

發明專利說明書

(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：

P513P08P

※ 申請日期：

96. 2. 13
95. 10. 24

※IPC 分類：

H04N 7/16

(2006.01)

一、發明名稱：(中文/英文)

加擾與解擾資料單元的方法 / METHODS OF SCRAMBLING
AND DESCRAMBLING UNITS OF DATA

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

伊達圖亞瑟士貝威公司 / IRDETO ACCESS B.V.

代表人：(中文/英文) 艾倫 費亞佛 / ALLEN PHEIFFER

住居所或營業所地址：(中文/英文)

荷蘭 霍夫德普 吉彼特街 42 號

JUPITERSTRAAT 42 NL-2132 HD HOOFFDORP THE NETHERLANDS

國 籍：(中文/英文) 荷蘭 / NL

三、發明人：(共 1 人)

姓 名：(中文/英文)

泛帝文 安東尼 約哈耐 彼特盧斯 瑪利亞

VAN ED VEN, ANTONIUS, JOHANNES, PETRUS MARIA

國 籍：(中文/英文)

荷蘭 / NL

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

歐盟(EPC)、2005/11/08、EP 05110495.8

本案優先權之主張應不予受理

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：
無

九、發明說明：

【發明所屬之技術領域】

本發明係關於加擾與解擾一資料流的方法，更確切地說，
本發明係關於以加擾與解擾一資料流的系統而執行加擾與解
擾一資料流的方法。

【先前技術】

在國際申請號 WO 95/10906 的說明書中獲知，在習知的方法中，劃分數位資料為 N 個區塊的封包，即 $X(1)$ 、 $X(2) \dots X(N)$ ，其中每一區塊具有 $2m$ 位元，在編碼操作之前反向區塊的序列為 $X(N)$ 、 $X(N-1) \dots X(1)$ ，此區塊的序列為以下列方式藉編碼演算法 E 而編碼(其中 $\wedge$ 是用以表示互斥或/XOR 運算子)：

$$Y(1) = E[X(N) \wedge IV]$$

$$Y(i) = E[X(N-i+1) \wedge Y(i-1)] \quad \text{對於 } i > 1 \text{ 且 } i \leq N$$

再一次反向該些已編碼區塊的序列，以致該序列 $Y(N)$ 、 $Y(N-1)\dots Y(1)$ 被傳送至該接收器。

在接收器側，藉由如下的解碼運算法 D 可獲得該初始資料區塊：

$$X(i) = D[Y(N-1+i) \wedge Y(N-i)] \quad \text{對於 } i = 1, 2, \dots, N-1$$

$$X(N) = D[Y(1)] \wedge IV$$

此運用在習知系統的方法即為反向密碼區塊鏈或 RCBC 方法，其優點為需要在接收器處的緩衝器儲存以儲存僅兩個資料區塊。

習知方法與系統的一問題為需要在發送者側設立有用於儲存 N 區塊之容量的緩衝器，以便施行區塊之序列的反向，如此對於用於資料傳輸且具有許多已編碼資料發送者之系統來說，或對需要具有資料的發送者與接收者之功能的裝置來說，係為一大問題。

【發明內容】

本發明係關於加擾一資料流的方法，其包括獲得來自串流一連串資料區塊的第一序列，

在每一區塊的第一序列中反向區塊的順序，以形成對應的資料區塊之第二序列，以及

在區塊的每一第二序列中於區塊鏈接模式使用一密碼而編碼該些區塊，該區塊鏈接模式係以用於每一區塊的第二序列之對應的初始化向量而初始化。

本發明亦關於加擾一資料流的系統，其包括

用以接收一連串資料區塊的第一序列的資料流之一輸入，多個暫存器以及至少一在每一第一序列之資料區塊中用於反向該些區塊之順序的邏輯單元，以形成對應的第二序列之資料區塊，以及

在每一區塊之第一序列中於區塊鏈接模式使用一密碼用於編碼該些區塊之處理配置，該區塊鏈接模式係以用於每一區塊之第二序列的對應的初始化向量而初始化。

本發明亦相關於解擾已加擾的一資料流的方法，而形成一資料流，其包括

自己加擾資料之資料流中獲得區塊之一序列的已加擾資料，以及

使用區塊之一相關序列的已解擾資料，解擾區塊之每一序列的已加擾資料，其中，藉在一反向鏈接模式使用一解碼密碼，以解擾區塊之一序列的已加擾資料，

藉應用該解碼密碼至在已加擾資料之區塊的相關序列中之最末區塊，且應用具有如同至少解碼密碼與初始化向量之運算元的一運算子，獲得在已解碼資料之區塊的該序列的一最末

區塊。並且其中在已解擾資料的區塊之序列中之先於最後區塊的每一區塊係藉由應用具有如同至少解碼密碼的結果與在已加擾資料之該區塊的序列中之一區塊的已加擾資料之下一位置的運算元的一運算子而獲得。

本發明亦關於用於解擾一已加擾資料之資料流的系統，而形成一資料流，包括

用以接收如同一連串的已加擾資料之多個區塊的序列之已加擾資料的資料流的一輸入，以及

用於解擾已加擾資料之區塊的每一序列之處理配置，以形成相關之已解擾資料多區塊的序列，其中，藉在一反向鏈接模式使用一解碼密碼，以解擾已加擾資料的多區塊之一序列，

藉應用該解碼密碼至在已加擾資料之區塊中的相關序列之最末區塊，且應用具有如同至少解碼密碼與初始化向量之運算元的一運算子，獲得在區塊之該序列的已解碼資料的一最末區塊。並且其中在區塊之序列的已解擾資料中之先於最後區塊的每一區塊係藉由應用具有如同至少解碼密碼的結果與在區塊的該序列之已加擾資料中之已加擾資料的一區塊之下一位置的運算元的一運算子而獲得。

本發明亦關於用於收發資料的設備。

本發明亦關於一電腦程式。

本發明之一目的在於提供方法、系統與裝置以及各種型態的電腦程式，該些電腦程式係用以使得在提供可接收程度的內容保護時，起始段落可更有效率地施行。

此目的可依據本發明藉由加擾一資料流而達成，其特徵為，對於包括在資料流的資料單元之一連串區塊的第一序列，依據至少在先前單元的區塊之第一序列之前的一區塊，產生至少一用於在單元中編碼自區塊的第一序列形成之區塊的第二序列之對應的初始化向量。

由於資料單元包括一連串第一序列的區塊，每一第一序列的區塊係以較少的區塊形成，意指需要較少的緩衝儲存以反向區塊的順序，此對於一可接受的安全性程度來說是可能的，因至少區塊的第二序列中之兩者為有效地鏈接。此鏈接是緣於至少一初始化向量的事實，即在最大化安全性需要除了第一個以外的每一個，以產生用於編碼形成自第一序列的區塊之第二序列的區塊的至少一初始化向量，依據至少在先前單元的區塊之第一序列之前的一區塊。

在一實施例中，依據在同樣的第一序列中之最後區塊前的至少一資料的區塊，產生在形成自第一序列的區塊之每一第二序列的區塊中用於編碼區塊對應的初始化向量。

此將在初始化向量中產生增大的差異，即便使用具有高度特殊性的初始化向量，在一單元中加擾第一序列的區塊之接下

來的區塊。依據於相同的第一序列在最後區塊之前至少一資料的區塊，藉產生初始化向量，而確保差異性。在解擾器需要初始化向量之前的解擾期間，據以生成初始化向量的該一或多個資料區塊係可獲致的。故達成用於在包括於單元中之第一序列之接續的每一第一序列之初始化向量的特殊性，其具有相對地高可攜性，而不需要在接收器對每一第一序列提供一個新的初始化向量。

● 在一實施例中，在單元中形成來自區塊的第一序列之每一用於編碼第二序列區塊的初始化向量係依據於單元中在每一任一先前的第一序列的區塊之至少一區塊而產生。

故，最大化第二序列間的鏈接，其中，接續包括在第一序列在無先前獲致在區塊的第一序列前的所有的情況下，很清楚地無法獲得第一序列之資料區塊。

包括接收資料封包的實施例包括一標頭與一封包內容，其中該單元係由該封包內容形成。

● 此實施例為具有相當多的優點，因為可加擾封包內容而無須事先緩衝。

在一實施例中，密碼為設置以操作在上預設大小之基本區塊的一區塊密碼，其中在至少資料的第二序列之區塊的大小係對應於該基本區塊大小。

在一實施例中，假使單元藉連串的第一序列的區塊所組成，且資料的接續數量在大小上相等於或少於多重的基礎區塊的大小，

擴大資料的數量至等同於多重基礎區塊的大小之大小，以形成至少兩個區塊的第一末序列，

交換區塊的第一末序列之該最後兩個區塊，且反向在區塊之第一端序列的區塊之順序，以形成資料區塊的第二端序列，

在區塊鏈接模式中於區塊使用密碼，而編碼在區塊的第二端序列中的區塊，此些區塊係藉由初始化向量而初始化，該些初始化向量係在單元之區塊的第一序列之前依據至少一區塊而生成。

