公告本

申請日期	88.4.21
案號	88106371
類別	H04L 9/06

（以上各欄由本局填註）

A4
C4

456127

發明 新型 專利說明書

一、發明新型名稱	中文	加密語音編碼器
	英文	ENCRYPTING SPEECH CODER
二、發明創作人	姓名	1.亞當 L. 貝倫茲維格　2.史帝芬 安東尼 費可 3.山揚 B. 米西考夫斯基　4.溫斯頓 艾德華 派洛 5.羅柏 約翰 蘭斯　6.唐諾 約瑟夫 尤克斯
	國籍	均美國
	住、居所	1.美國紐約州紐約市東十二街70號 2.美國新澤西州莫里斯平原市桃樹街6號 3.美國新澤西州摩根維爾市黃刀路227號 4.美國新澤西州比斯凱特威市洛傑斯路85-B號 5.美國麻州安朵佛市冬青圓環6號 6.美國新澤西州貝斯金脊市詹姆斯頓路82號
三、申請人	姓名（名稱）	美商朗訊科技公司
	國籍	美國
	住、居所（事務所）	美國新澤西州摩里山丘市山脈大道600號
	代表人姓名	麥克・R・格林

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

裝 訂 線

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有 □無主張優先權
美國	1998年06月15日	09/097,782	☑有 □無 主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱　背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部中央標準局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（1）

發明領域

本發明大致係關於通訊系統，而尤其有關用於無線通訊系統之加密技術。

相關技藝背景

無線通訊系統使用密碼學以提供其用户安全之通訊裝置。密碼學提供安全性，僅讓所希望之接收器可了解一由一經授權之傳送器所傳送的訊息內容(其可能例如爲聲音資料，使用者資料，或者FACCH/SACCH訊息)，並且僅經授權之傳送器可將訊息送至希望的接收器。密碼學之挑戰爲將訊息之內容改變成僅一希望之接收器可理解的形式。此必須以一對傳送器以及希望之接收器兩者很經濟的方式進行。同時，(於時間及/或裝備等項目上)一未授權之接收器(亦即並非所希望的接收器)必須很難理解該項內容。當未授權之接收器與傳送器變得更複雜時，對於安全通訊之需求變得更殷切。

圖1根據著名之分時多向近接(TDMA)的電信工業協會(TIA)IS-136(與修訂版)標準以及代數碼激發之線性預測(ACELP)的IS-641標準而說明一合併於一傳送器10內之加密語音處理器架構。傳送器10包含七位元循環檢查碼(7位元CRC)14，半數比率迴旋式編碼器(1/2比率CC)16，打孔器18，聲音加密器20以及雙槽插入器22。語音編碼器12將一訊息框編碼，特徵爲：160個16位元語音抽樣編碼，以產生148個具有96個等級1位元與52個等級2位元之編碼的語音位元，特徵爲：等級1位元包括48個等級1A位元與48個等級

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（2）

1B位元。等級1位元係重要之位元(例如位元表現之音階，音調等)，當傳送於無線電鏈路時必需有錯誤控制防護，特徵爲：錯誤控制防護係使用循環檢查碼(CRC)，迴旋碼及位元插入等提供。等級1A位元係提供以作爲七位元循環檢查碼(7位元CRC)14之輸入，以產生7個錯誤控制位元。該錯誤控制位元，等級1位元及5個尾碼位元(特徵爲：迴旋碼狀態資訊)係提供以作爲半數比率迴旋式編碼器(1/2比率CC)16之輸入，以產生216個代碼字位元。然後該代碼字位元(透過打孔器18)進行清除字元插入，以產生208個打孔之代碼字位元。

其次聲音加密器20係用以防護訊息，僅讓希望之接收器可理解訊息內容。尤其，打孔之代碼字位元與等級2位元提供以作爲聲音加密器20之輸入。聲音加密器20使用一相關於所希望之接收器的260位元固定之祕密罩幕將該輸入加密，以產生260個加密之位元。尤其，加密係藉由將一打孔之代碼字位元與使用祕密罩幕的等級2位元執行一XOR二元運算而達成。加密之位元係(藉由位元雙槽插入器22)進行位元插入以產生260個插入之位元。然後將該訊息予以多工化，調變並由傳送器10傳送。

傳送之訊息係由一接收器(未顯示)接收，該接收器執行傳送器10之反轉功能。於接收該傳送之訊息時，接收器將該傳送之訊息解調變及解多工化，以獲得260個插入之位元。然後該位元插入之處理(藉由一聲音解密器)進行反轉，以獲得一具有208個打孔之代碼字位元與52個等級2位元的輸出

（請先閱讀背面之注意事項 填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（3）

。如果接收器無法知道由傳送器10所使用之260位元固定之祕密罩幕(亦即接收器不是所希望之接收器)，則接收器將無法適當地將該加密之位元解密。

打孔之代碼字係提供予一1/2比率迴旋式解碼器，其中打孔之代碼字位元經解迴旋以獲得一具有96個等級1位元之輸出(特徵爲：48個等級1A位元與48個等級1B位元)與7個錯誤控制位元。注意：接收器沒有清除字元插入處理之反轉功能。清除字元插入所造成之位元損失係於解迴旋處理中恢復，如技藝中之著名作法。

等級1A位元係用於一接收器之7位元循環檢查碼(CRC)，以產生一第二組之7個錯誤控制位元(特徵爲：第一組之7錯誤控制位元係部分之1/2比率迴旋解碼器之輸出)。(使用一循環檢查碼(CRC)之檢查)比較第一與第二組的錯誤控制位元，以決定是否發生一相關於等級1A之傳送錯誤(亦即決定是否有壞框存在)。如果沒有傳送錯誤發生，則將(來自聲音解密器之)等級1位元與第級2位元傳遞至一解碼之語音解碼器。如果發生一傳送錯誤(亦即偵測得一壞框)，則可能丟棄等級1A位元與32個最高有效等級1B位元，並以最後良框其等級1A位元與32個最高有效等級1B位元之某函數或者插入法取代，並傳遞至語音解碼器。將(來自聲音解密器之)等級2位元與(來自1/2比率迴旋解碼器之)16個最低有效等級1B位元傳遞至語音解器，連同傳遞之最後良框其等級1A位元與32個最高有效等級1B位元之函數或者插入法予以解碼。注意：等級2位元與16個最低有效等級1B位元中若有任何位元

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（4）

錯誤，則這類錯誤對語音品質較其餘之等級1B與等級1A位元中的錯誤具有感覺較小之衝擊。

合併一聲音加密器之先前技藝加密架構提供某些優點。第一，來自一外部來源之密碼(以下稱爲"外部密碼")無需同步化兩端之260位元固定的祕密罩幕(亦即於傳送器與接收器)，特徵爲：密碼係輸入以確保兩加密演算法彼此同步化之資料。第二，發生傳送錯誤時語音品質不會降低。等級1A位元與32個最高有效等級1B位元其傳送中之錯誤可使用最後良框其等級1A位元與32個最高有效等級1B位元之某函數或者插入法提供罩幕。然而，先前技藝加密架構係以兩種方式感測安全問題。首先260位元固定之祕密罩幕可使用已知之明文(亦即輸入至聲音加密器者)決定，然後該明文可用以理解(或者解密)加密之位元，進而符合傳送之訊息的安全性。其次即使已知之明文消失，亦可僅以相之鄰260位元框進行XOR而去除固定的祕密罩幕，並可提供有關代數碼激發之線性預測(ACELP)語音演算法之參數如何改變的資訊。因此，需存在一語音處理器架構，其無需使用外部密碼，並以最小之語音衰減提供加強的安全性。

發明概述

本發明係一加密語音處理器架構，其無需使用外部加密並以最小之語音衰減提供加強的安全性。此係藉由將一區塊加密器與一密鑰流產生器合併(而非像是實行於聲音加密器的一固定之祕密罩幕加密方案)，於傳送器一端將編碼之語音位元區塊加密而完成。該區塊加密器使用一可逆之加

經濟部智慧財產局員工消費合作社印製
（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（5）

密演算法與內部密碼將一編碼之語音位元其第一區塊轉換成一第一密文區塊，特徵爲：如果其傳送期間發生一錯誤(並且使用該錯誤位元，而非來自先前之良框其位元的某函數或者內插法)，則編碼之語音位元的第一區塊包括第一位準位元，將造成語音品質上有效之有感衰減。

然後第一密文區塊提供以作爲密鑰流產生器與一循環檢查碼(CRC)之輸入。密鑰流產生器使用一用以作爲一鎖碼之單向函數的可逆之加密演算法，以及內部密碼將第一密文區塊轉換成一密鑰流，特徵爲：加密之第一密文區塊。該密鑰流後續係用以將一編碼之語音位元的第二與第三區塊加密，分別產生一第二密文區塊與一第三密文區塊。特徵爲：如果一錯誤發生於第一密文區塊之傳送期間，且編碼之語音位元其第二區塊包括第一與第二位準位元，則編碼之語音位元其第三區塊包括第二位準位元，將造成語音品質上極小或者無感之衰減。

於循環檢查碼(CRC)中，第一密文區塊係用以產生錯誤控制位元，用以偵測是否一錯誤發生於第一密文區塊之傳送中－亦即，第一密文區塊係由某型態的傳送錯誤偵測機制所偵測。第一，第二與第三密文區塊及錯誤控制位元係循序處理並且傳送。

於接收器一端，錯誤控制位元與接收之第一密文區塊係用以決定是否一錯誤發生於第一密文區塊的傳送中。如果未偵測得錯誤，則接收之第一密文區塊以一區塊解密器解密，並用以(經由一與傳送器一端之密鑰流產生器相同的密

（請先閱讀背面之注意事項，填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（6）

鑰流產生器)將接收之第二與第三密文區塊解密。如果偵測得一錯誤，則(第一與第二密文區塊中之)第一位準位元使用一或更多最後良框其第一位準位元之某函數或者內插法而提供罩幂。(第二與第三密文區塊中之)第二位準位元係直接傳遞至一語音解碼器而非(誤予)解密，以便儲存處理之週期。

