200840263

# 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： 96148338

※ 申請日期： 96.12.17 ※IPC 分類：H04K 1/00 (2006.01)

H04L 9/12 (2006.01)

H04M 1/68 (2006.01)

## 一、發明名稱：（中文/英文）

合併組合器密碼方法

COMBINATIONAL COMBINER CRYPTOGRAPHIC METHOD

## 二、申 請 人：（共 1 人）

**姓名或名稱：**（中文/英文）

美商高通公司
QUALCOMM INCORPORATED

**代表人：**（中文/英文）

湯瑪仕 R 勞斯
ROUSE, THOMAS R.

**住居所或營業所地址：**（中文/英文）

美國加州聖地牙哥市摩豪斯大道5775號
5775 MOREHOUSE DRIVE SAN DIEGO, CA 92121-1714, U.S.A.

**國 籍：**（中文/英文）

美國 U.S.A.

## 三、發明人：（共 4 人）

姓　名：（中文/英文）

1. 艾立斯安德　甘特曼
   GANTMAN, ALEXANDER
2. 葛格利　高登　羅斯
   ROSE, GREGORY GORDON
3. 邱傑希
   CHOI, JAE-HEE
4. 約翰　W　諾恩伯格二世
   NOERENBERG II, JOHN W.

國　籍：（中文/英文）

1. 美國　U.S.A.
2. 澳大利亞　AUSTRALIA
3. 美國　U.S.A
4. 美國　U.S.A.

## 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：

1. 美國；2006年12月15日；11/611,827

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 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。

## 九、發明說明：

【發明所屬之技術領域】

各種實例大體係關於安全通信，且更特定言之，係關於一種藉由有效地產生轉譯表來保全符號之數據流保密編碼方法。

【先前技術】

數據流保密編碼通常藉由產生偽隨機數密鑰流且使其與明文符號合併以產生加密輸出或密文而進行。通常，在逐位元的基礎上使用互斥或(XOR)運算來合併二進位密鑰流符號與二進位明文符號，因為其為自反的。然而，而非對明文符號執行逐位元加密，有時需要加密整個明文符號。因此，不能使用XOR運算。通常，以n為模數而將明文符號添加至密鑰流符號以獲得密文符號。但已知特定符號之位置的主動攻擊者可能能夠藉由自所傳輸密文符號中減去來改變彼符號。舉例而言，可藉由以十(10)為模數而將每一數位自密鑰流添加至偽隨機產生數位(0至9)來加密明文數位集合(0至9)。然而，已知對於特定明文數位為"1"但輸出密文數位為"7"之攻擊者可判定密鑰流數位為"6"且可接著正確地加密其針對彼特定符號位置之選擇的任何其他數位。因為攻擊者可判定明文符號與密鑰流符號如何合併，所以此部分解密會削弱其餘加密資訊之安全性。亦即，一旦發現密文符號與明文符號之間的關係，就會由於彼資訊可能允許其他密文符號被攻擊者解密而損害剩餘密文符號之安全性。另外，雖然簡單的數學運算(例如，加法、減

法、乘法，等等)快速且有效地合併明文符號與密鑰流符號，但使用更複雜的數學函數可能會引起加密之顯著延遲或需要較大的處理資源。

因此，需要一種在發現或破壞一加密符號時不會削弱其他符號之安全性的有效加密方法。

【發明內容】

提供一種在加密裝置上操作之方法以用於保全資料。藉由加密裝置來獲得複數個輸入符號。自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者的偽隨機選定轉譯表。使用輸入符號之用於輸入符號中之每一者的相應轉譯表而將輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號。可將輸出符號傳輸至解密裝置。

另外，可自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者的第二偽隨機選定轉譯表。可使用輸出符號之用於輸出符號中之每一者的相應第二轉譯表而將輸出符號轉譯為相應第二輸出符號以進一步個別地加密每一輸入符號。

在一實例中，獲得用於待加密之輸入符號中之每一者的偽隨機選定轉譯表可包括(a)獲得用於第一輸入符號之偽隨機選定第一轉譯表，及(b)獲得用於第二輸入符號之偽隨機選定第二轉譯表。使用輸入符號之用於輸入符號中之每一者的相應轉譯表而將輸入符號轉譯為相應輸出符號可包括(a)使用第一轉譯表而將第一輸入符號轉譯為第一輸出符

號，及(b)使用第二轉譯表而將第二輸入符號轉譯為第二輸出符號。複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且轉譯表為N個符號之排列。

在另一實例中，獲得用於待加密之輸入符號中之每一者的偽隨機選定轉譯表可包括(a)獲得用於待加密之第一輸入符號之第一偽隨機數，及(b)混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之轉譯表。

在一組態中，第一偽隨機數可藉由以下各項來獲得：(a)產生用於第一輸入符號之偽隨機數，其中偽隨機數為k個位元長且k為正整數；(b)判定偽隨機數是否在最大數Pmax內，其中Pmax為小於最大臨限值$2^k$之N階乘的最大倍數；(c)在偽隨機數大於最大數Pmax時廢除偽隨機數；(d)獲得用於第一輸入符號之不同偽隨機數，直至獲得小於或等於最大數Pmax之可接受偽隨機數為止；及/或(e)以N階乘為模數來除可接受偽隨機數以獲得第一偽隨機數。混洗N個符號之集合可包括(a)以N個符號之集合的所有符號來初始化排列向量P，及(b)基於第一偽隨機數來混洗排列向量中之符號。

亦提供一種包含輸入介面及處理電路之加密裝置。輸入介面可用以接收輸入符號流。處理電路可經組態以：(a)自輸入介面獲得複數個輸入符號；(b)自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者的偽隨機選定轉譯表；及/或(c)使用輸入符號之用於

輸入符號中之每一者的相應轉譯表而將輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號。加密裝置亦可包括耦接至處理電路以用於傳輸輸出符號之輸出介面。