故，上述方法係用以施行密文盜用(ciphertext stealing)的形式，此為確保加擾整個單元之一相當安全的方式，除此之外，其允許使用形成自預設數目的區塊之第一序列，以加擾該單元的第一部分。

在一實施例中，如果在資料流中的下一單元係由零或更多預設數目的區塊之第一序列，以及等同於小於基礎區塊的大小之資料數目所組成，

資料的數量係充填至等同於基礎區塊之大小的大小，以形成一最末區塊，

在區塊鏈結模式中使用該密碼，以編碼該最末區塊。該區域鏈結模式係依據一初始化向量而初始化，該初始化向量係依據在單元的區塊之第一序列之前的至少一區塊而生成。

因此，很清楚地不需要傳輸資料的達成數量，即便其小於用以配置密碼的基礎區塊的大小。

在實施例的變形中，在基於獨立於任何區塊的至少一向量的向量上，在任何單元的區塊之第一序列之前。藉由執行密碼操作而產生初始化向量，較佳地為相反於密碼的解碼。

所造成的影響為在先前單元中使用與產生用於資料之加擾區塊的初始化向量之相同的向量，而達成初始化向量的變形。故，在安全性相當良好的同時，較少向量需傳輸至解擾器。使用相反於密碼的解碼具有使用係由該解擾器之硬體及/或軟體架構所組成的效果，該解擾器已呈現於編碼用途上。

根據本發明之另一目的，根據本發明之用以加擾一資料流的系統其特徵在於，該系統係配置以在該資料流中用於包括於一資料單元中之一連串的區塊的第一序列，以在單元中產生用於編碼形成自區塊的第一序列之區塊的第二序列之至少一初始化向量，其係依據在單元的區塊的第一序列之前的至少一區塊。

此系統因其效率良好故很適合包括在設定的編碼處理器中。

較佳地，配置此系統以執行本發明之一方法。

根據本發明之另一目的，解擾已加擾之資料流的方法之特徵在於，用於在已加擾資料的資料流中的資料單元中的一連串已加擾資料的序列，用於解擾已加擾資料的區塊之序列的至少一初始化向量係依據至少一以解擾資料的區塊而產生。該區塊係藉由解擾單元之已加擾資料的區塊之先前序列，在以解擾資料的區塊之序列中獲致。

根據本發明，適宜用於解擾已加擾資料的資料流的方法係藉施加機擾一資料流的方法而獲致，因為接續的區塊的序列係分別地且依序地解擾，假使序列中的區塊沒有依序地被接收也沒有關係(例如以相反的順序)。由於序列係短於序列的整體接續。因為用於解擾已加擾資料的區塊之序列的至少一初始化向量係依據至少一已解擾資料的區塊而產生。該區塊係藉由解擾單元之已加擾資料的區塊之先前序列，在以解擾資料的區塊之序列中獲致，故至少鏈結兩個已加擾資料的區塊之序列，使得錯誤的解擾更形困難。

在一實施例中，對應的用於解擾已加擾資料的區塊之序列的初始化向量係依據由施加解碼密碼至在相同序列中接續已加擾資料的區塊再已加擾資料的最末區塊之區塊所獲致的至少一資料區塊，且由施加具有利如運算元的至少為該解碼密碼

的結果以及在已加擾資料的區塊之相同序列中的下一位置已加擾資料的區塊之運算子。

其具有的優點為許多單元的資料流並不需要許多初始化向量的傳輸以自加擾器傳輸到解擾器，以達成在初始化向量中的足夠的變形。

在一實施例中，在單元中用於解擾已加擾資料的區塊之序列的每一初始化向量係依據至少一已解擾資料的區塊而產生。該已解擾資料資料的區塊係自每一任何已解擾資料的區塊之每一序列藉在單元中解擾一先前已加擾資料的區塊的序列而獲致。

因此，包括在單元中可有效地鏈接接下來的所有序列。

一實施例包括接收包含標頭與封包內容的一資料封包，其中該單元係藉封包內容而形成。

在一實施例中，解碼密碼為一區塊密碼，其設置以操作於預設大小的基礎區塊上，其中該區塊在已加擾之區塊的序列中具有對應於基礎區塊大小之大小。

在一實施例中，假使單元為由接下來的已加擾資料的區塊之序列以及一相等於多重基礎區塊大小之大小的資料的充填數量，以及部分的基礎區塊大小所組成。

已解擾資料的區塊之末端序列之最末個為藉施加解碼密碼至一區塊而形成，該區塊恰好係於已加擾資料的末序列之最

末區塊，施加具有運算如同解碼密碼與已加擾資料的區塊之末端序列的最末區塊的結果之一 XOR 運算子，以及移除相關於預設資料大小之部份 XOR 運算子的結果。

在已解擾資料的塊之末端序列之最末兩個區塊之前的任一區塊係藉施加該解碼密碼至於已加擾資料的區塊之第一末端序列在相關的位置的區塊而形成，且施加具有在已加擾資料的區塊之末端序列中於下一位置運算解碼密碼與已加擾資料的區塊結果的一 XOR 運算子，並且在已解擾資料的區塊之末端序列中最末區塊之前的區塊為藉由施加解碼密碼至由連結相關於預設資料與加擾資料的區塊之末端序列之最末區塊的大小之移除部份而形成的區塊而獲致，並且藉由施加具有運算解碼密碼與初始化向量的結果之 XOR 運算子而獲致，其中該初始化向量係依據已解擾資料的至少一區塊藉在單元中解擾已加擾資料之區塊的先前序列而生成。

此即為在解擾側之密文盜用的實施。

在一實施例中，假使下一單元係藉零或多個預設數目的區塊，或藉等同於或少於基礎區塊大小之充填數目的資料而組成，

擴大資料的數量至等於基礎區塊的大小以形成最末區塊，

在區塊鏈接模式中使用密碼，解碼最末區塊，該區塊鏈接模式係藉初始化向量而初始化，該初始化向量係依據在藉於單

元中解擾已加擾區塊的先前序列而獲致的已解擾資料的區塊之任何序列之至少一的至少一區塊而生成。

使用區塊的預設數目的序列具有下述效果：每一序列的區塊數目為不需要藉由解擾器傳達，其中單元的臨界值為預設的，舉例來說，在單元係藉封包的封包內容而形成的情形中，在大小上小於密碼的基礎區塊大小之資料的任何剩餘數目仍可以已編碼的形式被送到該解擾器，相較於非加擾單元來說不需要增加已加擾單元的大小。

在一變形中，該初始化向量係藉執行密碼操作而產生，較佳地為解碼密碼，在基於獨立於藉在單元中解擾已加擾資料的區塊之先前序列而獲致的已解擾資料的先前區塊的任何區塊的至少一向量上。

此即是指解擾器不需要接收與儲存許多向量以產生初始化向量，生成初始化向量的向量可在單元中於資料之一定數目的單元保持不變。該密碼操作確保其不會被當成用於例如互斥或運算子之邏輯運算子的運算元而使用。

根據本發明之另一目的，用於解擾一已加擾資料的資料流以形成的一資料流系統其特徵為：配置此系統，在已加擾資料的資料流中於包括在資料單元已加擾資料的區塊的序列，以產生用於解擾已加擾資料之區塊的序列的至少一初始化向量，依

據在藉解擾單位之已加擾資料的區塊之一先前序列而獲致之已解擾資料的區塊之序列中的已解擾資料的至少一區塊。

較佳地，根據本發明配置該系統以實行解擾的方法。

根據本發明之另一目的，提供一用於收發資料的設備，其包含配置以提供根據本發明之加擾一資料流之方法的裝置，以及根據本發明之用以解擾已加擾資料的資料流之方法。

因為加擾與解擾的較佳方法可以相同的緩衝需求而施行，此種不需要具有用以儲存區塊的暫存器的設備不用於兩個操作之一，故在硬體中可有一較經濟的應用，特並適用於配置以具有資料之發送器與接收器兩者功能的裝置，例如兩網路間的閘道。

根據本發明之另一目的，其當與機器可讀取媒體相結合時，提供包括一組能使得具有資訊處理能力的系統以根據本發明執行加擾資料流的方法以及根據本發明執行解擾該已加擾資料流的方法的一電腦程式。

【實施方式】

圖 1 繪示傳播資料流之加擾方法的應用，至少部份已繪示的系統本身使用周知的技術：”數位電視傳播規範(Digital Video Broadcasting, DVB)；DVB 同密標準的施行規則(Implementation Guidelines of the DVB Simulcrypt Standard)”、歐洲通信標準局 2002，ETSI 技術報告 TR 102 035 v.1.1.1。