優點上，本發明之具體實施例不會將第一位準位元中之錯誤由此處蔓延。尤其，如果一錯誤發生於接收之第一密文區塊的任何位元中，則其將不蔓延至任何其他第一位準位元，因爲所有第一位準位元將由一或更多最後良框其第一位準位元之某函數或者內插法而提供罩幂。雖然發生於接收之第一密文區塊中任何位元的一錯誤將蔓延至第二位準位元，但這類錯誤將對語音品質僅爲極小或者無感之影響。注意如果接收之第一密文區塊中任何位元均無錯誤，則將不會有錯誤蔓延至任何其他第一位準或第二位準位元。且注意：第二與第三接收之密文區塊中任何錯誤將因爲密鑰流產生器的架構而不蔓延至其他位元，該密鑰流產生器架構中之密鑰流係與明文進行XOR。

再者，區塊加密器與密鑰流產生器進一步使用更具加密安全性之加密演算法(或者鎖碼之單向函數)，其中260位元固定之祕密罩幂用於先前技藝中所使用的聲音加密器。因此，本發明之加密語音處理器架構較先前技藝更具加密安全性。此外，內部密碼係用以同步化加密與解密之加密演算法。因此無需外部密碼。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（7）

圖示簡述

本發明之特性，方面與優點於考慮下列描述，附加主張，伴隨圖示後將可變得更爲了解，其中：

圖1說明一先前技藝語音處理器，錯誤防護，及聲音加密架構；

圖2說明一合併於一根據本發明而使用之傳送器內的語音處理器架構；

圖3說明一描述如本申案中所特徵化之編碼語音位元的表示圖；

圖4說明一根據本發明一具體實施例，使用加強之細胞式訊息加密演算法(ECMEA)，將48位元區塊之明文加密成密文的區塊加密器其功能區塊圖；

圖5說明一用以執行圖4中說明之區塊加密器其反轉功能的48位元區塊加密器一功能區塊圖；

圖6說明一根據本發明一具體實施例，使用加強之細胞式訊息加密演算法(ECMEA)密鑰流產生器之功能區塊圖；

圖7說明一合併於一根據本發明而使用之接收器內的語音處理器架構；

圖8說明一根據本發明一具體實施例，使用加強之細胞式訊息加密演算法(ECMEA)之40位元區塊加密器的一功能區塊圖；

圖9說明一用以執行圖8中說明之區塊加密器其反轉功能的40位元區塊加密器一功能區塊圖；以及

圖10說明一根據本發明一具體實施例，使用RC5之48位元

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（8）

區塊加密器的一功能區塊圖。

詳細描述

圖2說明一合併於一根據本發明而使用之傳送器30內的語音處理器架構。爲作說明之用途，此處本發明將參照一根據著名之分時多向近接(TDMA)的IS-136(及修正版)標準，以及代數碼激發之線性預測(ACELP)的IS-641標準之語音處理器架構而描述。然而，此不應藉由任何方法解釋而限制本發明。

傳送器30包含一語音處理器架構，具有語音編碼器32，區塊加密器34，密鑰流產生器36，XOR運算元38，40，七位元循環檢查碼(CRC)(7位元CRC)42，半數比率迴旋式編碼器(1/2比率CC)44，打孔器46與雙槽插入器48。該語音處理器架構可藉由執行於一電腦處理器，專用積體電路(ASIC)等軟體而實行。語音編碼器32，XOR運算元38，40，7-bit CRC 42半數比率迴旋式編碼器(1/2比率CC)44，打孔器46與雙槽插入器48皆於技藝中很著名。此處將描述區塊加密器34與密鑰流產生器36。

語音編碼器32接收一訊息框，特徵爲：160個傳送之16位元語音抽樣。爲了本申請案之用途，“語音抽樣”一詞將解釋成：包括但不限於語音資料，使用者資料或者控制頻道訊息。訊息框係藉由語音編碼器32編碼以產生輸出32，特徵爲：具有第一與第二位準編碼之語音位元的148個編碼之語音位元，特徵爲：第一位準(編碼之語音)位元代表：如果一傳送錯誤發生於第一區塊之任何位元中，則將明顯降

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（9）

低語音品質的語音特徵，而第二位準(編碼之語音)位元代表：如果一傳送錯誤發生於第一區塊之任何位元中，則將不會明顯降低語音品質的語音特徵。見圖3，其說明一表格45，描述如本申請案中所特徵化之編碼的語音位元。

編碼之語音位元後續係於三區塊中加以分攤及處理。第一區塊(此處同時稱爲等級1A或者輸出$_{32-1}$)包括48個第一位準位元；第二區塊(此處同時稱爲等級1B或者輸出$_{32-2}$)包括32個第一位準位元與16個第二位準位元；而第三區塊(此處同時稱爲等級2或者輸出$_{32-3}$)包括52個第二位準位元。尤其，相關第二區塊，第一位準位元係32個最高有效位元，而第二位準位元係16個最低有效位元。注意：本發明不應限制編碼之語音位元所分攤的區塊數，及各區塊中的位元數。由於如果一傳送錯誤發生，則第一位準位元將明顯降低語音品質，錯誤控制防護儘可能多應用於這些位元，特徵爲：錯誤控制防護係例如經由循環檢查碼(CRC)與迴旋碼提供。

來自語音編碼器32，等級1A位元(第一區塊)係提供以作爲區塊加密器34之輸入，等級1B位元(第二區塊)係提供以作爲XOR運算元38之輸入，而等級2位元(第三區塊)係提供以作爲XOR運算元40之輸入。區塊加密器34使用一可逆之加密演算法，其具有一相關於希望之接收器的密鑰，用以將明文區塊加密成密文。這類加密演算法之例子包括RC5以及加強之細胞式訊息加密演算法(ECMEA)。RC5係由Ron Rivest所開發，且於技藝中很著名。加強之細胞式訊息加密

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

90.3.08 年 月 日 修正 補充
A7
B7

五、發明說明（10）

演算法(ECMEA)係由Robert Rance，Daniel Heer，Semyon Mizikovsky, et. al所開發。加強之細胞式訊息加密演算法(ECMEA)係揭示於一九九七年十月二十八日之電信工業協會(TIA)TR45 Ad-Hoc認證群組會議，由電信工業協會(TIA)會員出席，並且由電信工業協會(TIA)對於出口行政調整中所指定之美國商業部的出口法規(統稱所包含之15個CFR部分730至774)，開放有限度及控制下之分配。

區塊加密器34中，等級1A位元係加密以產生輸出$_{34}$，特徵為： 48個等級1A之密文位元(或者一第一密文區塊)。圖4說明一區塊加密器34之功能區塊圖，該區塊加密器根據本發明一具體實施例使用加強之細胞式訊息加密演算法(ECMEA)將48位元明文區塊加密成密文。區塊加密器包含第一、第二、第三與第四函數呼叫52、54、58與60(以加密模式作業用以加密其輸入)以及XOR運算元56。等級1A位元其一第一與一第二16位元部分(以下分別稱為第一與第二等級1A部分)係提供以作為第一與第二加強之細胞式訊息加密演算法(ECMEA)函數呼叫52，54之輸入。第一加強之細胞式訊息加密演算法(ECMEA)函數呼叫52使用第二等級1A部分作為密碼輸入，將第一等級1A部分加密，以產生16位元輸出$_{52}$。

因為於技藝中很著名，密碼係作為同步化加密與解密其加密演算法之用途。然而，尤其對於加強之細胞式訊息加密演算法(ECMEA)，密碼同時用以作為鎖碼位元，以加強加強之細胞式訊息加密演算法(ECMEA)之加密強度。此一角色中，加強之細胞式訊息加密演算法(ECMEA)係用以作

煩請委員明示 90年3月8日所提之修正本有無變更實質內容是否准予修正。
經濟部中央標準局員工消費合作社印製
（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90. 3. 08
年 月 日
A7
B7
修正
補充

五、發明說明（11）

為一鎖碼之攪亂功能，以同時集中第一與第二等級1A部分之加密，並且增加48位元區塊加密器之整體加密強度。

輸出52係於XOR運算元56中與等級1A位元的一第三16位元部分(以下稱為一第三等級1A部分)進行XOR，以產生16位元輸出56。

輸出56提供作為第二與第三加強之細胞式訊息加密演算法(ECMEA)54，58之輸入。第二加強之細胞式訊息加密演算法(ECMEA) 54使用輸出56作為密碼，將第一與第二等級1A部分加密，並分別產生16位元輸出54-1與16位元輸出54-2。第三加強之細胞式訊息加密演算法(ECMEA) 函數呼叫58使用輸出54-2作為密碼而將輸出56與輸出54-1加密，以分別產生16位元輸出58與16位元輸出58-2。第四加強之細胞式訊息加密演算法(ECMZA)函數呼叫60使用輸出58-1作為密碼而將輸出58-2與輸出54-2加密，以產生32位元輸出60。圖5說明一48位元解密器35的一功能區塊圖，該解密器用以執行圖4中說明之區塊加密器34的反轉功能。

輸出58與輸出54-2整體包含區塊加密器34之輸出34。輸出34係提供以作為七位元循環檢查碼(CRC)(7位元CRC)42，半數比率迴旋式編碼器(1/2比率CC) 44及密鑰流產生器36之輸入。於七位元循環檢查碼(CRC)(7位元CRC)42中，輸出34係用以產生輸出42，特徵為：7個錯誤控制位元。輸出42後續係提供以作為半數比率迴旋式編碼器(1/2比率CC)44之輸入。

密鑰流產生器36係由48個等級1A之密文位元(亦即輸出34)驅動，於區塊加密器34之輸入端重覆足夠次數，以填滿一104位元之區塊。密鑰流產生器36中，等級1A密文位元係加