複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且轉譯表為N個符號之排列。加密裝置亦可包括：(a)耦接至處理電路之密鑰流產生器，密鑰流產生器經組態以自密鑰流產生器獲得用於待加密之第一輸入符號之第一偽隨機數；及/或(b)耦接至處理電路之轉譯表產生器，轉譯表產生器經組態以混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之轉譯表。

在一實例中，處理電路可進一步經組態以：(a)產生用於第一輸入符號之偽隨機數，其中偽隨機數為k個位元長且k為正整數；(b)判定偽隨機數是否在最大數Pmax內，其中Pmax為小於最大臨限值$2^k$之N階乘的最大倍數；(c)在偽隨機數大於最大數Pmax時廢除偽隨機數；(d)獲得用於第一輸入符號之不同偽隨機數，直至獲得小於或等於最大數Pmax之可接受偽隨機數為止；及/或(e)以N階乘為模數來除可接受偽隨機數以獲得第一偽隨機數。

在一組態中，加密裝置之處理電路亦可經組態以：(a)自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者的第二偽隨機選定轉譯表；及/或(b)使用輸出符號之用於輸出符號中之每一者的相應第二轉譯表而將輸出符號轉譯為相應第二輸出符號以進一步個

別地加密每一輸入符號。

因此，提供一種加密裝置，其包含：(a)用於獲得複數個輸入符號之構件；(b)用於自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者之偽隨機選定轉譯表的構件；(c)用於使用輸入符號之用於輸入符號中之每一者的相應轉譯表而將輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號之構件；及/或(d)用於將輸出符號傳輸至解密裝置之構件。加密裝置亦可包括：(a)用於自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者的第二偽隨機選定轉譯表之構件；及/或(b)用於使用輸出符號之用於輸出符號中之每一者的相應第二轉譯表而將輸出符號轉譯為相應第二輸出符號以進一步個別地加密每一輸入符號之構件。

在一組態中，加密裝置可包括：(a)用於獲得用於第一輸入符號之偽隨機選定第一轉譯表的構件；(b)用於獲得用於第二輸入符號之偽隨機選定第二轉譯表的構件；(c)用於使用第一轉譯表而將第一輸入符號轉譯為第一輸出符號之構件；及/或(d)用於使用第二轉譯表而將第二輸入符號轉譯為第二輸出符號之構件。

在一實例中，加密裝置亦可包括：(a)用於獲得用於待加密之第一輸入符號之第一偽隨機數的構件；及/或(b)用於混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之轉譯表的構件。

亦提供一種機器可讀媒體，其具有操作以用於加密符號

之一或多個指令，指令在由處理器執行時使處理器：(a)獲得複數個輸入符號；(b)自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之輸入符號中之每一者的偽隨機選定轉譯表；及/或(c)使用輸入符號之用於輸入符號中之每一者的相應轉譯表而將輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號。複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且轉譯表為N個符號之排列。

機器可讀媒體亦可包括一或多個指令，指令在由處理器執行時使處理器進一步：(a)獲得用於待加密之第一輸入符號之第一偽隨機數；及/或(b)混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之轉譯表。

在一組態中，機器可讀媒體亦可包括一或多個指令，指令在由處理器執行時使處理器進一步：(a)產生用於第一輸入符號之偽隨機數，其中偽隨機數為k個位元長且k為正整數；(b)判定偽隨機數是否在最大數Pmax內，其中Pmax為小於最大臨限值$2^k$之N階乘的最大倍數；(c)在偽隨機數大於最大數Pmax時廢除偽隨機數；(d)獲得用於第一輸入符號之不同偽隨機數，直至獲得小於或等於最大數Pmax之可接受偽隨機數為止；及/或(e)以N階乘為模數來除可接受偽隨機數以獲得第一偽隨機數。

亦提供一種用於解密符號之方法。獲得在n個符號之集合內所界定的複數個輸入符號。自界定不同符號至符號排

列之複數個反向轉譯表選擇一用於待解密之輸入符號中之每一者的偽隨機選定反向轉譯表。接著使用輸入符號之用於輸入符號中之每一者的相應反向轉譯表而將輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號。複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且反向轉譯表為N個符號之排列。該方法可進一步包括：(a)獲得用於待解密之第一輸入符號之第一偽隨機數；及/或(b)混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之反向轉譯表。

在一實例中，第一偽隨機數可藉由以下各項來獲得：(a)產生用於第一輸入符號之偽隨機數，其中偽隨機數為k個位元長且k為正整數；(b)判定偽隨機數是否在最大數Pmax內，其中Pmax為小於最大臨限值$2^k$之N階乘的最大倍數；(c)在偽隨機數大於最大數Pmax時廢除偽隨機數；(d)獲得用於第一輸入符號之不同偽隨機數，直至獲得小於或等於最大數Pmax之可接受偽隨機數為止；及/或(e)以N階乘為模數來除可接受偽隨機數以獲得第一偽隨機數。

在另一組態中，該方法可進一步包括：(a)自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之輸入符號中之每一者的第二偽隨機選定反向轉譯表；及/或(b)使用輸出符號之用於輸出符號中之每一者的相應第二反向轉譯表而將輸出符號轉譯為相應第二輸出符號以進一步個別地解密每一輸入符號。

提供一種包含輸入介面及處理電路之解密裝置。輸入介

面可接收輸入符號流。處理電路可經組態以：(a)獲得在n個符號之集合內所界定的複數個輸入符號；(b)自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之輸入符號中之每一者的偽隨機選定反向轉譯表；及/或(c)使用輸入符號之用於輸入符號中之每一者的相應反向轉譯表而將輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號。

複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且反向轉譯表為N個符號之排列。解密裝置亦可包括：(a)耦接至處理電路之密鑰流產生器，密鑰流產生器經組態以自密鑰流產生器獲得用於待解密之第一輸入符號之第一偽隨機數；及/或(b)耦接至處理電路之反向轉譯表產生器，反向轉譯表產生器經組態以混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之反向轉譯表。