內容提供器 1 提供攜帶明文(plaintext)之封包的串流，意即未加擾的內容資料至多工單元 2，一授權控制訊息(Entitlement Control Message, ECM)產生器 3 提供多工單元 2 一攜帶 ECM 的封包之串流，一授權管理訊息(Entitlement Management Message, EMM)產生器 4 提供該多工單元 2 攜帶 EMM 的封包之串流。多工該串流至 MPEG-2 傳輸串流(Transport Stream, TS)封包的單一串流，且係提供至加擾器 5，MPEG-2 的語法將更詳細地說明於國際標準 ISO/IEC 13818-1 中。將於下述更詳細說明加擾器使用加擾 MPEG-2 TS 封包的封包內容之一方法，其接收來自 CW 產生器 6 之控制字元(Control Word, CW)，該些控制字元係為用於區塊密碼的關鍵。

CW 產生器 6 提供 CW 至 ECM 產生器 3，其在自用戶授權系統(Subscriber Authorisation System, SAS)7 獲致的對稱金鑰(session key)下編碼 CW，此 SAS 提供具有個別用戶的授權之對稱金鑰至 EMM 產生器 4，此 EMM 產生器包括在 EMM 中傳達的金鑰與授權資訊，以確保提供的圖樣(token)至個別的用户。此種安全的圖樣可包括使用例如用於防止包括在其中的例行程序的分析之模糊程式碼(code obfuscation)的特性施行的軟體代理(software agent)。安全圖樣的其他例子包括包含提供以保護特性之處理器的裝置，以防止儲存在其中及/或例行程序硬線圈的分析之資料的存取。

該已加擾資料流自加擾器 5 至調變器 8，且由調變器至傳輸器 9，傳輸器 9 通過例如衛星、電纜地面網路、或包括數各此些網路之網路的傳播網路 10 傳播已加擾資料的串流。在一選擇性實施例中，已加擾 MPEG-2 TS 封包係封裝於接下來的資料封包、傳播、及如同基於網路協定之資料網路的多重傳播或單一傳播中。

對於例示性目的來說，初級的整合接收解碼器(Integrated Receiver Decoder, IRD)係顯示在圖 1 中，初級的 IRD11 包括用於接收傳輸過傳播網路 10 的資料之網路轉換器 12，解調器 13 使得加擾器/解擾器 14 可使用已加擾資料的串流，加擾器/解擾器係配置以實行解擾資料流的方法與加擾資料流的方法兩者。處理器 15 控制初級 IRD11 的操作，其可藉加擾器/解擾器以引導已加擾資料的串流至連接初級 IRD11 與區域網路 17 之第二網路轉換器 16。該區域網路 17 可為例如基於 IEEE 1394 標準的家庭網路，提供第二接收器 18 以對應的網路轉換器 19 以及一解擾晶片 20，更多的元件並無詳細的繪示，該解擾晶片 20 以相同於加擾器/解擾器 14 之方式操作，據此，將於下述中省略對於該晶片的說明。

回到加擾器/解擾器 14，此元件將解擾使用 CW 之已加擾的 MPEG-2 TS 封包，CW 係藉條件存取次系統(Conditional Access Sub-System, CASS)21 而提供，該 CASS 連接例如智慧

卡的用於用於解碼 ECM 之金鑰的安全處理裝置 22 至第一解碼器 23。第一解碼器獲得通過加擾器/解擾器之 CW，藉第二解碼器 24 解碼 EMM，以提供安全處理裝置 22 用以獲致服務金鑰的所需資訊，處理器引導解多工單元 25 以收回攜帶 EMC 與 EMM 之 MPEG-2 TS 封包，以提供至 CASS 21。

圖 2 繪示例如藉加擾器 5 以及加擾器/解擾器 14 所施行的加擾資料流之方法的實施例，在此例示性實施例中，方法係在藉 MPEG-2 TS 封包 27 之封包內容 26 形成的資料單元上實施，其進一步包括標頭 28。不加擾該標頭使其保持原樣，顯然此方法可實施在許多封包的其他型態上，而不必要藉傳輸層網路協定所定義，舉例來說，該方法亦可在攜帶 MPEG-2 TS 封包 27 內之程式基本流(Program elementary Stream, PES) 封包上實施。

雖然 MPEG-2 TS 封包 27 具有 188 位元組的固定長度，但封包內容 26 並非如此，此即因為標頭 28 的長度為可變之故，在圖 2 所繪示的例子中，此種大小的封包內容 26 使得其本身能劃分為固定大小之基礎區塊 P_i 的整數數目，且相等地劃分為所謂超級區塊(super block)的整數數目。每一超級區塊係藉基礎區塊 P_i 之地依序列而形成，第一第一序列 29 以及最後第一序列 30 係詳細地繪示，一連串的超級區塊由封包內容 26 所組成，舉例來說，每一超級區塊係藉三個基礎區塊 P_i 的第一

序列 29、30 而形成，在另一實施例中，每一超級區塊可藉由四、五、或十個基礎區塊，更多的數目需要在加擾器 5 或加擾器/解擾器 14 中設置更多的暫存器。

在封包內容 26 的大小並不等於藉由基礎區塊 P_i 之整數數目的超級區塊之整數數目的情況下，實施下述的步驟。

本方法的另一變形(未繪示)為，劃分該封包內容 26 為可變大小的超級區塊，亦即包括基礎區塊 P_i 的可變數目。

基礎區塊大小係較佳地藉區塊密碼 E_k 、操作在固定長度位元群的對稱金鑰密碼以及具有不變傳輸的基礎區塊而決定。在例示性實施例中，在 CW 下使用區塊密碼 E_k 以編碼個別的基礎區塊 P_i ，合適密碼包括例如 DES、三重 DES 以及 AES/Rijndael，故基礎區塊大小通常為 128 位元。

在此方法的第一步驟中，在第一第一序列 29 中反向基礎區塊 P_1 - P_3 的順序，以形成第二第二序列 31。

在第二步驟中，在密碼區塊鏈接模式中使用區塊密碼 E_k 以在第一第二序列 31 中編碼三個基礎區塊 P_1 - P_3 ，此序列係藉關於第一第二序列之初始化向量而初始化。用以代表關於基礎區塊之第一第二序列 31 的初始化向量 IV_3 之指標(index)係序列中之最後基礎區塊的基礎區塊，此將適用於全文的說明中，用以編碼相關的基礎區塊之第一第二序列 31 初始化向量 IV_3 係藉具有運算長期固定的初始化向量 IV_0 的互斥或運算子以及

基礎區塊的互斥或之應用而形成，基礎區塊 P_1, P_2 係於基礎區塊 P_1-P_3 的第一第一序列 29 中在最後基礎區塊之前。

配置加擾封包內容 26 的方法，使得長期固定的初始化向量 IV_0 不直接地用作初始化向量，其在區塊的第二序列(亦即，反向的)中，從未於第一基礎區塊 P_i 上直接地使用恰好在區塊密碼之前的 XOR 運算中。為此目的，其可使用於多重 MPEG-2 TS 封包 27 而無使密碼分析更為簡單，該長期固定的初始化向量 IV_0 不需要保密，將瞭解的是，當在概述於此之用於加擾與解擾資料單元的方法係使用於同級(peer to peer)通訊中。在圖 1 所繪示的情況中，其中單一提供器控制發送器與接收器，長期固定的初始化向量可被保密，其可在例如 ECM 或 EMM 中提供，在選擇性實施例中，獨立於將被加擾的資料區塊之用以生成初始化向量的向量係藉施加一預設演算法至包括於標頭的資料上。

由於用以編碼在相關的區塊之第一第二序列 31 中區塊 P_1-P_3 的初始化向量 IV_3 係依據在於自第一第一區塊 29 所獲致的最後區塊前之至少一資料區塊而產生，因而達成初始化區塊的更多變形。

第一第二序列的編碼結果係為已加擾區塊 C_3-C_1 之第一第一序列 32，在例示性實施例中，反向已加擾區塊 C_3-C_1 的順序以形成已加擾區塊 C_3-C_1 之第一第二序列 33，已加擾區塊

C_3-C_1 之該第一第二序列 33 係插入包括一未編碼標頭 35 以及已加擾封包內容 36 之已加擾 MPEG-2 TS 封包 34。

因此，對於基礎區塊 P_i 的第一第一序列 29， $i=1...M$ ，已編碼基礎區塊 C_i 為藉下述獲致：

$$C_M = E_k[P_M \wedge IV_M]$$

$$C_i = E_k[P_i \wedge C_{i+1}] \quad i=M-1...1$$

通常，編碼基礎區塊將如同下述：

$$C_{j*M} = E_k[P_{j*M} \wedge IV_{j*M}],$$

$$C_{(j-1)*M+i} = E_k[P_{(j-1)*M+i} \wedge C_{(j-1)*M+i+1}],$$

$$i=M-1...1, \quad j=1...N \setminus M$$

該符號“ $\setminus$ ”係指商或比值的整數部份。

在例示性實施例中，用以編碼在第 j 個序列的區塊之初始化向量 IV_{j*M} 可依下述獲致：

$$IV_{j*M} = IV_0 \wedge P_1 \wedge \dots \wedge P_i \wedge P_{j*M-1}$$

故，在區塊的自區塊的第一序列藉反向區塊數續而形成的每一第二序列中用於編碼相對的初始化向量係依據在同樣的第一序列中之最後區塊之前的至少一資料區塊而產生。在此實施例中，初始化向量係依據在同樣的第一序列中之最後區塊之前的所有資料區塊而產生。

