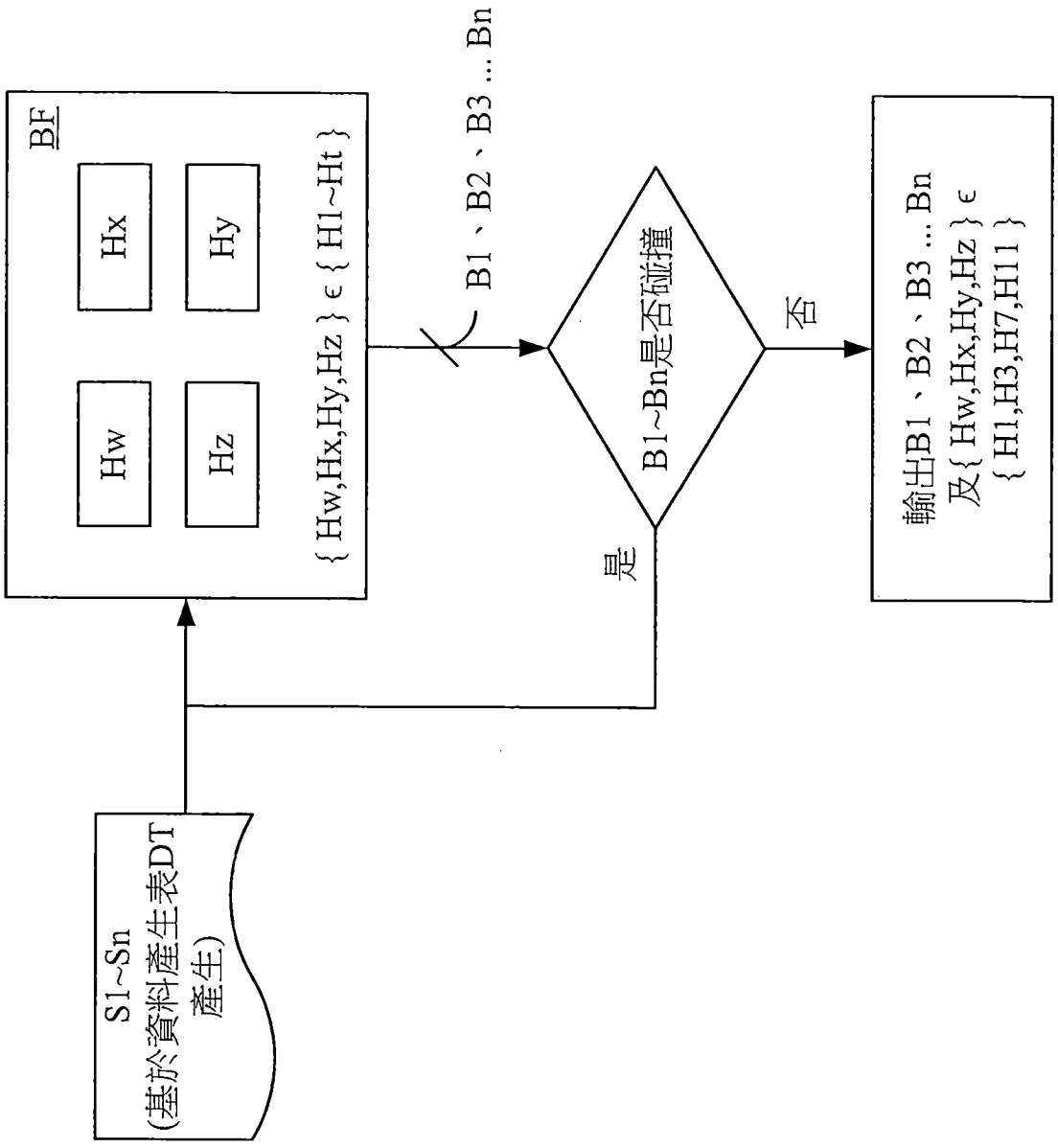
第 1 圖


Sp
BF
H1
H3
H7
H11
h1
h3
h7
h11
0 0 1 0 ··· 1 0 ··· 1 0 ··· 1 ··· 0
Bp
FRA
FRA(1) FRA(2) FRA(3) ····· FRA(256)
FRSp
SRA9
SRA9(1) SRA9(2) SRA9(3) ····· SRA9(256)
SRSp