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（12）

密以產生密鑰流輸出$_{36}$，特徵爲：100位元加密之等級1A的密文位元。尤其，輸出$_{36}$之產生係藉由以加密之公開的已知擬亂資料，實際上即爲等級1A密文位元，執行(由密鑰流產生器36所使用之)加密演算法。注意：(由於特徵爲：104位元區塊)將丟棄4個等級1A密文位元，因爲加強之細胞式訊息加密演算法(ECMEA)(以及大部分其他區塊演算法）僅加密整數數目之位元。

圖6說明一密鑰流產生器36之功能區塊圖，其根據本發明一具體實施例而使用加強之細胞式訊息加密演算法(ECMEA)。密鑰流產生器36包含加強之細胞式訊息加密演算法(ECMEA) 函數呼叫62，用以接收104位元區塊輸入，特徵爲：(來自區塊加密器34之)重覆的輸出$_{34}$。注意，區塊加密器34之輸出係添加或者自我串接以提供96位元，然後再部分添加一次，以提供一104位元區塊輸入予密鑰流產生器。該104位元區塊輸入係藉由加強之細胞式訊息加密演算法(ECMEA)函數呼叫62使用輸出$_{34}$之16個最高有效位元(亦即48個等級1A密文位元其16個最高有效位元)作爲密碼而加密，以產生輸出$_{36}$。

輸出$_{36}$係提供以作爲XOR運算元38與40之輸入。尤其，輸出$_{36}$一48位元部分係提供以作爲XOR運算元38之輸入，而輸出$_{36}$一52位元部分係提供以作爲XOR運算元40之輸入。於XOR運算元38中，等級1B位元(亦即第二區塊)係與輸出$_{36}$之48位元部分進行XOR，以產生輸出$_{38}$，特徵爲：48位元等級1B密文位元(亦即第二密文區塊)。然後輸出$_{38}$係

經濟部智慧財產局員工消費合作社印製

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（13）

提供以作爲半數比率迴旋式編碼器(1/2比率CC)44之輸入。類似地，於XOR運算元40中，等級2位元(亦即第三區塊)係與輸出$_{36}$之52位元部分進行XOR，以產生輸出$_{40}$，特徵爲：52個等級2密文位元(亦即第三密文區塊)。然後輸出$_{40}$提供以作爲雙槽插入器48之輸入。

於半數比率迴旋式編碼器(1/2比率CC)44中，輸出$_{42}$，輸出$_{34}$與輸出$_{38}$伴隨5個尾碼位元(特徵爲：迴旋碼狀態資訊)係用以產生輸出$_{44}$，特徵爲：216個代碼字位元。輸出$_{44}$提供予打孔器46，以產生輸出$_{46}$，特徵爲：208個打孔之代碼字位元。然後輸出$_{46}$提供予輸出$_{40}$進行位元插入之雙槽插入器48，以產生輸出$_{48}$，特徵爲：260個插入之位元。輸出$_{48}$後續予以多工化，調變並由傳送器30傳送。

傳送之訊息係由一執行傳送器10之反轉功能的接收器接收。圖7說明一合併於一接收器70內之語音處理器架構，該接收器係根據本發明而使用。接收器70包含一語音處理器架構，具有語音解碼器72，區塊解密器74，密鑰流產生器76，XOR運算元78，80，7位元循環檢查碼(CRC)82，1/2比率迴旋解碼器84以及雙槽位元解插入器86。語音處理器架構可由執行於一電腦處理器之軟體，專用積體電路(ASIC)等實行。語音解碼器72，XOR運算元78，80，7位元循環檢查碼(CRC)82，1/2比率迴旋解碼器84，以及雙槽位元解插入器86均於技藝中很著名。此處將描述區塊解密器74與密鑰流產生器76。

於接收所傳送之訊息時，接收器將傳送之訊息解調變並

經濟部智慧財產局員工消費合作社印製
（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

90.3.08 修正
年 月 日 補充
A7
B7

五、發明說明（14）

且多工化，以獲得輸出48'(亦即260個插入之位元)，特徵為：該主要記號將解釋為用以指示一傳送版本所對應之接收版本。雙槽位元解插入器86使用輸出48'以產生輸出46'(亦即208個打孔之代碼字位元與52個等級2密文位元或為第三密文區塊)。然後208個打孔之字代碼位元藉由1/2比率迴旋解碼器84解迴旋，以取得5個尾碼位元，輸出42'(亦即7個錯誤控制位元），輸出34'(亦即48個等級1A密文位元或為第一密文區塊）與輸出38'(亦即48個等級1B密文位元或為第二密文區塊)。注意：於XOR運算元80中沒有作業係用以反轉打孔器46之清除字元插入處理。清除字元插入所造成之位元損失係由接收器中的1/2比率迴旋解碼器84恢復。

輸出34'係提供以作為7位元循環檢查碼(CRC)82之輸入，以產生一第二組之7個錯誤控制位元(特徵為：第一組之7個錯誤控制位元統合包含輸出42'，係由1/2比率迴旋解碼器所輸出之7個錯誤控制位元)。檢查第一與第二組之錯誤控制位元，以決定第一密文區塊(亦即等級1A密文位元)之傳送中是有錯誤(亦即決定是否有壞框存在)。如果沒有傳送錯誤發生，則輸出34'(亦即等級1A密文位元)傳遞至區塊解密器74以及密鑰流產生器76。操作區塊解密器以執行區塊加密器34之反轉功能。見圖5，說明一48位元之解密器35的功能區塊圖，該解密器35用以執行圖4中所說明之區塊加密器34的反轉功能。密鑰流產生器76係與密鑰流產生器36相同。

於區塊解密器74中，輸出34'係解密以獲得輸出32-1'(亦即48個等級1A位元)。於密鑰流產生器76中，輸出34'係用以產

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90.3.08 修正
年 月 日 補充
A7
B7

五、發明說明（15）

生一密鑰流輸出36'（亦即100個解密之等級1A密文位元）。然後密鑰流係用以將輸出38'（亦即等級1B密文位元）與輸出40'（亦即等級2密文位元）進行XOR，以便獲得輸出32-2'（亦即等級1B位元）與輸出32-3'（亦即等級2位元）。輸出32-1'，輸出32-2'與輸出32-3'（亦即等級1A位元，等級1B位元與等級2位元）係由語音解碼器72解碼，以獲得原始訊息框。

如果一傳送錯誤發生，則丟棄第一位準位元（亦即等級1A位元與32個最高有效等級1B位元），並以一或更多前一良框其第一位準位元之某函數或者插入法（如著名之IS-641標準中所述）取代。並傳遞至語音解碼器72。無需將等級1A位元區塊解密，或者（使用密鑰流產生器76）產生一密鑰流，因為這些資料將不當地給定一失效之循環檢查碼（CRC）。因此不可能解密第二位準位元（亦即等級2位元與16個最低有效等級1B位元）。避免這些工作將可儲存處理器週期。這些維持加密之第二位準位元所造成的語音品質降低僅為極小或者無感之衝擊。

注意：FACCH與SACCH加密可由本發明以一相似方式提供聲音之隱密性，其中密碼係源自內部而非外部。各FACCH與SACCH訊息之第一字包括一8位元訊息型態，需維持未加密。因此，各FACCH或者SACCH 之第一字將使用如圖8（與圖9）中所示一40位元加密器XOR運算元80（與解密器90），而其餘字將使用圖4之48位元區塊加密器。

雖然本發明以重要細節並參照某些具體實施例而描述，但亦可有其他修訂。例如，可能有其他加密器與解密器。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（16）

見圖10，說明一使用RC5之48位元區塊加密器100。熟知此項技藝人士將明顯可見：可使用其他型態之語音編碼器，錯誤控制機制與加密及/或加密演算法，將本發明之觀念應用於語音處理器架構。因此，本發明之精神與範圍將不限於此處所包含的具體實施例之描述。

（請先閱讀背面之注意事項，填寫本頁）

裝 訂 線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90.3.08 修正 補充
年 月 日
A7
B7

五、發明說明（16a）

元件符號說明：

10	傳送器	48	雙槽插入器
12	語音編碼器	48'	輸出
14	七位元循環檢查碼	52	第一函數呼叫
16	半數比率迴旋式編碼器	52'	輸出
18	打孔器	54	第二函數呼叫
20	聲音加密器	54-1'	輸出
22	雙槽插入器	54-2'	輸出
30	傳送器	56	XOR運算元
32	語音編碼器	56'	輸出
32-1'	輸出	58	第三函數
32-2'	輸出	58-1'	輸出
32-3'	輸出	58-2'	輸出
34	區塊加密器	60	第四函數呼叫
34'	輸出	60'	輸出
36	密鑰流產生器	72	語音解碼器
36'	輸出	74	區塊解密器
38,40	XOR運算元	76	密鑰流產生器
38'	輸出	78, 80	XOR運算元
40'	輸出	82	七位元循環檢查碼
42	七位元循環檢查碼	84	1/2比率迴旋解碼器
42'	輸出	85	循環檢查碼檢查
44	半數比率迴旋式編碼器	86	雙槽位元解插入器
46	打孔器	90	解密器
46'	輸出	100	48位元區塊加密器
45	表格		

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A5
B5

四、中文發明摘要（發明之名稱：加密語音編碼器）

本發明係一加密語音處理器架構，其無需使用外部密碼並以最小之語音衰減提供加強的安全性。此係藉由將一區塊加密器(34)與一密鑰流產生器(36)合併(而非像是實行於聲音加密器一固定之祕密罩幕加密方案)，於傳送器一端將編碼之語音位元區塊加密而完成。區塊加密器(34)使用一可逆之加密演算法與內部密碼將一編碼之語音位元其第一區塊轉換成一第一密文區塊(輸出34)。該第一密文區塊(輸出34)係用以產生一密鑰流(輸出36)，用以將一第二密文區塊加密(圖2)。

英文發明摘要（發明之名稱：ENCRYPTING SPEECH CODER）

The present invention is an encrypting speech processor architecture that provides enhanced security without the use of external cryptosync and with minimal speech degradation. This is accomplished by incorporating a block encryptor (34) and a keystream generator (36) (instead of a fixed secret mask encryption scheme, such as those implemented in voice ciphers) for encrypting blocks of encoded speech bits at a transmitter side. The block encryptor (34) employs an invertible cryptographic algorithm and internal cryptosync to convert a first block of encoded speech bits into a first ciphertext block (output 34). The first ciphertext block (output 34) is used to generate a keystream (output 36), which is then used to encrypt a second ciphertext block (FIG. 2).