不僅如此，用以在封包內容中編碼來自區塊之第一序列的區塊之第二序列的每一初始化向量係依據至少一區塊而產

生，在所有的區塊、在每一任何先前的基礎區塊的第一序列或在超級區塊中的情形中。

為了於藉在基礎區塊的最後第一序列 30 反向基礎區塊的順序而獲致的最後第二序列 37 中編碼區塊 $P_{N-2}-P_N$ ，編碼密碼 E_k 再一次操作在密碼區塊鏈接模式中。相關於基礎區域的最後第二序列 37 之一初始化向量係在長期固定的初始化向量以及每一先於最後基礎區塊 P_N 的基礎區塊上藉執行 XOR 操作而生成。結果為已加擾資料之區塊的最後第一序列 38，反向區塊的順序已獲致已加擾資料的區塊之最後第二序列 39。

圖 3 繪示假使 MPEG 2 TS 封包內容係藉 $N \times M$ 基礎區塊的第一序列之整數以及在大小上等同於或少於 M 基礎區塊之接續的資料數量而組成時加擾方法如何進行。在此例示性的實施例中，資料的接續數量可分為兩個完全基礎區塊 P_{N-2} 、 P_{N-1} ，以及一偏區塊，最後區塊 P_N 是以零填充至相同於完全基礎塊的大小，故第一末端序列係藉區塊 P_{N-2} 、 P_{N-1} 而形成以及以填充的第 N 個區塊 P_N ，交換區塊的第一末端序列之最後兩個區塊的位置以形成區塊的第二末端序列 40(繪示於圖 3 中)，在區塊的第二末端序列之區塊係在區塊鏈接模式中使用編碼密碼 E_k 而編碼。對初始化向量來說，初始化向量係於 MPEG-2 TS 封包內容 26 中藉施行具有長期固定初始化向量與在先於偏區塊之最末完全基礎區塊之前的每一完全基礎區塊的操作元之

XOR 操作而產生。結果為已加擾資料的塊之第一末端序列 41，在區塊的第一末端序列中，對應於藉填充而增加的資料的大小與位置之已加擾資料 C' 之數量係自第一區塊而移除，並且區塊的順序係實質地反向以獲致已加擾區塊的第二末端序列(未繪示)，此第二末端序列係插入於已加擾封包內容 36 中，當然，接下來可移除已加擾資料 C' 以反向區塊的順序。

假使 MPEG-2 TS 封包內容 26 係藉區塊的 $N \setminus M$ 第一序列之整數與等於或小於基礎區塊之期望數量的資料而組成，則實行繪示於圖 4 的操作，以零填充偏區塊 P_N 至全大小的最末區塊 42。初始化向量 IV_N 係依據長期固定的初始化向量 IV_0 以及在封包內容 26 的區塊之第一序列之前的至少一區塊而產生，亦可能發生沒有先前的第一序列之情形，故在 XOR 運算中不直接使用長期固定的初始化向量 IV_0 為運算元。關於全大小的最末區塊 39 之初始化向量首先被解碼，使用與編碼密碼 E_k 以及作為金鑰之 CW 相反的解碼密碼，獲致結果以及全大小的最末區塊的互斥或操作，且藉施加區塊密碼 E_k 而編碼。結果為全大小的已加擾區塊，其係藉移除相關於藉填充該偏區塊 P_N 增加的資料之大小與位置的部份而截去上部，剩餘部份 CN 係插入已加擾封包內容 36 中。

一連串 MPEG-2 TS 封包 27 的封包內容係依此方式加擾，故形成資料的已加擾串流，密文盜用與處理單一偏區塊的方法

確保了已加擾封包內容 36 在大小上等同於起始明文 MPEG-2 TS 封包 27 的封包內容 26。故，相對於明文 MPEG-2 TS 封包已加擾 MPEG-2 TS 封包 34 之標頭 35 實質上不需要改變，除指出其已選擇地被加擾，其中奇數與偶數的 CW 已用作區塊密碼 E_k 。

圖 5 繪示關於描述於圖 2 中加擾操作之解擾操作，如同圖 2 的情形，圖 5 係基於假設在已加擾封包內容中確實具有 NM”超級區塊”，該已加擾封包內容形成已加擾資料的區塊之序列的接續，每一序列係相關於”超級區塊”，顯示已加擾資料的區塊 C1-C3 之第一序列 44 以及區塊 CN-2-CN 的最末序列 45。

已加擾資料之區塊的每一序列係分別地解擾，以形成已解擾之區塊的對應序列，故，解擾區塊 C1-C3 的第一序列 44 以形成明文區塊 P_1-P_3 的第一序列 46，解擾區塊 $C_{N-2}-C_N$ 的最末序列 45 以形成明文區塊 $P_{N-2}-P_N$ 的最末序列 47，使用明文區塊的序列以形成標頭 49 在前的明文 MPEG-2 TS 封包內容 48，故因此形成在組成的明文 MPEG-2 TS 封包 50。

在明文區塊第一序列 46 之已解擾資料的第一區塊係藉施行編碼區塊 E_k 的相反之解擾密碼 D_k 至已加擾資料的第一區塊 C_1 ，且應用具有如操作解碼密碼與在已加擾資料的區塊之序列中的下一已加擾區塊 C_2 之結果的一 XOR 操作子而獲致，第二

區塊 P_2 係以相同方式獲致，獲致來自 ECM 的 CW 係為用於解碼密碼 D_k 的金鑰。

在明文區塊之第一序列 46 中之已解碼資料的最末區塊 P_3 係藉施加解碼密碼 D_K 至在已加擾資料的區塊 C_1 - C_3 之第一序列 44 中的最末區塊 C_3 而獲致，結果即為藉關於第一”超級區塊”的初始化向量 IV_3 之互斥或操作，依據施加解碼密碼 D_K 至於同樣序列中已加擾資料之最末區塊 C_3 之前在已加擾資料區塊的第一序列 44 中之區塊，以及施加在已加擾資料的區塊之序列中於下一位置運算解碼密碼 D_K 以及已解擾資料之至少的結果之例如 XOR 運算子的運算子，而獲致至少一資料區塊以產生初始化。在例示性實施例中，初始化向量 IV_3 為長期固定的初始化向量 IV_0 與在於最末明文區塊 P_3 之明文區塊之第一序列 46 中的所有區塊的互斥或(XOR)，由於在最末明文區塊 P_3 被獲致前獲致此些先前的明文區塊，解擾方法將相對地有效率。

通常，使用已加擾資料的區塊之固定數目 M 於每一連串的包括在已加擾封包內容中之已加擾資料的區塊之序列，明文區塊為如下所示：

$$P_{j*M} = D_k[P_{j*M} \wedge IV_{j*M}],$$

$$P_{(j-1)*M+i} = C_{(j-1)*M+i+1} \wedge D_k[C_{(j-1)*M+i}],$$

$$i=M-1 \dots 1, \quad j=1 \dots N \setminus M$$

在例示性實施例中，用以解碼在第 j 個序列的區塊之初始化向量 IV_{j*M} 係藉下列而獲致：

$$IV_{j*M} = IV_0 \wedge P_1 \wedge \dots \wedge P_i \wedge P_{j*M-1}$$

在此方法中，用以解擾已加擾資料之第二以及接下來的序列初始化向量係依據在藉在已加擾封包內容 36 中解擾已解擾資料的區塊之先前序列而獲致的已解擾資料的區塊的序列中之至少一已解擾資料的區塊而產生。

圖 6 繪示假使已加擾封包內容 36 是由基礎區塊的 $N \setminus M$ 第一序列的整數以及大小相等於部分基礎區塊大小的多重基礎區塊大小之資料的期望數量所組成的加擾方法如何進行。在例示性實施例中，資料的期望數量可區分為兩個完全已加擾區塊 C_{N-2}, C_{N-1} 以及一偏區塊 C_N ，以零填充最末區塊 C_N 至相等於最末完全基礎區塊 51 的大小，故末端序列係藉區塊以及最末完全基礎區塊而形成，在已加擾資料的區塊的末端序列之最末區塊之前，一最末明文區塊 P_N 係藉由立即施加解密碼 D_K 至區塊 C_{N-1} 而形成，施加 XOR 操作子至解密密碼與最末完全基礎區塊 51 的結果，且移除對應於藉填充最末已加擾區塊 C_N 而增加的資料之大小與位置的 XOR 運算子的結果部份。在最末兩個明文區塊 P_{N-1}, P_N 前的每一區塊的情況中，唯序列的第一區塊 P_{N-2} 為此種區塊，其係藉施加解碼密碼 D_K 至在已擾資料的區塊之末端序列的對應位置，並且在已加擾資料的區塊之末端序