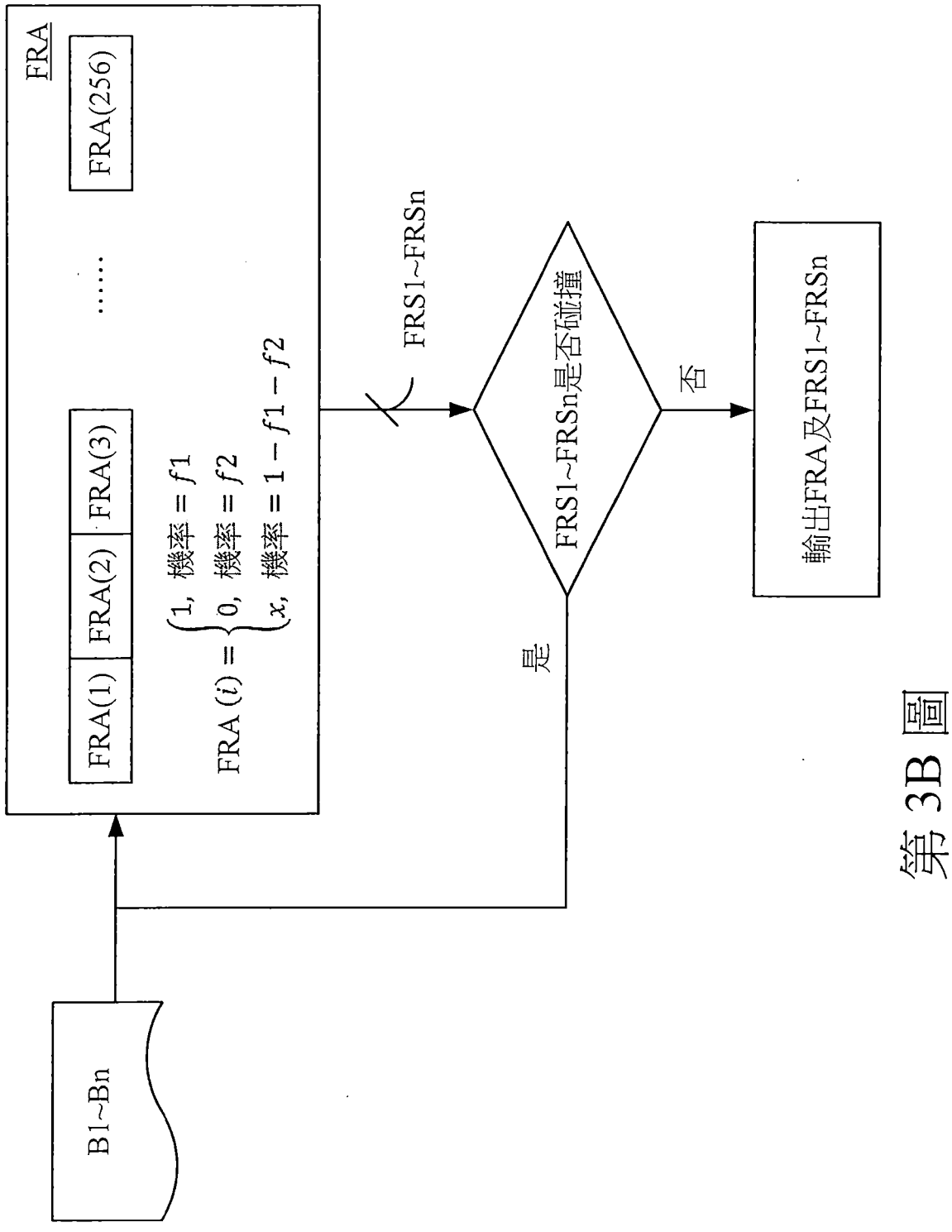
第 2A 圖


SRSp
SRA9
SRA9(1)
SRA9(2)
SRA9(3)
.....
SRA9(256)
FNSp
FRA
FRA(1)
FRA(2)
FRA(3)
.....
FRA(256)
Bp
BF
H(1)
H(3)
H(7)
H(11)
Sp