複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且反向轉譯表為N個符號之排列。處理電路可進一步經組態以：(a)產生用於第一輸入符號之偽隨機數，其中偽隨機數為k個位元長且k為正整數；(b)判定偽隨機數是否在最大數Pmax內，其中Pmax為小於最大臨限值$2^k$之N階乘的最大倍數；(c)在偽隨機數大於最大數Pmax時廢除偽隨機數；(d)獲得用於第一輸入符號之不同偽隨機數，直至獲得小於或等於最大數Pmax之可接受偽隨機數為止；及/或(e)以N階乘為模數來除可接受偽隨機數以獲得第一偽隨

機數。

在另一實例中，處理電路可進一步經組態以：(a)自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之輸入符號中之每一者的第二偽隨機選定反向轉譯表；及/或(b)使用輸出符號之用於輸出符號中之每一者的相應第二反向轉譯表而將輸出符號轉譯為相應第二輸出符號以進一步個別地解密每一輸入符號。

因此，亦提供一種解密裝置，其包含：(a)用於獲得在n個符號之集合內所界定之複數個輸入符號的構件；(b)用於自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之輸入符號中之每一者之偽隨機選定反向轉譯表的構件；及/或(c)用於使用輸入符號之用於輸入符號中之每一者的相應反向轉譯表而將輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號之構件。複數個輸入符號可藉由N個符號之集合來界定，其中N為正整數且反向轉譯表為N個符號之排列。解密裝置可進一步包括：(a)用於獲得用於待解密之第一輸入符號之第一偽隨機數的構件；及/或(b)用於混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之反向轉譯表的構件。第一偽隨機數藉由以下各項來獲得：(a)用於產生用於第一輸入符號之偽隨機數的構件，其中偽隨機數為k個位元長且k為正整數；(b)用於判定偽隨機數是否在最大數Pmax內之構件，其中Pmax為小於最大臨限值$2^k$之N階乘的最大倍數；(c)用於在偽隨機數大於最大數Pmax時廢除

偽隨機數之構件；(d)用於獲得用於第一輸入符號之不同偽隨機數直至獲得小於或等於最大數Pmax之可接受偽隨機數為止的構件；及/或(e)用於以N階乘為模數來除可接受偽隨機數以獲得第一偽隨機數之構件。

亦提供一種機器可讀媒體，其具有用於解密符號之一或多個指令，指令在由處理器執行時使處理器：(a)獲得在n個符號之集合內所界定的複數個輸入符號；(b)自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之輸入符號中之每一者的偽隨機選定反向轉譯表；及/或(c)使用輸入符號之用於輸入符號中之每一者的相應反向轉譯表而將輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號。複數個輸入符號藉由N個符號之集合來界定，其中N為正整數且反向轉譯表為N個符號之排列。

機器可讀媒體亦可包含一或多個指令，指令在由處理器執行時使處理器進一步：(a)獲得用於待解密之第一輸入符號之第一偽隨機數；及/或(b)混洗N個符號之集合以獲得N個符號之集合的不同排列且使用彼排列作為用於第一輸入符號之反向轉譯表。

在另一實例中，機器可讀媒體亦可包含一或多個指令，指令在由處理器執行時使處理器進一步：(a)自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之輸入符號中之每一者的第二偽隨機選定反向轉譯表；及/或(b)使用輸出符號之用於輸出符號中之每一者的相應第二反向轉譯表而將輸出符號轉譯為相應第二輸出符號以進一步

個別地解密每一輸入符號。

【實施方式】

在以下描述中，給出特定細節以提供對實例之徹底理解。然而，一般熟習此項技術者將理解，可在無此等特定細節的情況下實踐實例。舉例而言，可能不以方塊圖來展示電路，以便不以不必要的細節來使實例模糊。

又，應注意，實例可被描述為過程，過程被描繪為流程框圖(flowchart)、流程圖(flow diagram)、結構圖或方塊圖。儘管流程框圖可將操作描述為順序過程，但可並行或同時執行許多操作。另外，可重新配置操作之次序。過程在其操作完成時終止。過程可對應於方法、功能、程序、子常式、子程式，等等。當過程對應於功能時，其終止對應於功能至呼叫功能或主功能之返回。

此外，儲存媒體可表示用於儲存資料之一或多個裝置，包括唯讀記憶體(ROM)、隨機存取記憶體(RAM)、磁碟儲存媒體、光學儲存媒體、快閃記憶體裝置，及/或用於儲存資訊之其他機器可讀媒體。術語"機器可讀媒體"包括(但不限於)攜帶型或固定儲存裝置、光學儲存裝置、無線通道，及能夠儲存、含有或載運指令及/或資料之各種其他媒體。

此外，各種組態可藉由硬體、軟體、韌體、中間體(middleware)、微碼或其組合來實施。當以軟體、韌體、中間體或微碼來實施時，用以執行所描述任務之程式碼或碼段可儲存於諸如儲存媒體或其他儲存構件之機器可讀媒

體中。處理器可執行所界定任務。碼段可表示程序、功能、子程式、程式、常式、子常式、模組、套裝軟體、類別，或指令、資料結構或程式敘述之組合。碼段可藉由傳遞及/或接收資訊、資料、引數、參數或記憶體內容而耦接至另一碼段或硬體電路。資訊、引數、參數、資料及其類似者可經由其中包括記憶體共用、訊息傳遞、符記傳遞及網路傳輸之適當方式來傳遞、轉發或傳輸。本文中所揭示之方法可以硬體、軟體或兩者來實施。

結合本文中所揭示之實例而描述之各種說明性邏輯區塊、模組、電路、元件及/或組件可以通用處理器、數位信號處理器(DSP)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)或其他可程式化邏輯組件、離散閘或電晶體邏輯、離散硬體組件或其經設計以執行本文中所描述之功能之任何組合來實施或執行。通用處理器可為微處理器，但在替代例中，處理器可為任何習知處理器、控制器、微控制器或狀態機。處理器亦可被實施為計算組件之組合，例如，DSP與微處理器之組合、許多微處理器、結合DSP核心之一或多個微處理器，或任何其他此組態。