（請先閱讀背面之注意事項再填寫本頁各欄）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

1. 一種用以將一訊息框加密之方法，該訊息框包括一第一區塊，具有第一位準編碼之語音位元，以及一第二區塊，具有第二位準編碼之語音位元，該方法係特徵化爲下列步驟：

將第一區塊加密，以產生一第一密文區塊；

使用第一密文區塊產生一位元密鑰流；

使用該位元密鑰流將第二區塊加密，以產生一第二密文區塊；以及

使用第一密文區塊產生錯誤控制位元。

2. 如申請專利範圍第1項之方法，特徵爲：第二區塊進一步包括第一位準編碼之語音位元。

3. 如申請專利範圍第1項之方法，特徵爲：第一區塊包含48個第一位準位元。

4. 如申請專利範圍第1項之方法，特徵爲：第二區塊包含52個第二位準位元。

5. 如申請專利範圍第1項之方法，特徵爲：該訊息框進一步包括一第三區塊，具有第一位準編碼之語音位元與第二位準編碼之語音位元，該方法進一步特徵爲下列額外步驟：

使用位元密鑰流將第三區塊加密，以產生一第三密文區塊。

6. 如申請專利範圍第1項之方法，特徵爲：該產生位元密鑰流之步驟之特徵爲下列步驟：

重覆第一密文區塊，以產生一重覆之第一密文區塊；

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

六、申請專利範圍

以及

使用第一密文區塊之一部分將重覆的第一密文區塊加密，以產生位元密鑰流。

7. 如申請專利範圍第1項之方法，進一步之特徵爲下列額外步驟：

使用第一密文區塊產生錯誤控制位元。

8. 如申請專利範圍第1項之方法，特徵爲：該加密第一區塊之步驟的特徵爲下列步驟：

使用一密文區塊之第二部分作爲密碼而加密一第一密文區塊之第一部分，以產生一第一輸出；

使用一二元運算將第一輸出與一第一密文區塊之第三部分組合，以產生一第二輸出；

使用第二輸出作爲密碼將第一密文區塊之第一與第二部分加密，以產生一具有一第一部分與一第二部分之第三輸出；

使用第三輸出之第二部分作爲密碼將第二輸出與第三輸出之第一部分加密，以產生一具有一第一與一第二部分之第四輸出；以及

使用第四輸出之第一部分作爲密碼將第四輸出之第一部分與第三輸出之第二部分加密，以產生一第五輸出。