列的下一位置中，施加 XOR 運算子至解碼密碼與已加擾資料的區塊。

在明文區塊的末端序列之最末區塊前的區塊 P_{N-1} 係藉施加解碼密碼至藉連結最末已加擾區塊 C_N 以及對應於用於充填之零的大小與位置的移除部份 C' 形成的區塊 52 而獲致。且之後施加 XOR 運算子以運算解碼密碼 D_K 與初始化向量 IV_N 的結果，對於初始化向量而言，初始化向量 IV_N 係藉施加 XOR 運算子以運算長期固定初始化向量與在明文 MPEG-2 TS 封包內容 48 中之每一最末兩個區塊 P_{N-1}, P_N 的結果而產生。

假使已加擾封包內容係藉已加擾資料的 $N \setminus M$ 序列的整數以及相等或少於基礎區塊的資料之期望數量而組成，而實行繪示於圖 7 的操作。以零填充偏已加擾區塊至全大小最末已加擾區塊，初始化向量 IV_N 係依據在已加擾封包內容 36 中長期固定的初始化向量 IV_0 以及在已加擾區塊的任何先前序列之至少一區塊而產生。可能發生沒有已加擾資料的先前序列的情形，而不致直接使用長期固定的初始化向量 IV_0 為 XOR 運算中的操作元，首先解碼關於全大小最末已加擾區塊 53 的初始化向量，使用如同使用 CW 為金鑰的區塊鏈接模式的相同解碼密碼。而獲致結果與全大小最末已加擾區塊 53 的互斥或運算，此結果為一全大小區塊 54，其藉由移除對應於藉填充偏已加

擾區塊而增加的資料大小與的位置部份 C'而於截頂於上部，剩餘部份插入 MPEG-2 TS 封包內容中。

因此，已詳細地說明一方法，其中”超級區塊”具有預設大小，但其可依包括不在多重既定大小之”超級區塊”的數目內之可變大小的封包內容來處理。用於每一”超級區塊”的初始化向量從不直接地作為 XOR 操作子的遮蔽(mask)，其盡量依據在封包內容中之先前明文區塊，以獲致初始化向量之變形。用於儲存運算結果的記憶體需求實質上相同於用於加擾器與解擾器的記憶體需求，且可藉由選定”超級區塊”的較低大小而可接受較小的記憶體。

本發明並不限於以述之實施例，其可於所附之申請專利範圍內具有各種的變形。特別是，在一實施例中，藉由在加擾器中反向區塊順序但已加擾區塊的第一序列並無轉換成已加擾區塊的第二序列的情形是有可能的，其係在實行繪示於此的解擾已加擾資料之串列的方法前，在解擾器中實行的反向。

【圖式簡單說明】

本發明將配合附圖而進一步地說明，其中

圖 1 繪示用於實施加擾與解擾傳播資料流之方法的系統；

圖 2 繪示加擾資料流之方法的一實施例；

圖 3 繪示在加擾資料流的方法中實施密文盜用的方法；

圖 4 繪示如何處理形成 MPEG-2 傳輸流封包內容之單偏區塊；

- 23 第一解碼器
- 24 第二解碼器
- 25 解多工單元
- 26、36、48 封包內容
- 27、34、50 MPEG-2 TS 封包
- 28、35、49 標頭
- 29、30、32、44、46 第一序列
- 31、33、37 第二序列
- 41、45、47 末端序列
- 39、42 最末區塊
- P_i 、 P_1 - P_3 、 P_{N-2} - P_N 、 P_{N-1} 、51 基礎區塊
- C_1 - C_3 、 C_i 、 C_{N-2} - C_N 已加擾資料的區塊
- E_k 密碼
- D_k 解擾密碼
- C' 已加擾資料
- IV_0 、 IV_3 、 IV_N 初始化向量
- C_3 - C_1 、53 已加擾區塊
- 54 全大小區塊

五、中文發明摘要：

一種加擾資料流的方法包括：

自串流獲得一連串(29,30)的資料之區塊(P_i)的第一序列，
在每一區塊(P_i)的第一序列(29,30)中反向區塊的順序，以
形成對應的資料的區塊之第二序列(31,37)，以及

在每一區塊的第二序列(31,37)中於區塊鏈接模式使用密碼(E_k)而編碼區塊，區塊鏈接模式係以用於每一區塊的第二序列(31,37)之對應初始化向量(IV_3, IV_N)而初始化，對在串流內資料的單元(26)中之一連串的區塊之第一序列(29,30)來說，用於在單元中編碼來自區塊的第一序列之區塊的第二序列(37)之至少一初始化向量(IV_N)係依據在先前的單元之區塊的第一序列(29)中至少一區塊而產生。

六、英文發明摘要：

A method of scrambling a stream of data includes
obtaining from the stream a succession of first sequences
(29,30) of block (P_i) of data,

reversing the order of the data (P_i) in each of the first
sequences (29,30) of blocks to form respective second sequences
(31,37) of blocks of data, and

encrypting the blocks in each second sequence (31,37) of
blocks using a cipher (E_k) in block chaining mode, initialized

with a respective initialization vector (IV_3, IV_N) for each second sequence (31,37) of blocks. For a succession of first sequences (29,30) of blocks included in a unit (26) of data within the stream, at least one initialization vector (IV_N) for encrypting a second sequence (37) of blocks formed from a first sequence (30) of blocks in the unit is generated in dependence on at least one block in a preceding first sequence (29) of blocks of the unit.

十、申請專利範圍：

1. 一種加擾資料流的方法，包括：

自串流獲得一連串的資料之區塊(P_i)的第一序列(29,30)，
在每一區塊(P_i)的第一序列(29,30)中反向區塊的順序，以
形成對應的資料的區塊之第二序列(31,37)，以及

在每一區塊的第二序列(31,37)中於區塊鏈接模式使用密碼(E_k)而編碼區塊，區塊鏈接模式係以用於區塊的第二序列(31,37)之對應初始化向量(IV_3, IV_N)而初始化，

其特徵在於：

對在串流內資料的單元中之一連串的區塊之第一序列(29,30)來說，用於在單元(26)中編碼來自區塊的第一序列(30)之區塊的第二序列(37)之至少一初始化向量(IV_N)係依據在先前的單元之區塊的第一序列(29)中至少一區塊而產生。

2.如申請專利範圍第1項所述的方法，其中在形成自區塊的第一序列(29,30)之區塊的每一第二序列(31,37)中用以編碼區塊之相對的初始化向量(IV_3, IV_N)係依據相同的第一序列(29,30)中在於最後區塊前的至少一資料區塊而產生。

3.如申請專利範圍第1項與第2項之任一項所述的方法，其中在單元中用於編碼形成自區塊的第一序列之區塊(30)的第二序列(37)的每一初始化向量(IV_N)係藉在單元(26)的區塊之第一序列(29)前的任何至少一區塊而產生。

4.如申請專利範圍第 1 項至第 3 項之任一項所述的方法，其中包括接收包括一標頭(28)與一封包內容(26)的一資料封包(27)，其中該單元係藉封包內容形成。

5.如申請專利範圍第 1 項與第 4 項之任一項所述的方法，其中密碼(E_k)為配置以操作在預設大小的基礎區塊上之區塊密碼，其中在至少大小係對應基礎區塊大小之資料的第二序列(31,37)中的區塊(P_i)。

6.如申請專利範圍第 5 項所述的方法，其中假使單元(26)係藉一連串的區塊的第一序列(29,30)以及大小等同於或小於多重區塊資料的大小之期望的資料數量所組成，

填充資料的數量至等於多重基礎區塊的大小以形成至少兩塊的第一末端序列，

交換至少區塊的第一末端序列的兩區塊，並且反向在區塊之第一末端序量的至少兩區塊以形成資料區塊的第二末端序列(40)，

在區塊鏈接模式中使用密碼(E_k)以編碼在區塊的第二末端序列的區塊，其依據在單元的區塊之先前第一序列(29,30)中的至少一區塊，藉由所產生的初始化向量(IV_N)而初始化。

7.如申請專利範圍第 5 項所述的方法，其中假使單元係藉零或區塊之預設數目的更多第一序列，以及藉等於或小於基礎區塊大小之資料的數量(P_N)所組成，

填充資料的數量至相等於基礎區塊的大小以形成最末區塊(42)，

在區塊鏈接模式中使用密碼(E_k)而解碼最末區塊(42)，其係依據在任何先於單位中的區塊之第一序列之至少一的至少一區塊而生成的初始化向量而初始化。

8.如申請專利範圍第7項所述的方法，其中初始化向量係藉執行密碼操作(D_k)而產生，較佳為密碼之相反的解碼，在基於至少在獨立於在任何先於單元的區塊之第一序列中的任何區塊之最後一個向量(IV_0)的向量上。