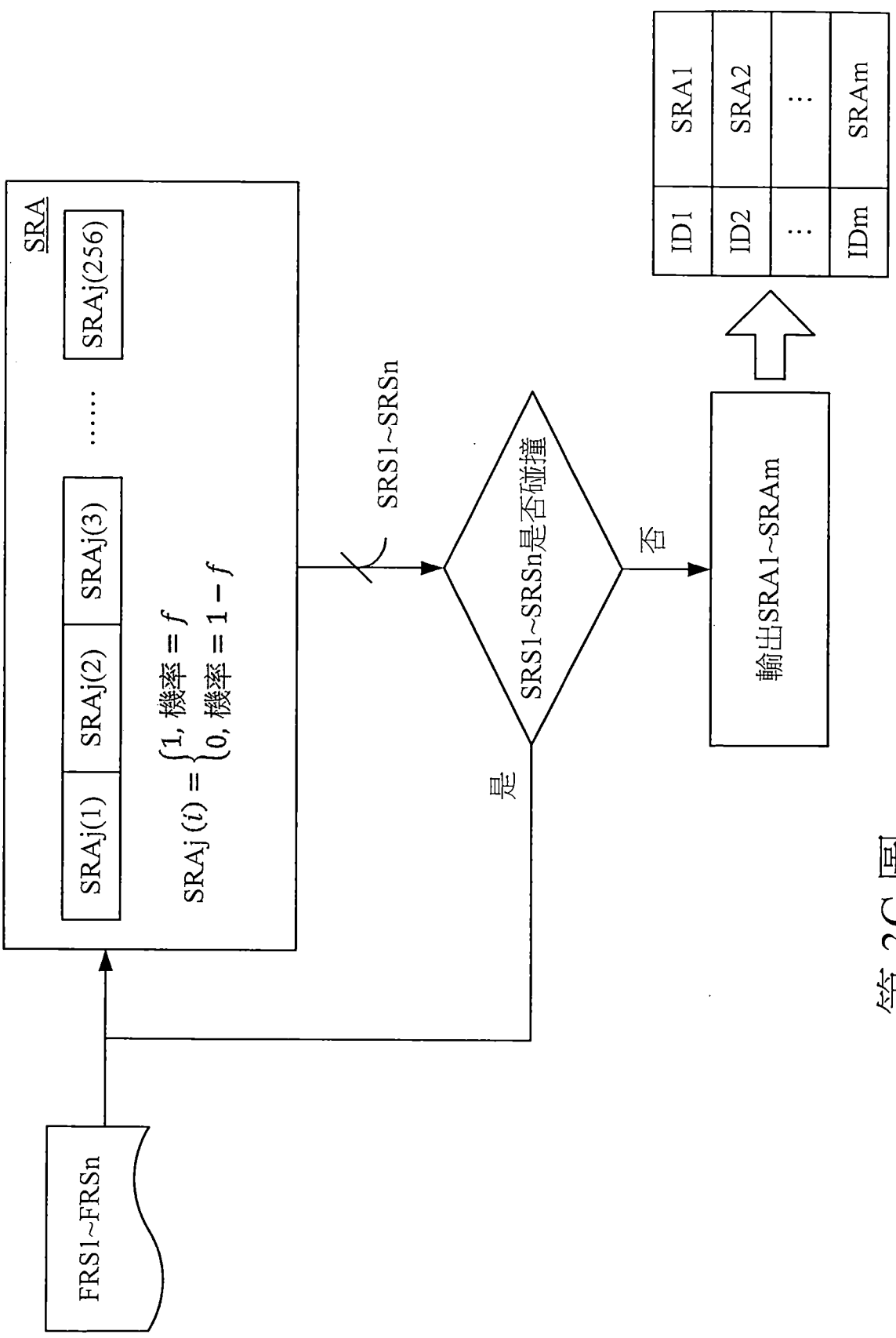
第 2B 圖


S1~Sn
(基於資料產生表DT
產生)
BF
Hw
Hx
Hy
Hz
{ Hw,Hx,Hy,Hz } ∈ { H1~Ht }
B1、B2、B3 ... Bn
B1~Bn是否碰撞
是
否
輸出B1、B2、B3 ... Bn
及{ Hw,Hx,Hy,Hz } ∈
{ H1,H3,H7,H11 }