結合本文中所揭示之實例而描述之方法或演算法可以處理單元、程式設計指令或其他方向之形式而直接以硬體、以由處理器可執行之軟體模組或以兩者之組合來體現，且可包含於單一裝置中或分布於多個裝置上。軟體模組可駐存於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、抽取式碟片、

CD-ROM，或此項技術中已知之任何其他形式的儲存媒體。儲存媒體可耦接至處理器，使得處理器可自儲存媒體讀取資訊及將資訊寫入至儲存媒體。在替代例中，儲存媒體可與處理器成一體式。

一特徵提供一種可與客戶之電話線串聯地被插入之小形狀因數安全裝置，其用作兩因數鑑認機制中之第二因數且加密DTMF載頻調，藉此防止敏感性資訊之揭示。裝置不會干擾電話之正常操作。裝置可包括小形狀因數外殼，該外殼亦可為銀行及與其相關聯之支付服務提供標記機會。裝置可自其所耦接之電話線被供電。在一組態中，複數個此等裝置可沿一電話線而被鏈接或級聯以提供與多個不同方(例如，銀行)之安全通信。

另一特徵提供一種防護加密符號之安全性的有效加密方法。藉由使用獨立偽隨機選定轉譯表來加密每一明文符號。而非將符號之每一可能排列預儲存為轉譯表，可基於偽隨機數及符號混洗演算法而在運作中(on-the-fly)有效地產生轉譯表。接收裝置可類似地在運作中產生反向轉譯表以解密所接收加密符號。

**保全DTMF載頻調**

圖1說明安全裝置102可沿通信線而耦接至電話104以保全電話104與安全伺服器108之間的特定通信之系統。安全裝置102可為小形狀因數裝置，其可成列或串聯地連接於電話104與通信網路106之間的電話線上。安全裝置102可靠近或鄰近於電話104而耦接至電話線。

在一實例中，安全裝置102可與帳戶及/或發行機構108(例如，銀行、信用卡公司，等等)相關聯。舉例而言，銀行可將此安全裝置102發行至其客戶，每一安全裝置與一客戶或客戶之帳戶唯一地相關聯。發行機構108可具有有助於與客戶之電話交易的安全伺服器110。

圖2為說明用於保全電話104與屬於圖1之發行機構108之安全伺服器110之間的特定通信之方法的流程圖。安全裝置102可具有主動操作模式及不主動(被動)操作模式。當安全裝置102用於呼叫除了發行機構108以外之某者(例如，安全伺服器110)時，其為不主動的且呼叫僅無改變地穿過安全裝置102(包括DTMF載頻調)。然而，當電話104起始至發行機構之呼叫208時，安全伺服器110(例如，安全伺服器110)發送喚醒安全裝置之啟動信號210。啟動信號可為充分地長及/或唯一的(例如，具有足夠數位或符號)以合理地確保安全裝置102不可能碰巧被觸發。在一實例中，此啟動信號實際上可能不載運任何資訊，但僅觸發或啟動安全裝置102以自不主動(被動)模式切換至主動模式。舉例而言，啟動信號可為由安全裝置102所辨識之短音樂或載頻調片段。安全裝置102收聽及辨識來自安全伺服器110之啟動信號(例如，唯一DTMF載頻調集合)且改變至主動模式212。在一實例中，在接收到啟動信號後，安全裝置102就可開始加密自電話至安全伺服器110之所有DTMF載頻調。

在一組態中，可在安全裝置102與安全伺服器110之間實

施查問回應機制。除了啟動信號以外，安全伺服器110可將隨機查問發送至安全裝置214。安全裝置102接收查問、產生答覆(例如，識別符及對查問之回應)216且將答覆發送至安全伺服器110。答覆可包括與安全裝置102相關聯之識別符及對查問之回應。安全裝置102亦可產生會話密鑰，其可用於加密自電話104至安全伺服器110之後續DTMF載頻調。

答覆向安全伺服器110通知其與關聯安全裝置通信。安全伺服器110可使用識別符來查找特定客戶之帳戶220，藉此使客戶免去相互識別自身之麻煩(例如，避免使客戶輸入其帳號)。安全伺服器110亦可基於安全裝置102與安全伺服器110兩者中所供應之隨機查問及鑑認密鑰來驗證回應為正確的222，以鑑認使用者。注意，由於安全裝置102位於使用者之電話附近(例如，在使用者家裏)，所以攻擊者將必須將其竊取以起始攻擊。

藉由使用相同查問及回應，安全伺服器110與安全裝置102所計算224相同地計算會話密鑰226。若安全伺服器110不同意其自安全裝置102所接收之答覆(或根本未接收到回應)，則呼叫可轉向替代路徑以用於更嚴格的識別及/或鑑認。亦即，安全裝置102可基於所接收隨機查問及鑑認密鑰來計算其回應。安全伺服器110可接著藉由計算區域回應(基於隨機查問及鑑認密鑰)來驗證所接收回應且比較其與來自安全裝置102之所接收回應。

若查問回應被適當地鑑認，則安全伺服器110發送使用

新近導出會話密鑰而鑑認之確認228。此確認通知安全裝置102開始加密來自電話104之DTMF載頻調。若來自安全伺服器之確認存在問題(例如，其在特定最大時間內未被安全裝置102接收或確認失敗，等等)，則安全裝置102可對使用者產生警告信號。舉例而言，若查問回應鑑認失敗，則燈可閃爍(或變為ON)或警報可發聲。另外，燈(例如，發光二極體--LED)可發光以指示安全裝置102為主動的及/或查問回應被成功地鑑認。

一旦查問回應被成功地鑑認，在一實例中，會話密鑰就可由安全裝置102用於加密自電話104至安全伺服器之傳輸。一旦加密開始，安全裝置就截取來自電話之DTMF載頻調232且替代地傳輸加密DTMF載頻調234。在DTMF載頻調之此加密的一實例中，來自電話104之DTMF載頻調可被轉譯為接著被發送至安全伺服器110之不同DTMF載頻調。在另一組態中，DTMF載頻調可由安全裝置102轉換為接著被加密且發送至安全伺服器110之數位符號。安全裝置102亦在兩個方向上傳遞其他者(非DTMF載頻調或信號)而不將其修改或加密。由於使用者可被要求之首要事情中之一者為輸入與其帳戶相關聯之PIN號，所以與此PIN號相關聯之DTMF載頻調經加密且可形成用於鑑認之第二因數。類似地，安全伺服器110可使用會話密鑰來解密經由安全裝置而自電話所接收之DTMF載頻調236。