9.一種用於加擾一資料流的系統，其包括：

用以接收串流作為一連串的資料的區塊(P_i)之第一序列(29,30)的輸入，

多個暫存器以及用於反向在區塊(P_i)的第一序列(29,30)之區塊之順序的至少一邏輯單位，以形成資料區塊之第二序列(31,37)，以及

於區塊鏈接模式中使用密碼(E_k)用於在區塊的每一第二序列(31,37)中編碼區塊的處理配置，其藉區塊之每一第二序列(31,37)之對應的初始化向量(IV_3, IV_N)而初始化，

其特徵在於：

配置該系統，用於包括於串列內在資料單元(26)中之一連串的區塊，依據在單元中區塊的先行第一序列(29)之至少一區

塊，以在單元中產生用於編碼形成自區塊的第一序列(30)之區塊的第二序列之至少一初始化向量。

10.如申請專利範圍第 9 項所述的系統，其中該系統係配置以執行申請專利範圍之第 1 項至第 8 項之任一項所述的方法。

11.一種解擾已加擾資料的串流以形成資料流的方法，其包括：

自己加擾資料的串流獲致一連串的已加擾資料的區塊(C_i)之序列(44,45)，以及

解擾已加擾資料的區塊的每一序列(44,45)，以形成已解擾資料的區塊(P_i)之相關序列(46,47)，藉由在反向鍊接模式中使用解擾密碼(D_K)，其中，解擾已加擾資料的區塊之序列(46,47)，

在已解擾資料的區塊之序列中(46,47)的最末區塊(P_3, P_N)係藉在已加擾資料之區塊的相關序列中施加解碼密碼(D_K)至最末區塊(C_3, C_N)，以及施加具有至少解碼密碼(D_K)的結果以及初始化向量(IV_3, IV_N)的操作之操作子而獲致，且其中在已加擾資料的區塊之序列(46,47)中先於最末區塊(P_3, P_N)之每一區塊係藉施加解碼密碼(D_K)至對應的位置在已加擾資料的區塊之序列(44,45)的區塊，與於已加擾資料的區塊之序列(44,45)中施加具有操作至少解碼密碼的結果以及在下一位置之已加擾資料的區塊操作子而獲致，

其特徵在於：

在一資料單元(36)中對於一連串已加擾資料的區塊之序列(44,45)，用以解擾已加擾資料的區塊之序列(45)的至少一初始化向量(IV_N)係依據在藉解擾單元(36)的已加擾資料之區塊的一先前序列(44)而獲致的已解擾資料的區塊之序列(46)中已解擾資料的至少一區塊而產生。

12.如申請專利範圍第 11 項所述的方法，其中產生用以解擾已加擾資料的區塊(C_i)之每一序列(44,45)之相對的初始化向量(IV_3, IV_N)，其係在相同序列(44,45)已加擾資料的最末區塊(C_3, C_N)之前的已加擾資料的區塊之序列(44,45)中依據已解擾資料的至少一區塊，且藉施加在已加擾資料的區塊之相同序列(44,45)於下一位置具有運算至少解碼密碼(D_K)的以及已加擾資料的區塊之結果的運算子。

13.如申請專利範圍第 11 項與第 12 項之任一項所述的方法，其中依據在單元(36)中來自藉解擾已加擾資料的區塊的序列(45)之先前序列(44)而獲致的已解擾資料的區塊之每一任何序列(46)的已解擾資料之至少一區塊，而在單元(36)中產生用於解擾已加擾資料之區塊的序列之初始化向量(IV_N)。

14.如申請專利範圍第 11 項至第 13 項之任一項所述的方法，其中包括接收包括一標頭(35)以及封包內容(36)的資料封包(34)，其中該單元係藉封包內容形成。

15.如申請專利範圍第 11 項至第 14 項之任一項所述的方法，其中解碼密碼(D_K)為配置以操作於預設大小的基礎區塊上的一區塊密碼，其中在已加擾資料的區塊的序列(44,45)中之區塊(C_i)的大小係對應於基礎區塊大小的大小。

16.如申請專利範圍第 15 項所述的方法，其中假使該單元(36)係藉由一連串的已加擾資料之區塊的序列以及相等於整數的多重基礎區塊大小以及部分(C_N)的基礎區塊大小之資料的接續數目所組成，

以預設資料填充資料的數目至多重基礎區塊的大小，而形成已加擾資料之區塊的末端序列，

已解擾資料之區塊的末端序列之最末一個(P_N)為藉施加解碼密碼至恰於已解擾資料的末端序列的最末區塊之前的區塊而形成，施加運算解碼密碼以及已加擾資料之區塊的末端序列的最末區塊之結果的一 XOR 運算子，並移除相關於預設資料大小之部份(C')的 XOR 運算子的結果，

在已解擾資料的區塊的末端序列之最末兩個區塊(P_{N-1} , P_N)前的每一任何區塊係藉施加解碼密碼(D_K)至在已加擾資料的區塊之第一末端序列中對應位置處區塊，以及藉施加運算解碼密碼與在已加擾資料的區塊之末端序列中下一位置處的已加擾資料的區域的結果之 XOR 運算子而形成，以及

在於已解擾資料的區塊之末端序列中之最末區塊之前的區塊(P_{N-1})係藉施加解碼密碼至藉連結相關於預設資料大小的已移除部份(C')與已加擾資料的區塊之末端序列的末端區塊而形成的區塊(52)，並且藉施加運算解碼密碼與初始化向量的結果之 XOR 運算子而獲致，初始化向量(IV_N)係在單元(36)中依據在藉解擾已加擾資料的區塊之先前序列而獲致的已解擾資料之區塊的任何序列中之至少一區塊而產生。

17. 如申請專利範圍第 15 項所述的方法，其中假使下一單元係藉零或區塊的預設數目之更多序列，以及相等於或小於基礎區塊大小之資料的期望數量(C_N)而組成，

填充資料的數量至相等於基礎區塊大小的大小，以形成最末區塊(53)，

在區塊鏈接模式中使用密碼以解碼最末區塊(53)，該區塊鏈接模式係藉初始化向量而初始化，在單元中該初始化向量係依據在藉解擾已加擾資料的區塊之先前序列而獲致的已解擾資料的區塊之任何序列之至少一中的至少一區塊而產生。

18. 如申請專利範圍第 17 項所述的方法，其中初始化向量係藉執行一密碼操作而產生，較佳地為解碼密碼(D_K)，在基於至少一向量之向量上，在任何已解擾資料之先前區塊中該向量係獨立於任意區塊，該已解擾資料係在單元中藉解擾已加擾資料的區塊之先前序列而獲致。

19.一種用於解擾已加擾資料的串流以形成一資料流的系統，其包括：

用以接收已加擾資料的串流作為一連串的已加擾資料的區塊(C_i)之序列(44,45)的輸入，

用以解擾已加擾資料的區塊(C_i)之每一序列(44,45)的處理配置，以形成已解擾資料的區塊之相關序列(46,47)，其中藉在反向鍊接模式中使用解碼密碼(D_K)，以解擾已加擾資料的區塊之序列(44,45)，

在序列(46,47)中已解擾資料的最末區塊(P_3, P_N)係藉施加解碼密碼(D_K)至在相關的已加擾資料的區塊之序列(44,45)中的最末區塊(C_3, C_N)，以及藉施加運算解碼密碼(D_K)與初始化向量(IV_3, IV_N)之結果的運算子而獲致，且其中在序列(46,47)中已解擾資料的每一先前區塊係藉施加解密密碼至在已加擾資料的區塊之序列中的區塊於對應位置，以及在已加擾資料的區塊之序列(44,45)中藉施加運算解碼密碼與已加擾資料的區塊於下一位置的結果運算子而獲致，