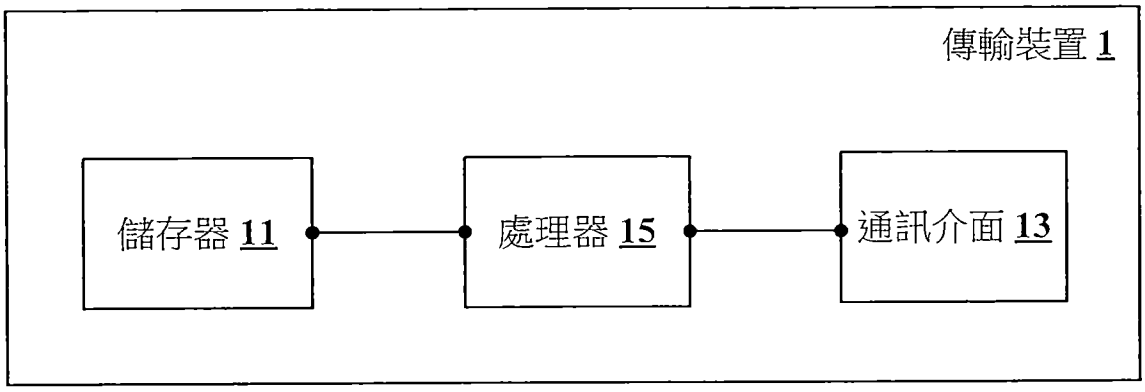
第 3A 圖


B1~Bn
FRA
FRA(1)
FRA(2)
FRA(3)
.....
FRA(256)
FRA (i) = 1, 機率 = f1
0, 機率 = f2
x, 機率 = 1 − f1 − f2
FRS1~FRSn
FRS1~FRSn是否碰撞
是
否
輸出FRA及FRS1~FRSn

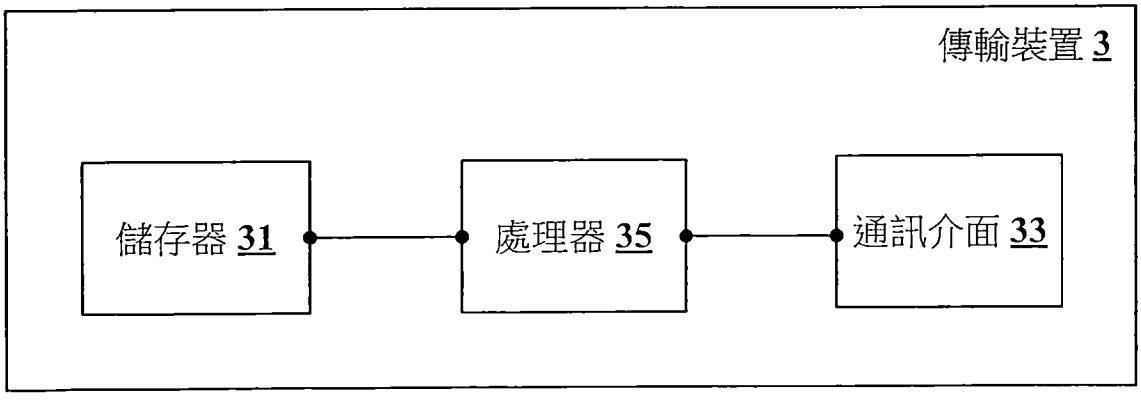
第 3B 圖


FRS1~FRSn
SRA
SRAj(1)
SRAj(2)
SRAj(3)
……
SRAj(256)
SRAj (i) = {1, 機率 = f; 0, 機率 = 1 − f}
SRS1~SRSn
SRS1~SRSn是否碰撞
是
否
輸出SRA1~SRAm
ID1
SRA1
ID2
SRA2
IDm
SRAm