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

8810137

圖 1

先前技藝 10

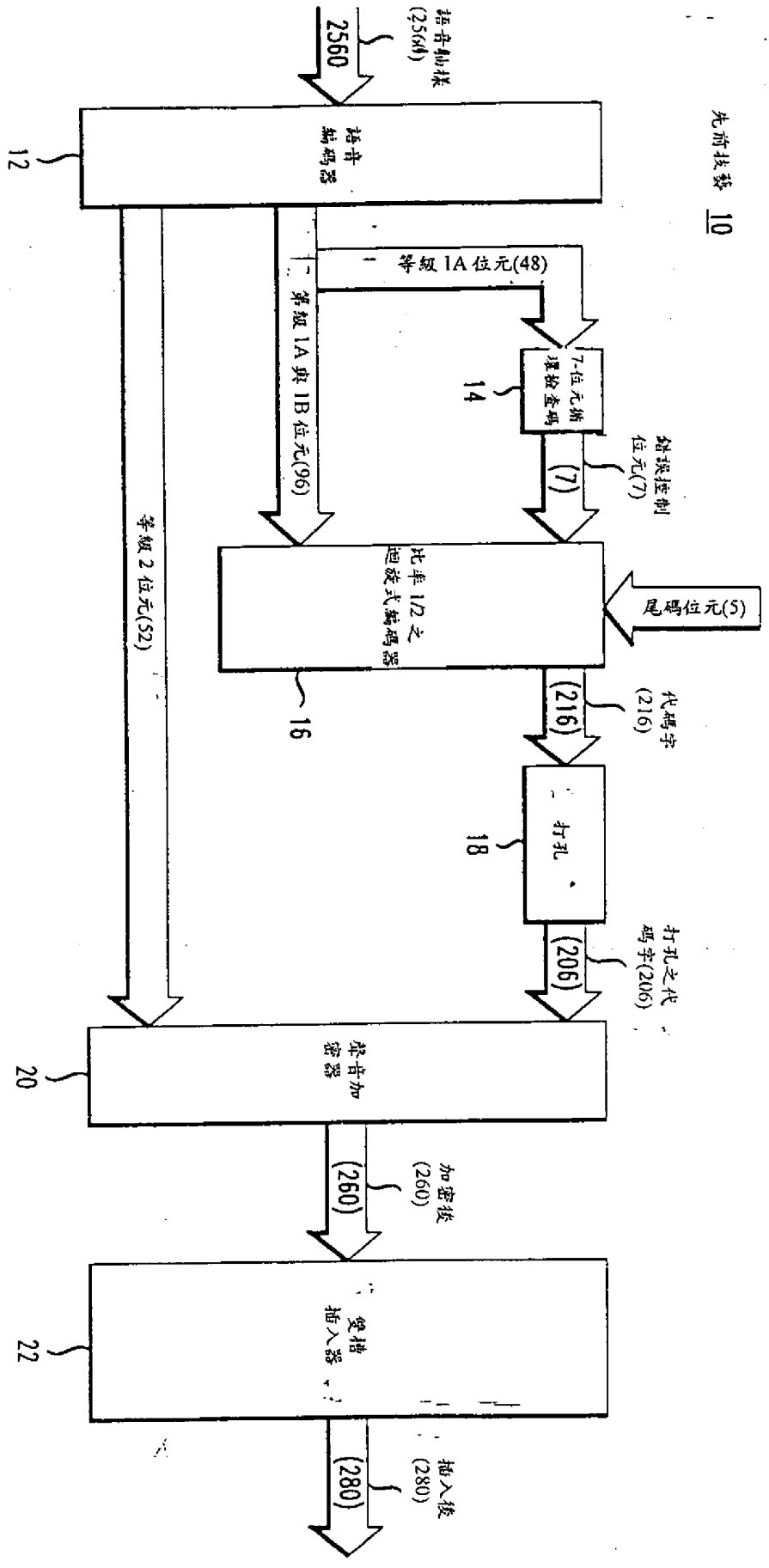


圖 2

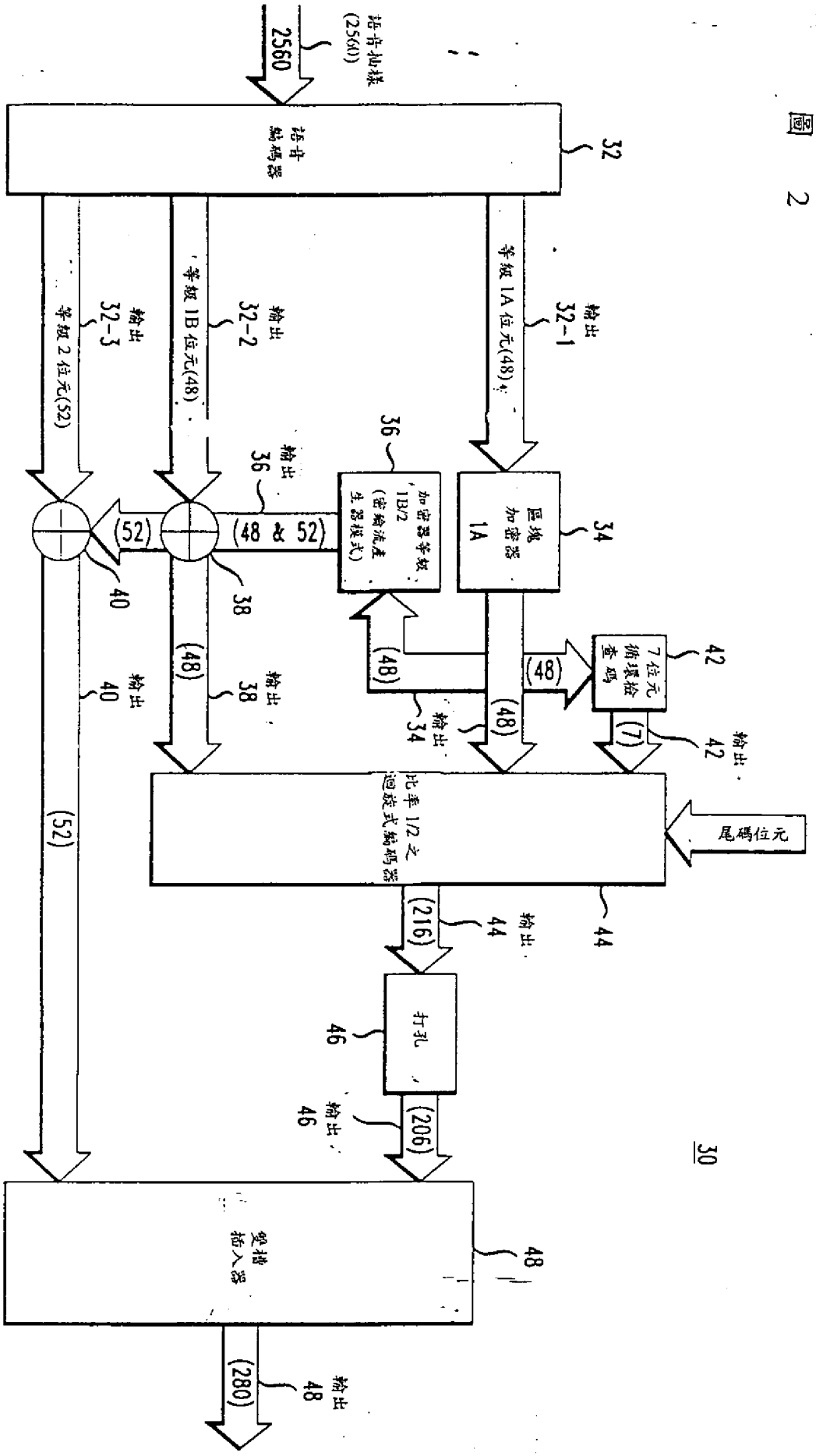

話音抽樣
(2560)
2560
話音
編碼器
32
輸出
32-1
等級 1A 位元(48)
輸出
32-2
等級 1B 位元(48)
輸出
32-3
等級 2 位元(52)
36
加密器等級
1B/2
(密鑰流產
生器模式)
輸出
36
(48 或 52)
區塊
加密器
1A
34
(52)
40
38
(48)
輸出
40
輸出
38
(48)
輸出
34
(48)
(48)
7 位元
循環檢
查碼
42
(7)
輸出
42
尾碼位元
比率 1/2 之
迴旋式編碼器
44
輸出
44
(216)
打孔
46
輸出
46
(206)
(52)
30
資料
插入器
48
(280)
輸出
48

圖 3

45

<table>
<tr><td colspan="3">148 個編碼之語音位元</td></tr>
<tr><td colspan="2">80 個第一位準位元</td><td>68 個第二位準位元</td></tr>
<tr><td>輸出 32-1</td><td>輸出 32-2</td><td>輸出 32-3</td></tr>
<tr><td>第一區塊</td><td>第二區塊</td><td>第三區塊</td></tr>
<tr><td>48 個等級 1A 位元</td><td>48 個等級 1B 位元
32 個第一位準位元
16 個第二位準位元</td><td>52 個等級 2 位元</td></tr>
</table>

90. 3. 8 修正補充
年 月 日

圖 4

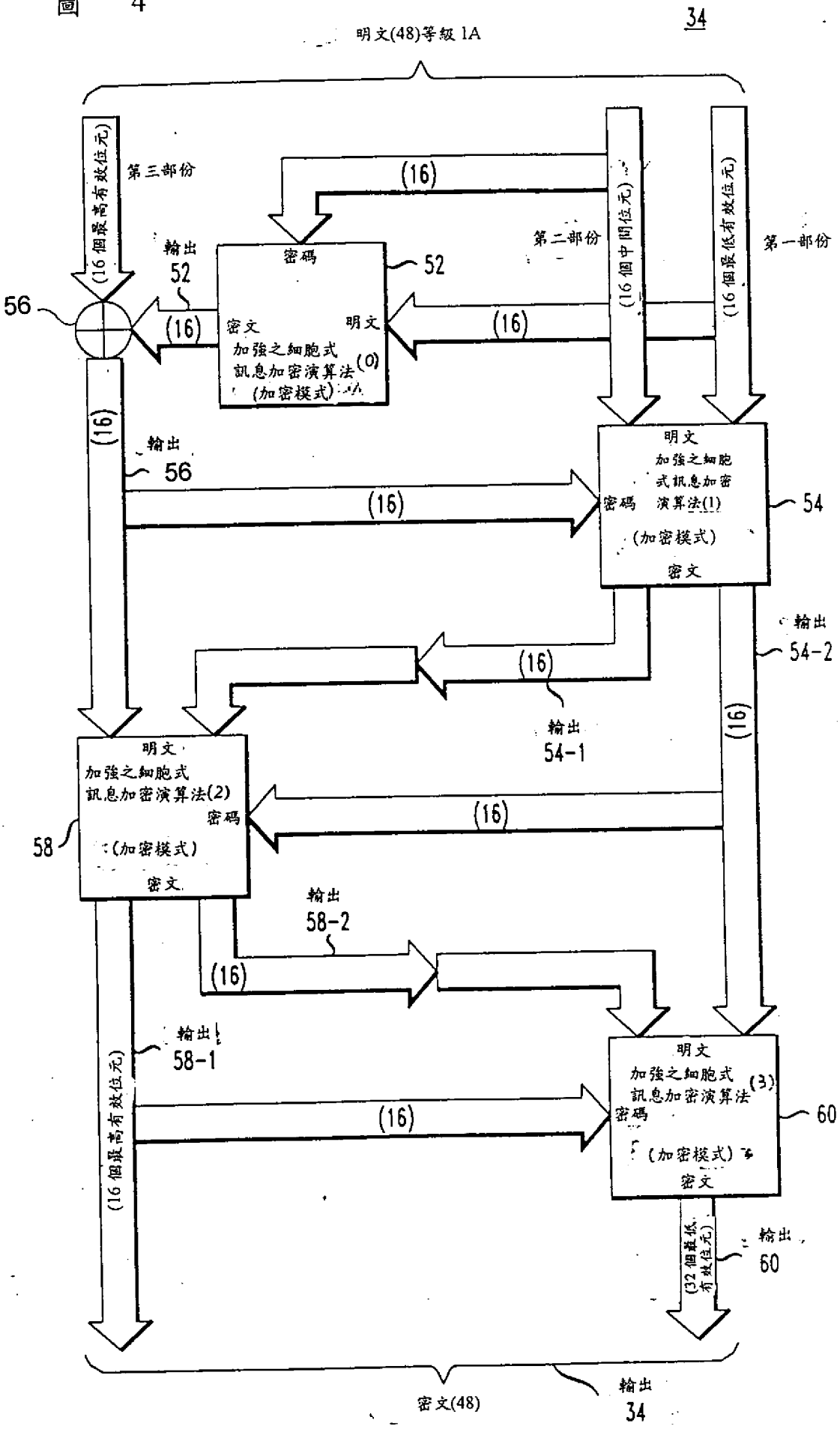


圖 5

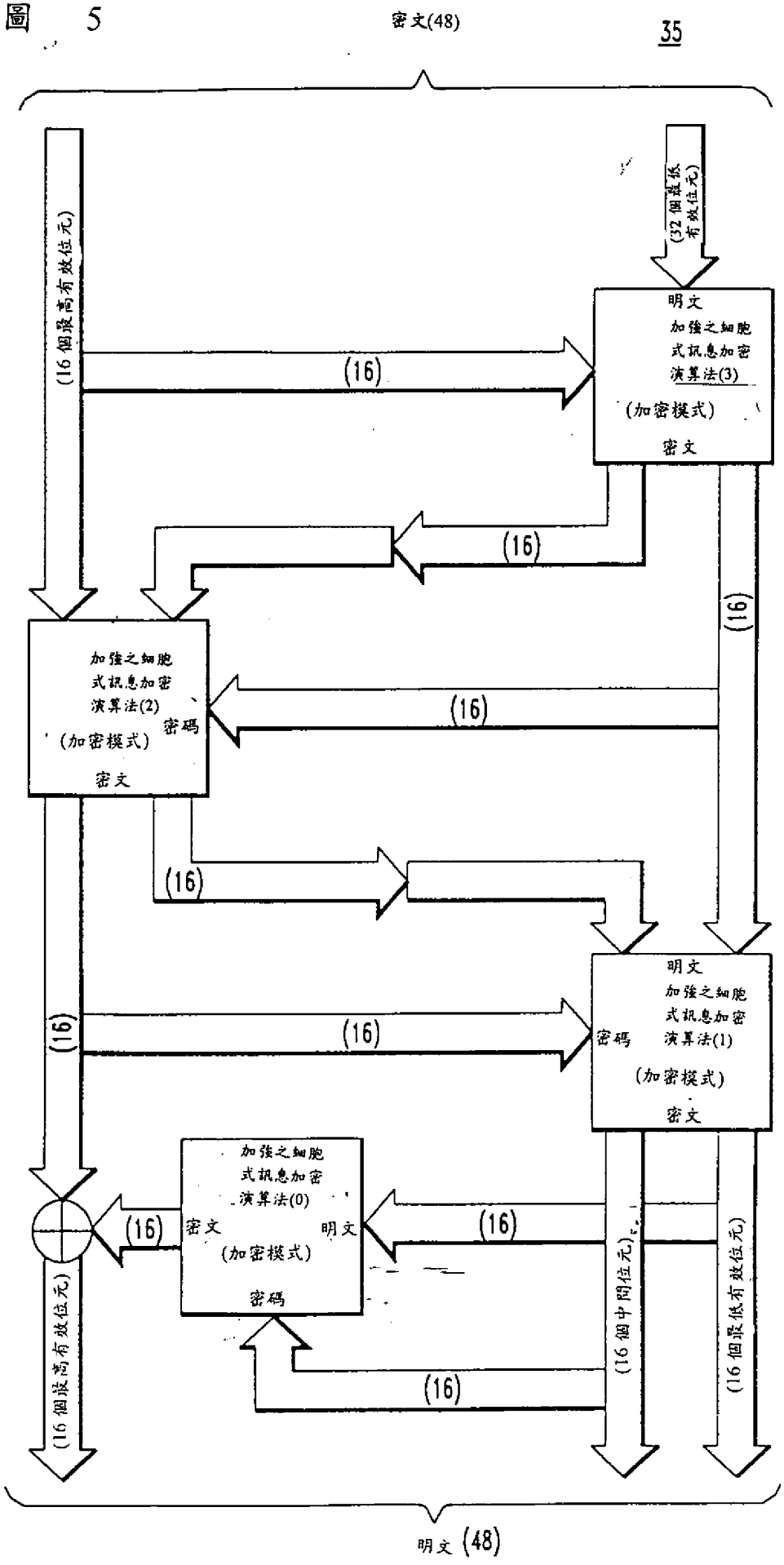
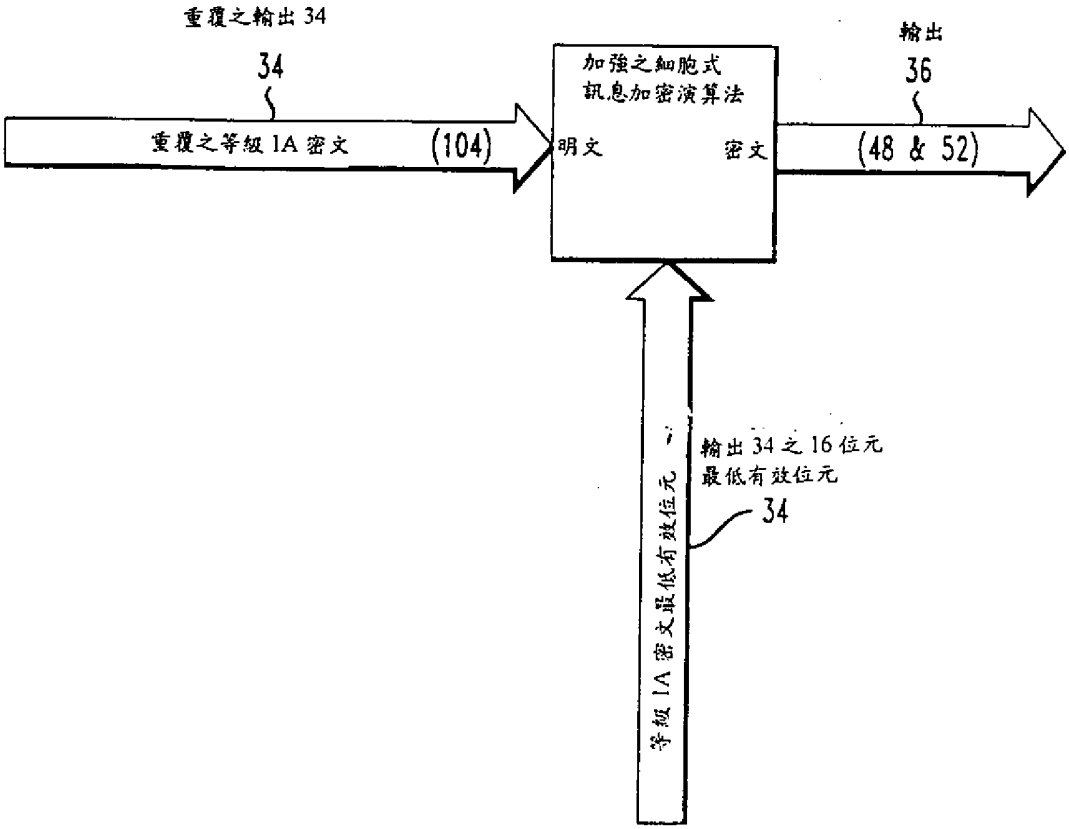