其特徵在於，

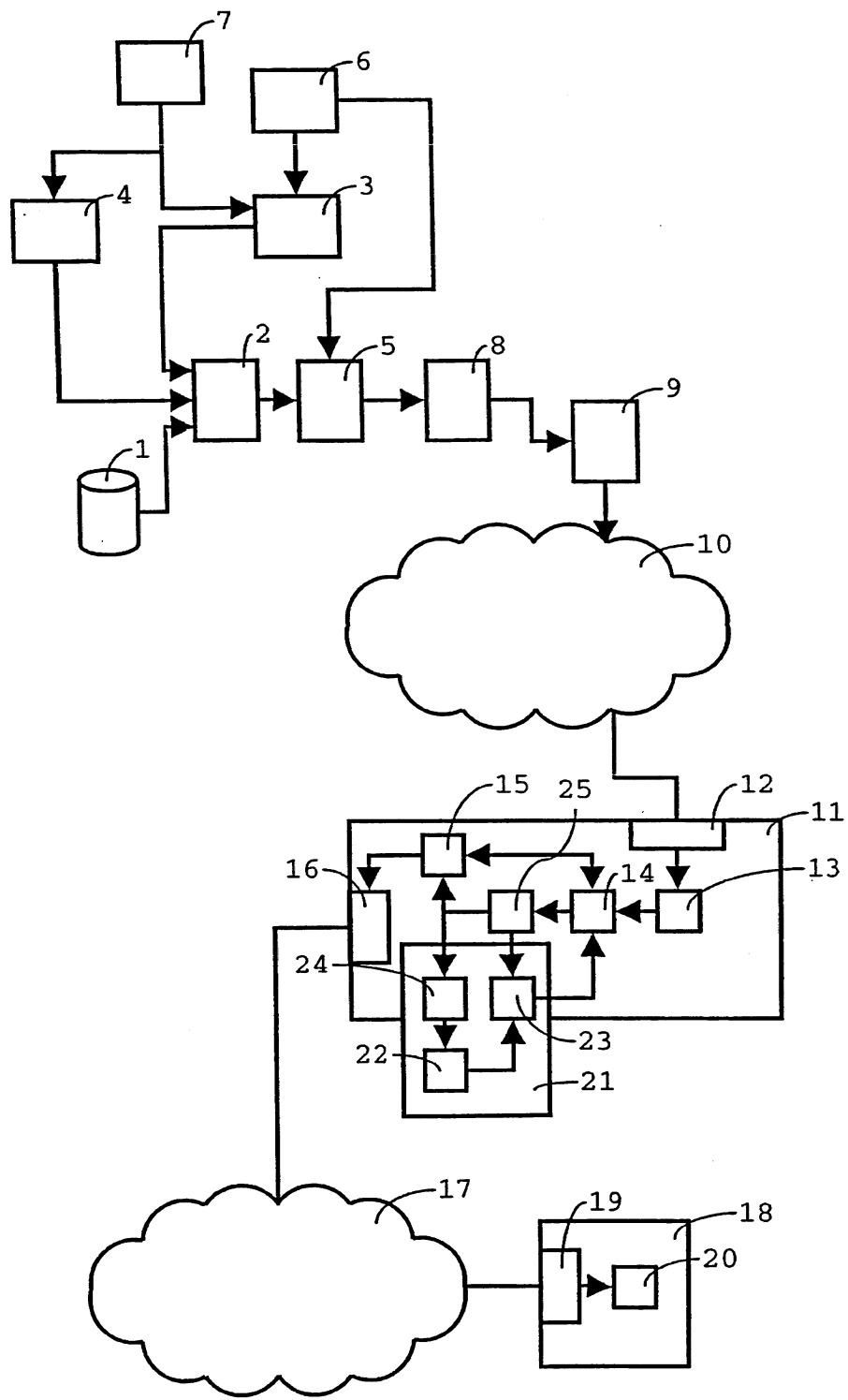
配置該系統，該系統係用於包括在資料單元(36)中在已加擾資料之串流內一連串的已加擾資料的區塊之序列(44,45)，以產生用於解擾已加擾資料的區塊之序列(45)的至少一初始化向量(IV_N)，其依據在藉解擾單元(36)的已加擾資料的區塊之先

前序列(44)而獲致已解擾資料的區塊之序列中已解擾資料之至少一區塊。

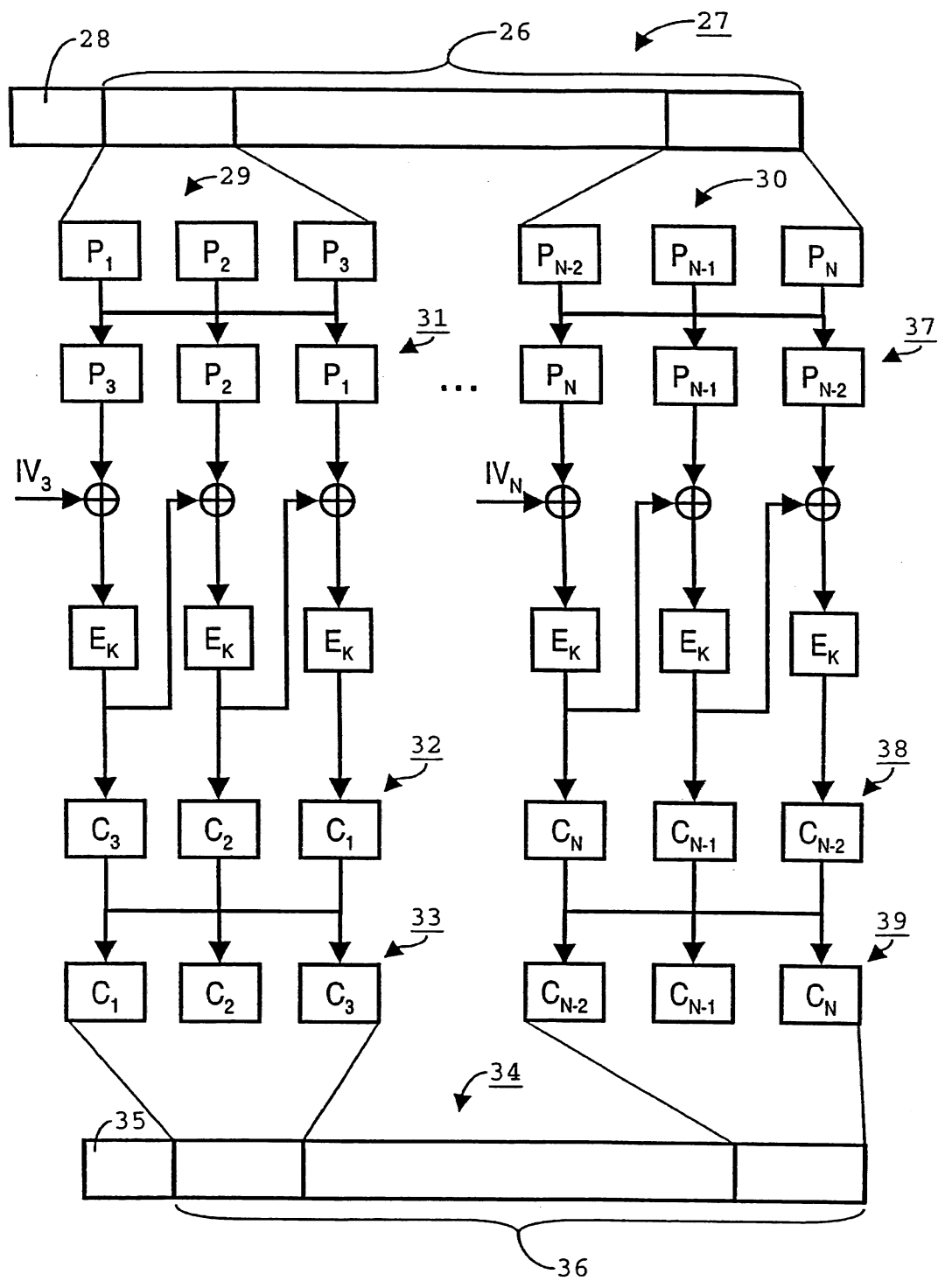
20.如申請專利範圍第 19 項所述的系統，其中該系統係配置以執行申請專利範圍之第 11 項至第 18 項之任一項所述的方法。

21.一種用於收發資料的設備，其包括配置以實行根據申請專利範圍第 1 項至第 9 項之任一項所提供之方法以及申請專利範圍第 11 項至第 18 項之任一項所提供之方法的裝置。

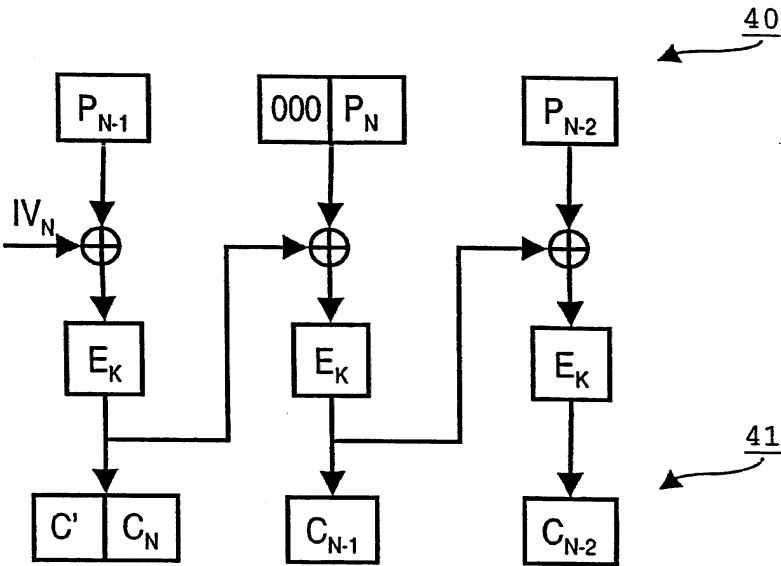
22.一種電腦程式，包括一組指令，其在與機器可讀取媒體相結合時能使得具有資訊處理能力的一系統執行根據根據申請專利範圍第 1 項至第 9 項之任一項所提供之方法以及申請專利範圍第 11 項至第 18 項之任一項所提供之方法。