在替代組態中，安全裝置102可經組態以辨識與特定發行機構108相關聯之特定電話號碼。當安全裝置102辨識到

電話已撥號特定電話號碼時，其可自動地切換至主動模式及/或加密自電話至安全伺服器110之所有DTMF載頻調。

安全裝置102可繼續加密來自電話104之DTMF載頻調，直至呼叫終止為止，此時，安全裝置102切換回至允許所有DTMF載頻調無改變地穿過之不主動模式。

由於安全裝置102可具有小形狀因數且可容易地插入於電話線中。使用者可具有與單一機構或帳戶相關聯之多個安全裝置，以使得使用者能夠安全地自不同位置(例如，家、辦公室，等等)存取帳戶。使用者亦可具有與各種不同機構及/或帳戶相關聯之多個安全裝置。此等多個安全裝置可沿一電話線而被串聯地耦接。鏈中之不主動安全裝置僅將信號傳遞至鏈中之下一安全裝置。若鏈中之安全裝置由安全伺服器啟動，則其加密來自電話之DTMF載頻調。

在另一實例中，安全裝置102可伺服來自一電話或位置之多個使用者。在此狀況下，安全伺服器可識別到安全裝置與複數個使用者或帳戶相關聯。為了區別每一使用者，安全伺服器可發送請求使用者輸入PIN或識別特定使用者或帳戶之其他識別符的語音提示。

圖3說明可使得能夠在傳輸期間保全DTMF載頻調之電話服務安全伺服器之一實例的方塊圖。安全伺服器302可包括諸如小及/或低功率微處理器之處理電路304。安全伺服器302可包括用於將安全伺服器302耦接至通信網路之第一通信模組306。鑑認模組308允許安全伺服器302鑑認與其

通信之安全裝置。DTMF解密模組310允許安全伺服器302解密自安全裝置所接收之加密DTMF載頻調。

圖4說明在安全伺服器上操作以用於保全來自電話裝置之DTMF載頻調的方法。自DTMF啟用電話接收呼叫402。將啟動信號發送至與DTMF啟用電話相關聯之安全裝置404。安全裝置可位於DTMF啟用電話附近。接著藉由安全伺服器來鑑認安全裝置。舉例而言，將查問信號發送至安全裝置406。安全伺服器判定是否自安全裝置接收到回應408。若否，則可假定無安全裝置存在於電話線上410。否則，安全伺服器判定是否可成功地鑑認所接收回應412。若不能成功地鑑認所接收回應，則鑑認失敗414。否則，產生會話密鑰416。將由會話密鑰所鑑認之確認訊息發送至安全裝置418。安全伺服器可自安全裝置接收加密DTMF載頻調420。安全伺服器可接著解密所接收DTMF載頻調以獲得由電話所發送之資訊422。此等DTMF載頻調可表示機密資訊(例如，帳號、密碼、PIN，等等)，其在傳輸期間藉由加密原始DTMF載頻調而被保護以免由偷聽者偷聽。

圖5說明可經組態以在傳輸期間保護DTMF載頻調之安全裝置之一實例的方塊圖。安全裝置502可包括諸如小及/或低功率微處理器之處理電路504。安全裝置502可由其所耦接之電話線供電。第一通信介面A 506可用於將安全裝置502耦接至電話。第二通信介面B 508可用於將安全裝置502耦接至通信網路。在被動操作模式中，安全裝置502使所有DTMF載頻調無改變地穿過。處理電路504可經組態以

收聽啟動信號(例如，來自安全伺服器)。DTMF偵測器510可經組態以偵測DTMF啟動信號以將安全裝置切換至主動操作模式。在主動模式中，安全裝置502可經組態以回應於來自安全伺服器之鑑認查問。

在啟動模式中，DTMF偵測器510亦可經組態以偵測經由通信介面A 506而接收之DTMF載頻調(例如，來自電話)。若偵測到一或多個DTMF載頻調，則DTMF載頻調由DTMF加密模組512加密或另外修改。加密DTMF載頻調接著經由通信介面B 508而傳輸至安全伺服器。

圖6說明在安全裝置上操作以用於保全來自電話裝置之DTMF載頻調的方法。在電話與安全伺服器之間起始呼叫後就對安全裝置供電602。亦即，由於在進行呼叫時激發通信線，所以安全裝置可自通信線取得其電力。在被動操作模式中，安全裝置允許DTMF載頻調無改變地穿過第一通信介面與第二通信介面之間604。舉例而言，第一通信介面可耦接至電話而第二通信介面可耦接至一安全伺服器622。安全裝置監視傳輸以判定是否自安全伺服器接收到(DTMF)啟動信號606。除非接收到啟動信號，否則安全裝置繼續在被動模式中操作。若接收到DTMF啟動信號，則安全裝置改變至主動操作模式608。安全裝置亦可收聽來自安全伺服器之其他信號610。

安全裝置可自安全伺服器接收查問612。安全裝置以對查問之回應來答覆614。若回應為有效的，則安全裝置可接收指示安全伺服器已成功地鑑認安全裝置之確認616。

一旦經啟動且經適當地鑑認，安全裝置就收聽來自電話之DTMF載頻調。若經由第一通信介面而自電話(其與安全裝置耦接)接收到DTMF載頻調618，則將所接收DTMF載頻調加密為不同DTMF載頻調620。在一實例中，來自電話之DTMF載頻調可被轉譯為接著被發送至安全伺服器之不同DTMF載頻調。在另一組態中，DTMF載頻調可由安全裝置102轉換為接著被加密且發送至安全伺服器之數位符號。接著經由第二通信介面而將加密DTMF載頻調發送至安全伺服器622。安全裝置繼續加密來自電話之DTMF載頻調，直至呼叫結束為止，此時，安全裝置返回至被動模式624。安全裝置102防止來自電話之未加密DTMF載頻調傳遞至安全伺服器。在一實例中，安全裝置102可斷開來自電話之所有輸入(例如，傳輸)，同時網路為主動的。在此狀況下，例如，若客戶需要與代表人談話，則可存在用於使客戶或安全伺服器重新連接輸入(例如，允許來自安全裝置102之傳輸)的某供應。