密文(48)
35
(32個最低有效位元)
(16個最高有效位元)
明文
加強之細胞式訊息加密演算法(3)
(加密模式)
密文
(16)
(16)
(16)
加強之細胞式訊息加密演算法(2)
密碼
(加密模式)
密文
(16)
(16)
(16)
明文
加強之細胞式訊息加密演算法(1)
密碼
(加密模式)
密文
(16)
加強之細胞式訊息加密演算法(0)
密文
明文
(加密模式)
密碼
(16)
(16)
(16)
(16個最高有效位元)
(16個中間位元)
(16個最低有效位元)
明文(48)

圖 6


重覆之輸出 34
34
重覆之等級 1A 密文
(104)
加強之細胞式
訊息加密演算法
明文
密文
輸出
36
(48 & 52)
等級 1A 密文最低有效位元
輸出 34 之 16 位元
最低有效位元
34

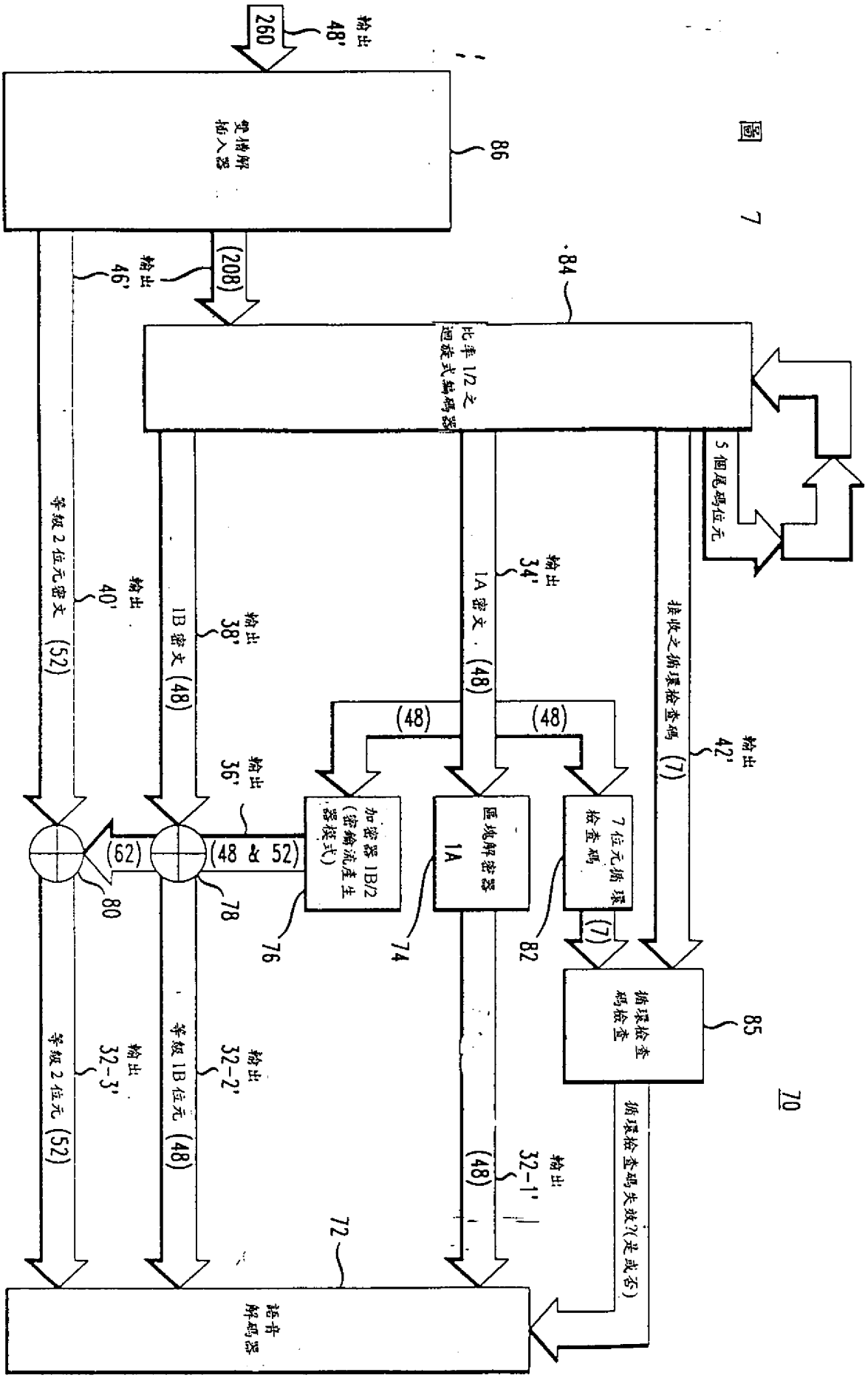

輸出
48'
260
86
(208)
輸出
46'
84
比率 1/2 之
迴旋式編碼器
5 個尾碼位元
輸出
34'
1A 密文 (48)
接收之循環檢查碼 (7)
輸出
42'
等級 2 位元密文 (52)
輸出
40'
1B 密文 (48)
輸出
38'
(48)
(48)
輸出
36'
(62)
(48 或 52)
加密器 1B/2
(密鑰流產生
器模式)
區塊解密器
1A
7 位元循環
檢查碼
(7)
循環檢查
碼檢查
85
80
78
76
74
82
循環檢查碼失效?(是或否)
輸出
32-3'
輸出
32-2'
輸出
32-1'
等級 2 位元 (52)
等級 1B 位元 (48)
(48)
72
語音
解碼器
70