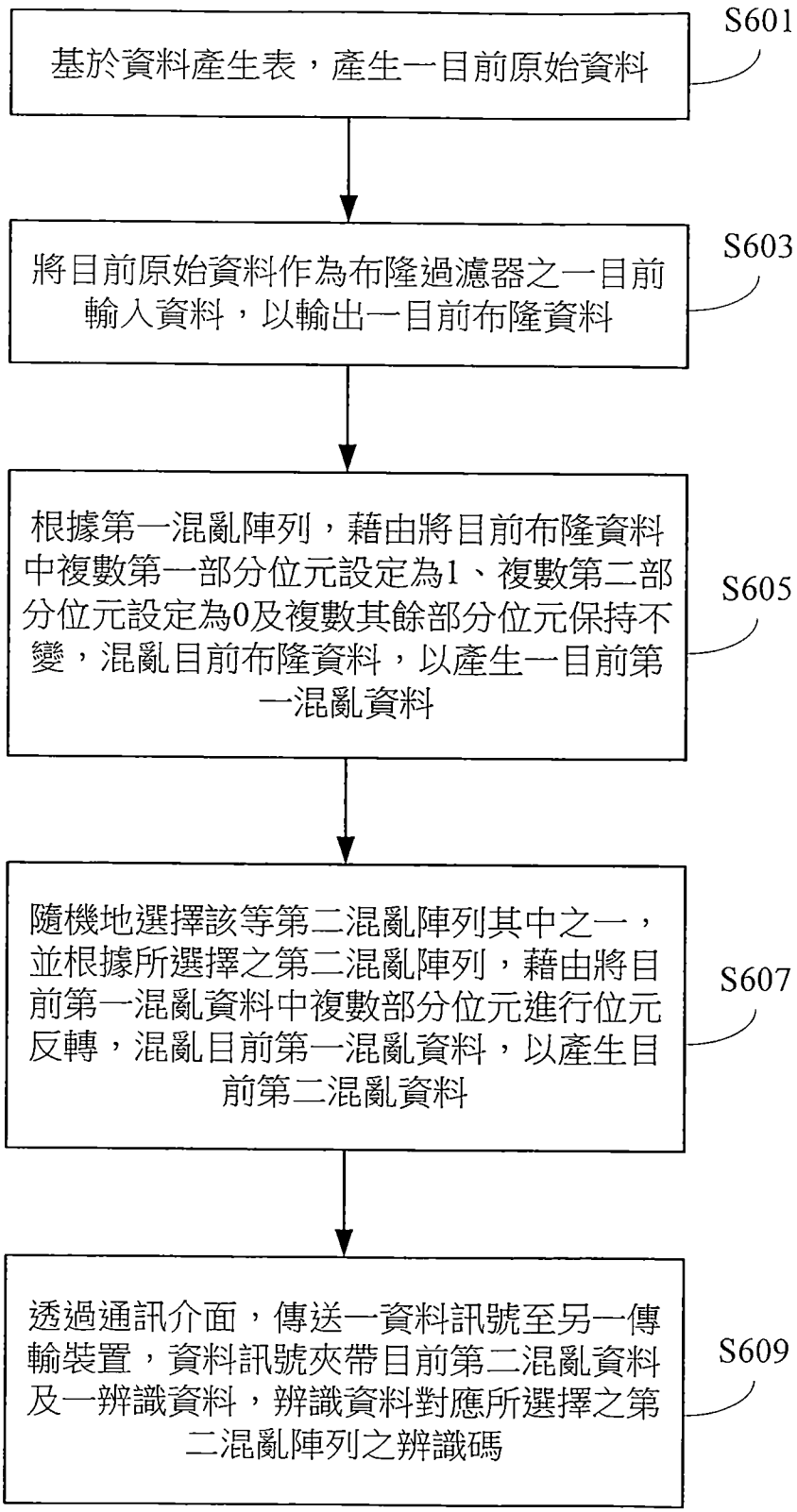
第 3C 圖



第 4 圖



第 5 圖


S601
基於資料產生表，產生一目前原始資料
S603
將目前原始資料作為布隆過濾器之一目前輸入資料，以輸出一目前布隆資料
S605
根據第一混亂陣列，藉由將目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂目前布隆資料，以產生一目前第一混亂資料
S607
隨機地選擇該等第二混亂陣列其中之一，並根據所選擇之第二混亂陣列，藉由將目前第一混亂資料中複數部分位元進行位元反轉，混亂目前第一混亂資料，以產生目前第二混亂資料
S609
透過通訊介面，傳送一資料訊號至另一傳輸裝置，資料訊號夾帶目前第二混亂資料及一辨識資料，辨識資料對應所選擇之第二混亂陣列之辨識碼

第 6 圖

第 106126380 號專利申請案
申請專利範圍替換本（108 年 12 月）

申請專利範圍

1. 一種傳輸裝置，包含：

一儲存器，用以儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列以及各該第二混亂陣列之一辨識碼，該布隆過濾器具有複數獨立雜湊函數，該等獨立雜湊函數使輸入至該布隆過濾器之複數不同原始資料具有一對一之複數不同布隆資料；