**蜂巢式電話安全性機制**

圖7為經組態以利用安全伺服器來鑑認自身之行動通信裝置的方塊圖。行動通信裝置702包括耦接至通信模組706及使用者輸入介面708之處理電路704。通信模組706使得行動通信裝置702能夠經由無線通信網路而通信710。處理電路704可經組態以在呼叫期間利用一或多個安全伺服器來鑑認自身。舉例而言，行動通信裝置可經組態成具有鑑認密鑰及/或使用者識別符，其允許銀行或金融機構鑑認

行動通信裝置702之使用者。鑑認密鑰及/或使用者識別符可由銀行或金融機構預先(例如，在設置或組態期間)提供。另外，處理電路704亦可自使用者請求PIN、密碼及/或其他輸入以完成鑑認程序。

圖8為說明用於鑑認經由通信網路至電話服務臺804之行動通信裝置802之方法的流程圖。行動通信裝置802可為行動電話，且電話服務臺804可包括與銀行業或金融機構相關聯之安全伺服器。行動通信裝置802及電話服務臺804可各自具有相同鑑認密鑰。

行動通信裝置可起始至與電話服務臺相關聯之發行機構之呼叫806。舉例而言，發行機構可為銀行或金融機構。電話服務臺將隨機鑑認查問發送至行動通信裝置808。行動通信裝置接著基於隨機查問及鑑認密鑰來產生回應809且將回應及(可能)使用者識別符發送至電話服務臺810。電話服務臺接著驗證來自行動通信裝置之回應是否為正確的812。此可藉由電話服務臺基於其鑑認密鑰及隨機鑑認查問來計算驗證值且比較其與自行動通信裝置所接收之回應來進行。若成功地鑑認回應，則可將鑑認確認814發送至行動通信裝置。行動通信裝置可自電話服務臺請求敏感性資訊(例如，銀行帳戶記錄，等等)816。若成功地鑑認行動通信裝置，則電話服務臺接著將所請求敏感性資訊提供至行動通信裝置818。以此方式，行動通信裝置(例如，行動電話)可由電話服務臺鑑認以在呼叫期間保全敏感性資訊之傳輸。

**威脅模型**

由本文中所描述之安全裝置及/或方法所處理之一威脅類型為偷聽攻擊。在此攻擊中，攻擊者可將記錄器附接至電話線以收聽與由使用者輸入於電話上之數字相關聯的DTMF載頻調。此等DTMF載頻調可識別被呼叫之銀行、使用者之客戶及/或帳號、專用識別號(PIN)、社會安全號、連同其他專用及/或機密資訊一起。攻擊者可接著使用此資訊以自使用者之帳戶執行欺騙性交易。本文中所描述之安全裝置藉由加密DTMF載頻調且提供進一步鑑認來擊敗此攻擊。由於大多數機構(例如，銀行，等等)可使用用於鑑認之兩個因數(例如，安全裝置之佔有及PIN之知識)，所以很少將必須要求其他敏感性資訊。簡單地截取加密DTMF載頻調不會揭露關於相應帳號、PIN等等之任何東西。

攻擊者為了成功而將必須藉由(例如)防止呼叫轉至預期接收者(例如，預期銀行)、假裝為預期接收者、要求呼叫者輸入所有敏感性資訊來干擾呼叫之進程。為了擊敗此攻擊，安全裝置可在自接收機構接收到"開始加密"信號(亦即，鑑認確認)之後接通安全指示器(例如，燈)。呼叫者(例如，客戶)僅檢查安全指示器以確保安全裝置在輸入任何敏感性或機密資訊之前加密其載頻調。

另一攻擊類型可為會話劫持攻擊，其中攻擊者等待直至使用者已建立與預期接收者(例如，銀行)之通信為止，因此啟動安全指示器，且接著接管呼叫。攻擊者可接著假裝

呼叫出錯且要求使用者口頭地提供敏感性資訊。或者，攻擊者可要求使用者輸入特定回應(其已經為攻擊者已知)以設法建立逐載頻調加密樣式，且接著使用逐載頻調轉換來加密其自己對銀行之回應。為了處理此攻擊類型，可在偽隨機基礎、旋轉基礎及/或抑制數字與載頻調關係之發現的其他基礎上改變或修改逐載頻調加密。

**訊息及會話鑑認**

安全裝置可經組態以藉由使用(例如)訊息鑑認碼(MAC)功能來執行訊息鑑認及會話密鑰導出。舉例而言，安全伺服器可藉由自$MAC_K$(查問)之單一調用分裂輸出來鑑認呼叫者之安全裝置。舉例而言，典型MAC功能可傳回128個位元之輸出，其可被表示為32個DTMF載頻調。在安全伺服器及安全裝置已計算MAC之後，安全伺服器可將最初16個DTMF載頻調(表示MAC之一部分)發送至安全裝置，且在回應中，安全裝置發送回另外16個DTMF載頻調(表示MAC之另一部分)。以此方式，安全伺服器與安全裝置兩者可向彼此證明其為經授權或合法的。

類似地，會話密鑰可由每一方計算，使得會話密鑰=$MAC_K$(鑑認密鑰 ‖ 查問)，其中鑑認密鑰被預載入於安全裝置中。為了防止在安全裝置將其回應發送至安全伺服器時揭示會話密鑰，回應可包括額外資訊。舉例而言，回應可為回應=$MAC_K$("額外資訊串" ‖ 鑑認密鑰 ‖ 查問)。