圖 7

456127

圖 8

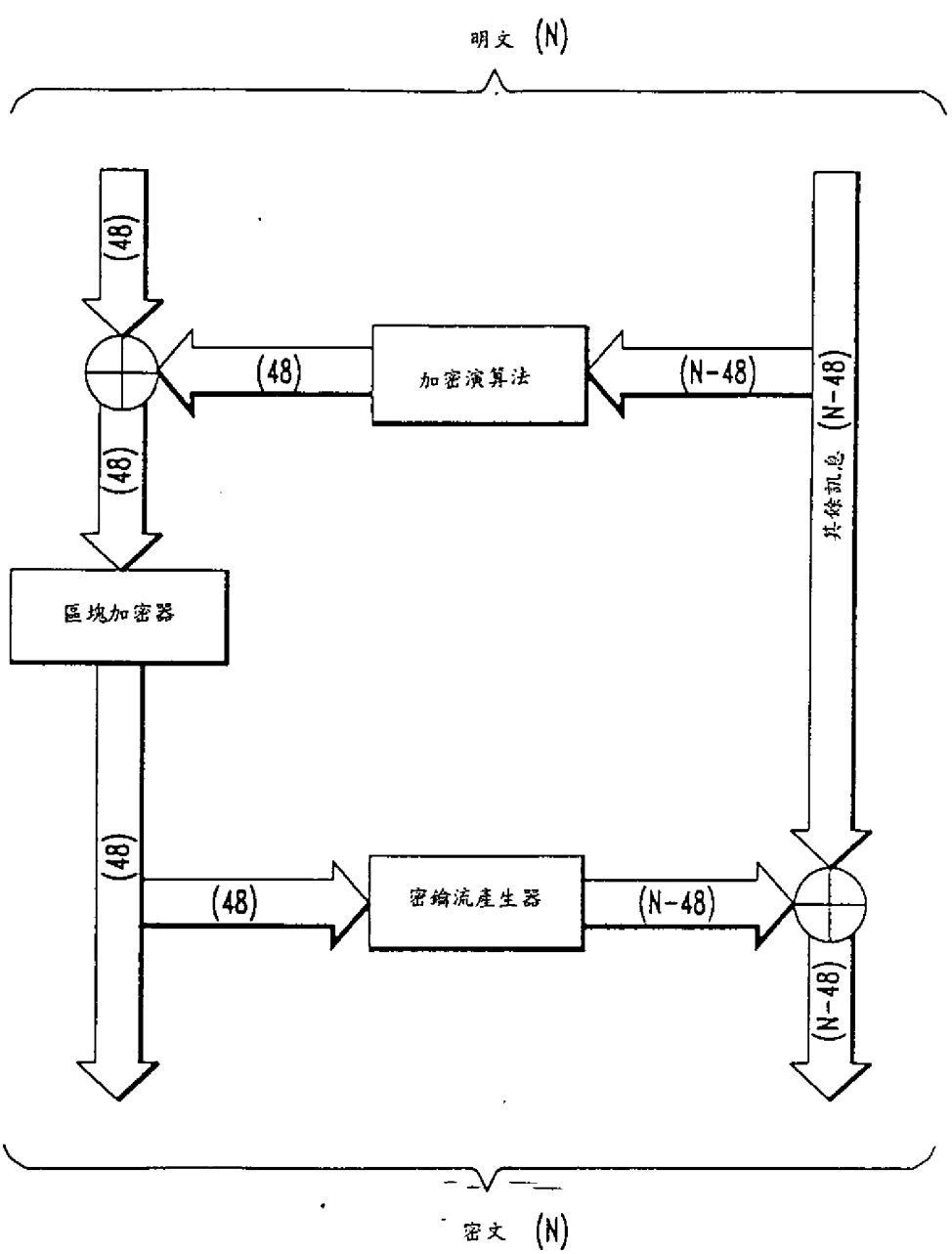

80
明文 (N)
(48)
(48)
加密演算法
(N-48)
(N-48)
其餘訊息
(48)
區塊加密器
(48)
(48)
密鑰流產生器
(N-48)
(N-48)
密文 (N)

圖 9

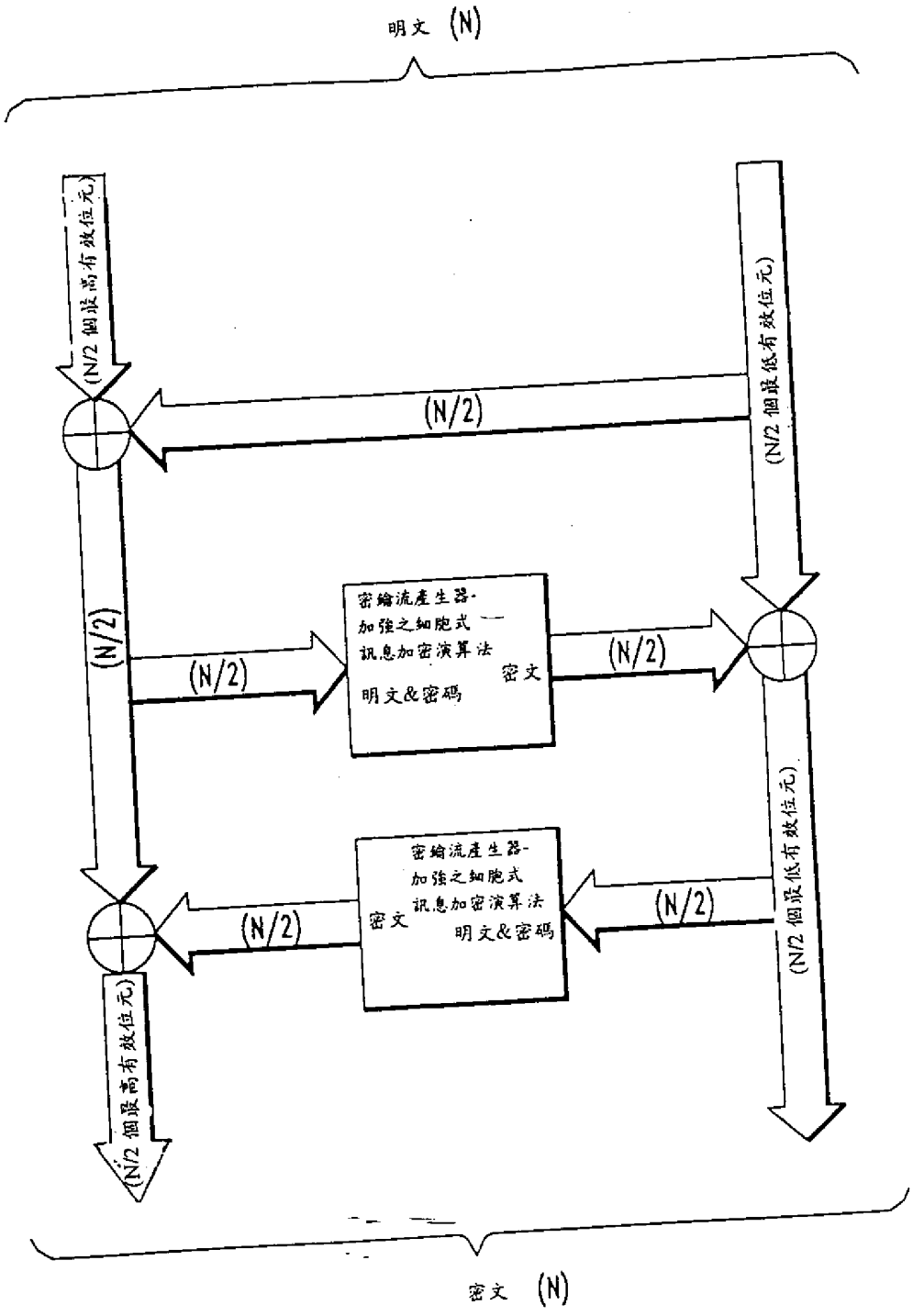
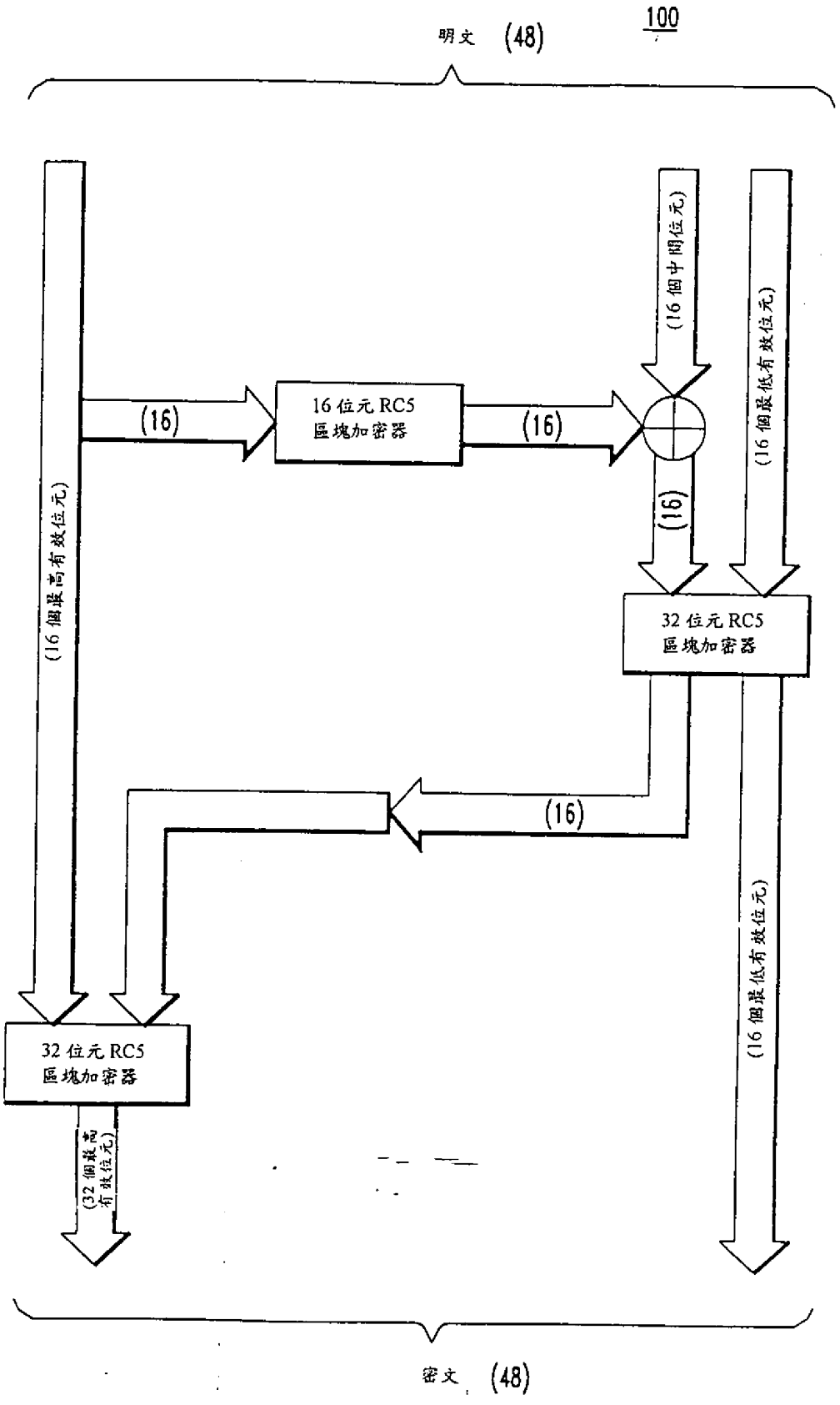