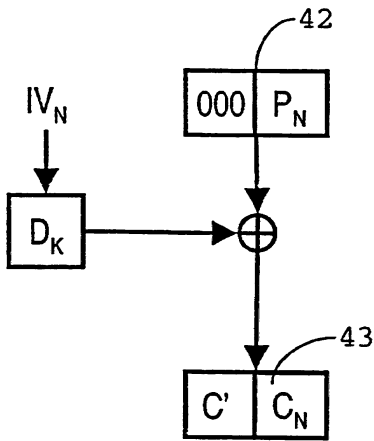
第一圖



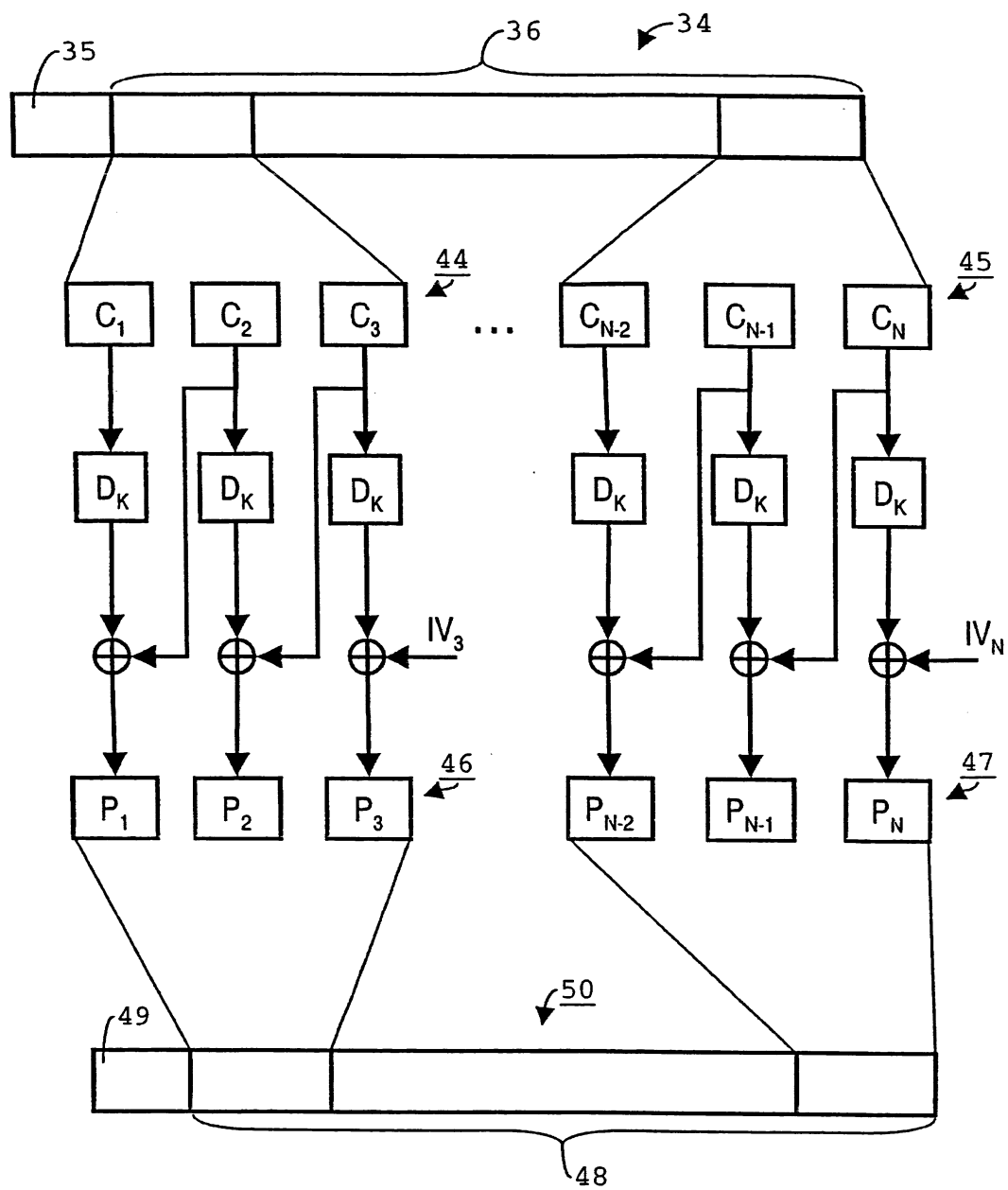
第二圖



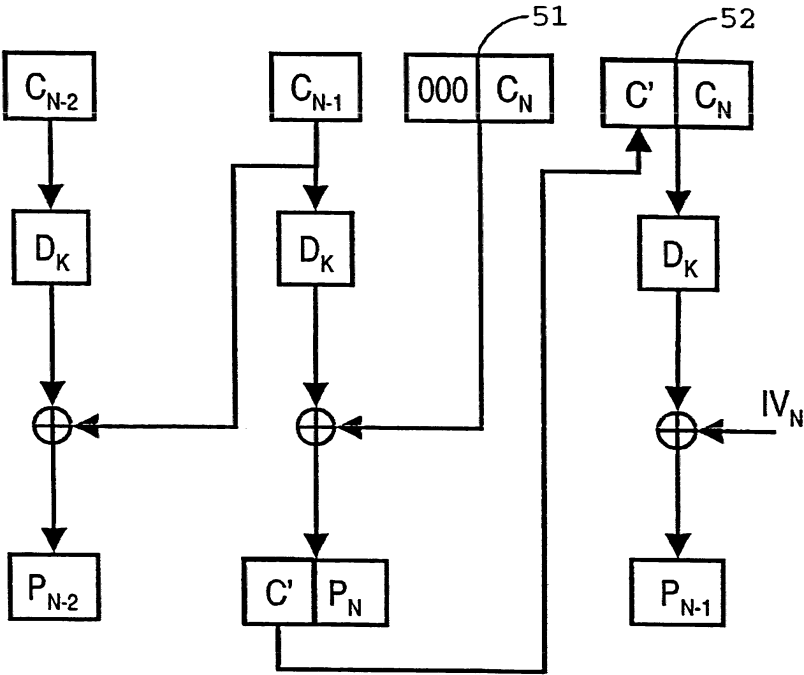
第三圖



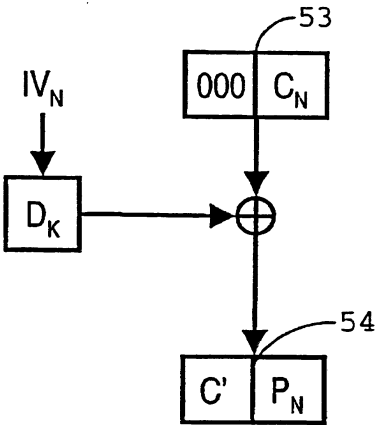
第四圖



第五圖



第六圖



第七圖

七、指定代表圖：

(一)本案指定代表圖為：第(1)圖。

(二)本代表圖之元件符號簡單說明：

- 1 內容提供器
- 2 多工單元
- 3 授權控制訊息產生器
- 4 授權管理訊息產生器
- 5 加擾器
- 6 控制字元產生器
- 7 用戶授權系統
- 8 調變器
- 9 傳輸器
- 10 傳播網路
- 11 整合接收解碼器
- 12 網路轉換器
- 13 解調器
- 14 加擾器/解擾器
- 15 處理器
- 16 網路轉換器
- 17 區域網路
- 18 接收器
- 19 網路轉換器
- 20 解擾晶片
- 21 條件存取次系統
- 22 安全處理裝置
- 23 第一解碼器
- 24 第二解碼器
- 25 解多工單元

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：
無

九、發明說明：

【發明所屬之技術領域】

本發明係關於加擾與解擾一資料流的方法，更確切地說，
本發明係關於以加擾與解擾一資料流的系統而執行加擾與解
擾一資料流的方法。

【先前技術】

在國際申請號 WO 95/10906 的說明書中獲知，在習知的方法中，劃分數位資料為 N 個區塊的封包，即 X(1)、X(2)...X(N)，其中每一區塊具有 2m 位元，在編碼操作之前反向區塊的序列為 X(N)、X(N-1)...X(1)，此區塊的序列為以下列方式藉編碼演算法 E 而編碼(其中[^]是用以表示互斥或/XOR 運算子)：

$$Y(1) = E[X(N) \wedge IV]$$

$$Y(i) = E[X(N-i+1) \wedge Y(i-1)] \quad \text{對於 } i > 1 \text{ 且 } i \leq N$$