一通訊介面；以及

一處理器，電性連接至該儲存器及該通訊介面，用以執行以下操作：

基於該資料產生表，產生一目前原始資料；

將該目前原始資料作為該布隆過濾器之一目前輸入資料，以輸出一目前布隆資料；

根據該第一混亂陣列，藉由將該目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂該目前布隆資料，以產生一目前第一混亂資料；

隨機地選擇該等第二混亂陣列其中之一，並根據所選擇之該第二混亂陣列，藉由將該目前第一混亂資料中複數部分位元進行位元反轉，混亂該目前第一混亂資料，以產生該目前第二混亂資料；以及

透過該通訊介面，傳送一資料訊號至另一傳輸裝置，該資料訊號夾帶該目前第二混亂資料及一辨識資料，該辨識資料對應所選擇之該第二混亂陣列之該辨識碼。

2. 如請求項1所述之傳輸裝置，其中該布隆過濾器具有4個獨立雜湊函數，以產生256位元之該目前布隆資料。

第 106126380 號專利申請案
申請專利範圍替換本（108 年 12 月）

3. 如請求項2所述之傳輸裝置，其中該4個獨立雜湊函數係經一循環訓練，將根據該資料產生表所產生之該等不同原始資料作為該布隆過濾器之複數輸入資料，而自t個獨立雜湊函數中選出。

4. 如請求項1所述之傳輸裝置，其中該第一混亂陣列包含複數欄位，該等欄位一對一地對應至該目前布隆資料之複數位元，各該欄位之一數值表示所對應之該目前布隆資料之該位元需設定為1、0或保持不變，各該欄位之該數值係基於一機率函數獨立地產生，該機率函數使得對應之該位元被設為1之一機率等於f1、被設為0之一機率等於f2以及保持不變之一機率等於1-f1-f2，以及該第一混亂陣列係經一循環訓練決定，以使該布隆過濾器輸出之該等不同布隆資料分別被該第一混亂陣列混亂後，具有一對一之複數不同第一混亂資料。

5. 如請求項1所述之傳輸裝置，其中各該第二混亂陣列包含複數欄位，該等欄位一對一地對應至該目前第一混亂資料之複數位元，各該欄位之一數值表示所對應之該目前第一混亂資料之該位元是否需進行位元反轉，各該欄位之該數值係基於一機率函數獨立地產生，該機率函數使得對應之該位元進行位元反轉之一機率等於f以及保持不變之一機率等於1-f，以及各該第二混亂陣列係經一循環訓練決定，以使複數不同第一混亂資料分別被該等第二混亂陣列任一者混亂後，具有一對一之複數不同第二混亂資料。

6. 如請求項1所述之傳輸裝置，其中該辨識資料係以一明文方式記載所選擇之該第二混亂陣列之該辨識碼。

7. 如請求項1所述之傳輸裝置，其中該辨識資料係經由將所選擇之該第二混

亂陣列之該辨識碼以一雜湊函數計算所產生。

8. 一種用於一傳輸裝置之傳輸資料保護方法，該傳輸裝置包含一儲存器、一通訊介面及一處理器，該儲存器儲存一資料產生表、一布隆過濾器、一第一混亂陣列、複數第二混亂陣列以及各該第二混亂陣列之一辨識碼，該布隆過濾器具有複數獨立雜湊函數，該等獨立雜湊函數使輸入至該布隆過濾器之複數不同原始資料具有一對一之複數不同布隆資料，該傳輸資料保護方法由該處理器執行且包含下列步驟：

基於該資料產生表，產生一目前原始資料；

將該目前原始資料作為該布隆過濾器之一目前輸入資料，以輸出一目前布隆資料；

根據該第一混亂陣列，藉由將該目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂該目前布隆資料，以產生一目前第一混亂資料；

隨機地選擇該等第二混亂陣列其中之一，並根據所選擇之該第二混亂陣列，藉由將該目前第一混亂資料中複數部分位元進行位元反轉，混亂該目前第一混亂資料，以產生該目前第二混亂資料；以及