明文 (N)
(N/2 個最高有效位元)
(N/2)
(N/2 個最低有效位元)
(N/2)
密鑰流產生器-
加強之細胞式
訊息加密演算法
明文&密碼
密文
(N/2)
(N/2)
密鑰流產生器-
加強之細胞式
訊息加密演算法
密文
明文&密碼
(N/2)
(N/2 個最低有效位元)
(N/2 個最高有效位元)
密文 (N)

圖 10


100
明文 (48)
(16 個最高有效位元)
(16)
16 位元 RC5
區塊加密器
(16)
(16 個中間位元)
(16 個最低有效位元)
(16)
32 位元 RC5
區塊加密器
(16)
32 位元 RC5
區塊加密器
(32 個最高有效位元)
(16 個最低有效位元)
密文 (48)

90.3.08 年 月 日 修正 補充
A7
B7

五、發明說明（10）

演算法(ECMEA)係由Robert Rance，Daniel Heer，Semyon Mizikovsky, et. al所開發。加強之細胞式訊息加密演算法(ECMEA)係揭示於一九九七年十月二十八日之電信工業協會(TIA)TR45 Ad-Hoc認證群組會議，由電信工業協會(TIA)會員出席，並且由電信工業協會(TIA)對於出口行政調整中所指定之美國商業部的出口法規(統稱所包含之15個CFR部分730至774)，開放有限度及控制下之分配。

區塊加密器34中，等級1A位元係加密以產生輸出$_{34}$，特徵為： 48個等級1A之密文位元(或者一第一密文區塊)。圖4說明一區塊加密器34之功能區塊圖，該區塊加密器根據本發明一具體實施例使用加強之細胞式訊息加密演算法(ECMEA)將48位元明文區塊加密成密文。區塊加密器包含第一、第二、第三與第四函數呼叫52、54、58與60(以加密模式作業用以加密其輸入)以及XOR運算元56。等級1A位元其一第一與一第二16位元部分(以下分別稱為第一與第二等級1A部分)係提供以作為第一與第二加強之細胞式訊息加密演算法(ECMEA)函數呼叫52，54之輸入。第一加強之細胞式訊息加密演算法(ECMEA)函數呼叫52使用第二等級1A部分作為密碼輸入，將第一等級1A部分加密，以產生16位元輸出$_{52}$。

因為於技藝中很著名，密碼係作為同步化加密與解密其加密演算法之用途。然而，尤其對於加強之細胞式訊息加密演算法(ECMEA)，密碼同時用以作為鎖碼位元，以加強加強之細胞式訊息加密演算法(ECMEA)之加密強度。此一角色中，加強之細胞式訊息加密演算法(ECMEA)係用以作

煩請委員明示 90年3月8日所提之修正本有無變更實質內容是否准予修正。
經濟部中央標準局員工消費合作社印製
（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90. 3. 08
年 月 日
A7
B7
修正
補充

五、發明說明（11）

為一鎖碼之攪亂功能，以同時集中第一與第二等級1A部分之加密，並且增加48位元區塊加密器之整體加密強度。

輸出52係於XOR運算元56中與等級1A位元的一第三16位元部分(以下稱為一第三等級1A部分)進行XOR，以產生16位元輸出56。

輸出56提供作為第二與第三加強之細胞式訊息加密演算法(ECMEA)54，58之輸入。第二加強之細胞式訊息加密演算法(ECMEA) 54使用輸出56作為密碼，將第一與第二等級1A部分加密，並分別產生16位元輸出54-1與16位元輸出54-2。第三加強之細胞式訊息加密演算法(ECMEA) 函數呼叫58使用輸出54-2作為密碼而將輸出56與輸出54-1加密，以分別產生16位元輸出58與16位元輸出58-2。第四加強之細胞式訊息加密演算法(ECMZA)函數呼叫60使用輸出58-1作為密碼而將輸出58-2與輸出54-2加密，以產生32位元輸出60。圖5說明一48位元解密器35的一功能區塊圖，該解密器用以執行圖4中說明之區塊加密器34的反轉功能。

輸出58與輸出54-2整體包含區塊加密器34之輸出34。輸出34係提供以作為七位元循環檢查碼(CRC)(7位元CRC)42，半數比率迴旋式編碼器(1/2比率CC) 44及密鑰流產生器36之輸入。於七位元循環檢查碼(CRC)(7位元CRC)42中，輸出34係用以產生輸出42，特徵為：7個錯誤控制位元。輸出42後續係提供以作為半數比率迴旋式編碼器(1/2比率CC)44之輸入。

密鑰流產生器36係由48個等級1A之密文位元(亦即輸出34)驅動，於區塊加密器34之輸入端重覆足夠次數，以填滿一104位元之區塊。密鑰流產生器36中，等級1A密文位元係加

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90.3.08 修正
年 月 日 補充
A7
B7

五、發明說明（14）

且多工化，以獲得輸出48'(亦即260個插入之位元)，特徵為：該主要記號將解釋為用以指示一傳送版本所對應之接收版本。雙槽位元解插入器86使用輸出48'以產生輸出46'(亦即208個打孔之代碼字位元與52個等級2密文位元或為第三密文區塊)。然後208個打孔之字代碼位元藉由1/2比率迴旋解碼器84解迴旋，以取得5個尾碼位元，輸出42'(亦即7個錯誤控制位元），輸出34'(亦即48個等級1A密文位元或為第一密文區塊）與輸出38'(亦即48個等級1B密文位元或為第二密文區塊)。注意：於XOR運算元80中沒有作業係用以反轉打孔器46之清除字元插入處理。清除字元插入所造成之位元損失係由接收器中的1/2比率迴旋解碼器84恢復。

輸出34'係提供以作為7位元循環檢查碼(CRC)82之輸入，以產生一第二組之7個錯誤控制位元(特徵為：第一組之7個錯誤控制位元統合包含輸出42'，係由1/2比率迴旋解碼器所輸出之7個錯誤控制位元)。檢查第一與第二組之錯誤控制位元，以決定第一密文區塊(亦即等級1A密文位元)之傳送中是有錯誤(亦即決定是否有壞框存在)。如果沒有傳送錯誤發生，則輸出34'(亦即等級1A密文位元)傳遞至區塊解密器74以及密鑰流產生器76。操作區塊解密器以執行區塊加密器34之反轉功能。見圖5，說明一48位元之解密器35的功能區塊圖，該解密器35用以執行圖4中所說明之區塊加密器34的反轉功能。密鑰流產生器76係與密鑰流產生器36相同。

於區塊解密器74中，輸出34'係解密以獲得輸出32-1'(亦即48個等級1A位元)。於密鑰流產生器76中，輸出34'係用以產

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90.3.08 修正
年 月 日 補充
A7
B7

五、發明說明（15）

生一密鑰流輸出36'（亦即100個解密之等級1A密文位元）。然後密鑰流係用以將輸出38'（亦即等級1B密文位元）與輸出40'（亦即等級2密文位元）進行XOR，以便獲得輸出32-2'（亦即等級1B位元）與輸出32-3'（亦即等級2位元）。輸出32-1'，輸出32-2'與輸出32-3'（亦即等級1A位元，等級1B位元與等級2位元）係由語音解碼器72解碼，以獲得原始訊息框。

如果一傳送錯誤發生，則丟棄第一位準位元（亦即等級1A位元與32個最高有效等級1B位元），並以一或更多前一良框其第一位準位元之某函數或者插入法（如著名之IS-641標準中所述）取代。並傳遞至語音解碼器72。無需將等級1A位元區塊解密，或者（使用密鑰流產生器76）產生一密鑰流，因為這些資料將不當地給定一失效之循環檢查碼（CRC）。因此不可能解密第二位準位元（亦即等級2位元與16個最低有效等級1B位元）。避免這些工作將可儲存處理器週期。這些維持加密之第二位準位元所造成的語音品質降低僅為極小或者無感之衝擊。

注意：FACCH與SACCH加密可由本發明以一相似方式提供聲音之隱密性，其中密碼係源自內部而非外部。各FACCH與SACCH訊息之第一字包括一8位元訊息型態，需維持未加密。因此，各FACCH或者SACCH 之第一字將使用如圖8（與圖9）中所示一40位元加密器XOR運算元80（與解密器90），而其餘字將使用圖4之48位元區塊加密器。

雖然本發明以重要細節並參照某些具體實施例而描述，但亦可有其他修訂。例如，可能有其他加密器與解密器。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90.3.08 修正 補充
年 月 日
A7
B7

五、發明說明（16a）

元件符號說明：

10	傳送器	48	雙槽插入器
12	語音編碼器	48'	輸出
14	七位元循環檢查碼	52	第一函數呼叫
16	半數比率迴旋式編碼器	52'	輸出
18	打孔器	54	第二函數呼叫
20	聲音加密器	54-1'	輸出
22	雙槽插入器	54-2'	輸出
30	傳送器	56	XOR運算元
32	語音編碼器	56'	輸出
32-1'	輸出	58	第三函數
32-2'	輸出	58-1'	輸出
32-3'	輸出	58-2'	輸出
34	區塊加密器	60	第四函數呼叫
34'	輸出	60'	輸出
36	密鑰流產生器	72	語音解碼器
36'	輸出	74	區塊解密器
38,40	XOR運算元	76	密鑰流產生器
38'	輸出	78, 80	XOR運算元
40'	輸出	82	七位元循環檢查碼
42	七位元循環檢查碼	84	1/2比率迴旋解碼器
42'	輸出	85	循環檢查碼檢查
44	半數比率迴旋式編碼器	86	雙槽位元解插入器
46	打孔器	90	解密器
46'	輸出	100	48位元區塊加密器
45	表格		

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部中央標準局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

90. 3. 8 修正補充
年 月 日

圖 4