**數據流保密編碼**

另一特徵提供一種防護加密符號之安全性的有效密碼方

法。藉由使用獨立偽隨機選定轉譯表來加密每一明文符號。而非將符號之每一可能排列預儲存為轉譯表，可基於偽隨機數及符號混洗演算法而在運作中有效地產生轉譯表。接收裝置可類似地在運作中產生反向轉譯表以解密所接收加密符號。

此密碼方法可在各種組態中被實施。舉例而言，電話安全裝置可藉由使用每一數位值之偽隨機選定轉譯表而將DTMF載頻調轉換為數位值、加密數位值。可接著以數位形式或作為與加密數位值相關聯之DTMF載頻調而將加密數位值傳輸至安全伺服器(例如，電話服務臺)。

因為DTMF載頻調由數位符號表示(或與數位符號相關聯)，所以其可藉由(例如)數據流保密編碼來保全。在各種實例中，數據流保密編碼可使用由塊密碼所產生之密鑰流，諸如以計數器模式之高級加密標準(AES)、輸出反饋(OFB)，或密文反饋(CFB)模式。舉例而言，MAC功能可以CBC-MAC模式之塊密碼來實施。此在(例如)安全裝置具有以硬體所實施之AES時可能為有利的。

若此等功能以軟體來實施，則可能較佳的是使用諸如非線性SOBER(NLS)之專用流密碼。雖然以低效率，但流密碼亦可藉由將待加密之資料用作密鑰或臨時標誌輸入、接著產生輸出密鑰流而用作MAC功能。由於所產生之密鑰流的長度可如所要的一樣長，所以回應與會話密鑰兩者皆可在單一呼叫中被產生。

習知數據流保密編碼(無論使用以串流模式之真實流密

碼還是塊密碼)通常藉由產生偽隨機數密鑰流且使其與明文(亦即，DTMF載頻調之數位表示)合併以形成加密輸出或密文而進行。通常，使用互斥或(XOR)運算來合併密鑰流與明文，因為其為自反的。然而，習知DTMF啟用電話具有十個或十個以上鍵，每一鍵具有唯一載頻調。因此，XOR運算不能用於以密鑰流來加密該等DTMF載頻調。實情為，與電話鍵相關聯之DTMF載頻調可被轉換為不同數位符號(或與不同數位符號相關聯)，該等數位符號可被添加至自密鑰流所獲得之偽隨機數/符號以產生加密符號或密文。但已知特定數位之位置的主動攻擊者可能能夠藉由自所傳輸密文數中減去來改變彼數。舉例而言，已知對於特定DTMF載頻調而言輸入為"1"但輸出為"7"之攻擊者可判定經產生用於此載頻調之偽隨機數為"6"且可接著正確地加密其針對彼特定數位位置之選擇的任何字元。

**合併組合器**

一特徵提供用於使用密鑰流來獲得或產生用於待加密之每一明文符號的偽隨機選定或產生轉譯表。而非自密鑰流取得偽隨機數及以相同方式(例如，藉由以n為模數來添加)來改變明文，一特徵提供用於藉由偽隨機地選擇複數個轉譯表中之一者來轉譯輸入流中之每一明文符號。轉譯表可提供數字或符號集合之不同可能排列。此在本文中被稱為合併組合器。

圖9說明用於藉由偽隨機地選擇用於待加密之每一符號之轉譯表來保全明文符號之合併組合器的方塊圖。密碼產

生器902用於產生偽隨機數/符號密鑰流Si 904。密鑰流904之偽隨機數用於自複數個可能轉譯表產生或獲得用於輸入流中之每一明文輸入符號Pi 908的不同轉譯表906。藉由將明文輸入符號908轉譯為偽隨機輸出，產生加密輸出符號Ci 910。

此轉譯操作在密鑰流904之控制下界定明文輸入符號908之排列。轉譯表906可被表示為n個元素之向量，且明文輸入符號908之轉譯可藉由查找轉譯表906之第p個元素來進行。給出加密輸出符號Ci，反向轉譯可藉由建立反向排列之表或藉由搜尋含有符號Ci之輸入的表且使其指數作為p而傳回來進行。

一般而言，對於n個明文符號之集合，存在n!(階乘)個可能排列。排列可自所有此等排列之集合被隨機地選擇，且用作轉譯表906以將明文輸入符號Pi 908轉譯為加密輸出符號Ci 910(亦被稱為密文)。對於輸入流中之每一明文符號，選擇偽隨機選定轉譯表。接著，看見加密符號Ci 910且已知其對應於特定明文符號之攻擊者仍不知道關於其他明文符號與相應加密符號之間的對應性之任何東西。亦即，攻擊者可確定之所有資訊為：改變加密符號將會得到不同於其所已知之明文符號的明文符號，但該明文符號並非其將成為之其他明文符號。因此，偽隨機選定轉譯表不會揭露明文輸入符號與加密輸出符號(密文)之間的關係，且攻擊者不能利用任何單一明文符號至密文符號轉譯之知識。

在用於安全電話銀行業之一實例中，將由安全裝置自電話所接收之每一DTMF載頻調轉換為數位明文符號(或與數位明文符號相關聯)。接著藉由轉譯表(基於來自密鑰流之一或多個偽隨機數所獲得)來轉譯明文符號以獲得加密符號。接著將加密符號傳輸至安全伺服器(以數位形式或作為對應於加密符號之DTMF載頻調)，其中加密符號由反向轉譯表解密。可藉由在產生相同密鑰流之安全裝置與安全伺服器兩者處具有同步密碼產生器來產生或獲得反向轉譯表。在一實例中，可藉由使用相同種值(seed)(例如，會話密鑰，等等)來使密碼產生器同步。

在一實例中，可藉由安全裝置及/或安全伺服器來預產生及/或儲存複數個轉譯表。而非在運作中產生新轉譯表(亦即，輸入符號之排列)，可預產生及儲存轉譯表。密鑰流904之偽隨機值/符號可用於選擇用於待加密之每一明文符號之預產生轉譯表中的一者。預產生轉譯表可界定n個明文符號之集合的每一排列或排列子集。