透過該通訊介面，傳送一資料訊號至另一傳輸裝置，該資料訊號夾帶該目前第二混亂資料及一辨識資料，該辨識資料對應所選擇之該第二混亂陣列之該辨識碼。

9. 如請求項8所述之傳輸資料保護方法，其中該布隆過濾器具有4個獨立雜湊函數，以產生256位元之該目前布隆資料。

10. 如請求項9所述之傳輸資料保護方法，其中該4個獨立雜湊函數係經一循

環訓練，將根據該資料產生表所產生之該等不同原始資料作為該布隆過濾器之複數輸入資料，而自t個獨立雜湊函數中選出。

11.如請求項8所述之傳輸資料保護方法，其中該第一混亂陣列包含複數欄位，該等欄位一對一地對應至該目前布隆資料之複數位元，各該欄位之一數值表示所對應之該目前布隆資料之該位元需設定為1、0或保持不變，各該欄位之該數值係基於一機率函數獨立地產生，該機率函數使得對應之該位元被設為1之一機率等於f1、被設為0之一機率等於f2以及保持不變之一機率等於1-f1-f2，以及該第一混亂陣列係經一循環訓練決定，以使該布隆過濾器輸出之該等不同布隆資料分別被該第一混亂陣列混亂後，具有一對一之複數不同第一混亂資料。

12.如請求項8所述之傳輸資料保護方法，其中各該第二混亂陣列包含複數欄位，該等欄位一對一地對應至該目前第一混亂資料之複數位元，各該欄位之一數值表示所對應之該目前第一混亂資料之該位元是否需進行位元反轉，各該欄位之該數值係基於一機率函數獨立地產生，該機率函數使得對應之該位元進行位元反轉之一機率等於f以及保持不變之一機率等於1-f，以及各該第二混亂陣列係經一循環訓練決定，以使複數不同第一混亂資料分別被該等第二混亂陣列任一者混亂後，具有一對一之複數不同第二混亂資料。

13.如請求項8所述之傳輸資料保護方法，其中該辨識資料係以一明文方式記載所選擇之該第二混亂陣列之該辨識碼。

14.如請求項8所述之傳輸資料保護方法，其中該辨識資料係經由將所選擇之該第二混亂陣列之該辨識碼以一雜湊函數計算所產生。

15.一種傳輸裝置，包含：

一儲存器，用以儲存一資料產生表、一布隆過濾器之一輸入輸出表、一第一混亂陣列、複數第二混亂陣列及各該第二混亂陣列之一辨識碼，該輸入輸出表紀錄基於該資料產生表所產生之複數原始資料與該布隆過濾器輸出之複數布隆資料及該等原始資料與該等布隆資料間之一對一關係；

一通訊介面；以及

一處理器，電性連接至該儲存器及該通訊介面，用以執行以下操作：

透過該通訊介面自另一傳輸裝置接收一資料訊號，該資料訊號夾帶一目前第二混亂資料及一辨識資料；

根據該辨識資料，獲得該等第二混亂陣列其中之一之該辨識碼；

根據所獲得之該辨識碼所對應之該第二混亂陣列，將該目前第二混亂資料中複數部分位元進行位元反轉，以還原一目前第一混亂資料；

根據該第一混亂陣列，比對該目前第一混亂資料與該等布隆資料，以獲得一目前布隆資料，其中該目前第一混亂資料係根據該第一混亂陣列，藉由將該目前布隆資料中複數第一部分位元設定為1、複數第二部分位元設定為0及複數其餘部分位元保持不變，混亂該目前布隆資料而產生；以及

根據該布隆過濾器輸入輸出表，獲得對應至該目前布隆資料之該目前原始資料。

16.如請求項15所述之傳輸裝置，其中當該處理器根據該第一混亂陣列，比對該第一混亂資料與該等布隆資料，而獲得複數目前候選布隆資料時，

該處理器更將該等目前候選布隆資料經由該第一混亂陣列混亂，以產生複數目前候選第一混亂資料，以及該處理器更比對該目前第一混亂資料與該等目前候選第一混亂資料，以自該等目前候選布隆資料中獲得該目前布隆資料。

17.如請求項15述之傳輸裝置，其中該儲存器更儲存該第一混亂陣列之一混亂映射表，該混亂映射表紀錄該布隆過濾器之該等布隆資料與其經第一混亂陣列混亂後之複數第一混亂資料，及該等布隆資料與該等第一混亂資料間之一對一關係，以及該處理器根據該第一混亂陣列之該混亂映射表，比對該目前第一混亂資料與該等第一混亂資料，以獲得該目前布隆資料。