在另一實例中，可藉由使用密鑰流且偽隨機地混洗符號以形成轉譯表而在運作中產生所使用之轉譯表。注意，在將存在n!個表且為選擇此等表中之一者所需之密鑰流的量與為藉由混洗來建立此表所需之量相同的意義上，此等解決方案為等效的。

圖10說明用於將明文符號轉譯為加密符號之符號至符號轉譯表1002的實例。在此實例中，十六(16)個明文符號轉譯為不同加密符號。在此實例中展示二進位表示以僅說明

可使用四位元加密符號來加密十六個明文符號。在其他實例中，若將加密更多或更少數目之明文符號，則不同數目之位元可用於每一符號。舉例而言，對於高達兩百五十六(256)個明文符號，可自密鑰流提取八(8)個位元以產生每一加密符號。

另一特徵提供用於在特定轉譯表內明文符號與加密符號之間的一對一對應性。亦即，在特定轉譯表內，兩個明文符號不會轉換為相同加密符號。此允許解密裝置將加密符號準確地解密為其原始明文符號。

在解密裝置處，可產生符號至符號反向轉譯表以反向加密裝置之符號至符號轉譯且藉此解密所接收加密符號。

圖11說明可如何使用不同轉譯表1104來加密明文符號1102以獲得加密符號1106之一實例。對於每一明文符號P0、P1、P2、P3、……P*i*，各自具有不同符號排列之不同轉譯表1104用於獲得加密符號C0、C1、C2、C3、……C*i*。

對於集合中之少量符號，有可能列出(亦即，預產生)此等符號之所有排列且使用指數(來自密鑰流)以自排列選擇轉譯表。舉例而言，對於十二(12)個可能符號之集合，所產生之可能排列的數目為12!或479,001,600。為了適當地選擇排列，三十二(32)個位元密鑰流可足以將一排列選擇為轉譯表而無偏差。然而，當集合中之符號的數目增加時，此方法變得無效。舉例而言，對於256個可能符號之集合，所產生之可能排列的數目為256!或$8.5x10^{506}$，其將

自偽隨機密鑰流取得超過1684個位元以將排列中之一者選擇為轉譯表。

圖12說明用於自n個符號之集合的複數個可能排列選擇轉譯表之演算法，其中n為正整數。在此實例中，可使用密碼產生器，其提供均一地分布於0及$2^k$-1之範圍內的偽隨機密鑰流值k個位元長(例如，8個位元、32個位元，等等)。密鑰流用於獲得偽隨機數w 1202。由於n!可能不均勻地分成$2^k$，所以在不引入偏差的情況下不能直接使用偽隨機數w。為此，將最大臨限值Pmax界定為n!之最大倍數，其小於$2^k$。若偽隨機數w小於此最大臨限值Pmax，則可在不引入偏差的情況下將其使用。否則，若偽隨機數w大於或等於此最大臨限值Pmax，則將其廢除且選擇新偽隨機數w，直至獲得小於最大臨限值Pmax之偽隨機數w為止1204。

以n!為模數來除偽隨機數w，使得w=w modulo (n!) 1206。因此，在0至n!之範圍內獲得無偏差偽隨機數w，其可用於獲得排列(亦即，轉譯表)。

而非儲存預產生排列且藉由使用偽隨機數w來選擇一個此排列，一特徵提供用於藉由混洗基本排列之符號以產生轉譯表來產生排列。以符號集合之所有值來初始化基本排列向量P，使得P=[0, 1, 2, … n-1] 1208。符號混洗演算法1210接著用於使用偽隨機數w來混洗基本排列向量P中之符號。

符號混洗演算法1210之一實例初始化計數器i至n-1，其

中n為集合中之符號的數目。當計數器i >= 0時，偽隨機數w=w/(i+1)，變數j=w modulo (i+1)，且排列向量P之值經混洗，使得$P_t[i]=P_{t-1}[j]$且$P_t[j]=P_{t-1}[i]$。注意，在不偏離本揭示特徵的情況下，可使用其他符號混洗演算法。

一旦已混洗排列向量P，則可將排列向量P提供1212至可使用其之任何應用，例如，作為轉譯表以加密輸入符號流。

圖13為說明可藉由使用多個轉譯表以加密單一明文符號來達成符號鑑認之另一加密機制的方塊圖。亦即，明文輸入符號P*i* 1302由轉譯表A1 1304加密以獲得第一加密輸出符號C*i*' 1310，轉譯表A1 1304可基於自第一密碼產生器1308所獲得之第一密鑰流S*i*' 1306而被產生或選擇。第一加密輸出符號C*i*' 1310接著用作至第二轉譯表A2 1312之輸入以用於獲得第二加密輸出符號C*i* 1318，轉譯表A2 1312可基於自第二密碼產生器1316所獲得之第二密鑰流S*i* 1314而被產生或選擇。以此方式，冗餘可用於鑑認第一加密輸出符號C*i*' 1310。亦即，藉由共同使用符號C*i*' 1310與C*i* 1318，符號C*i* 1318鑑認C*i*' 1310。因此，例如，若攻擊者成功地改變符號C*i*' 1310，則其將未由符號C*i* 1318適當地鑑認。

圖14說明多個轉譯表1404及1406可如何用於加密每一明文符號1402以獲得相應加密符號對1408。應注意，轉譯表1404及1406可經偽隨機地選擇及/或產生以將每一明文符號P*i*加密為一符號對C*i*'/C*i*。

圖15說明兩個轉譯表可如何用於將明文符號P*n*轉譯或加密為一符號對C*n*'及C*n*之實例。舉例而言，對於第一明文符號P*n*="5"，第一轉譯表A1 1502提供第一輸出符號C*n*'=8(亦即，"5"轉譯為"8")。第一輸出符號"8"可接著用作至第二轉譯表A2 1504之輸入以獲得第二輸出符號C*n*=7(亦即，"8"轉譯為"7")。因為第二輸出符號C*n*基於第一輸出符號C*n*'而產生，所以冗餘符號C*n*及C*n*'可用於鑑認。若任一或兩個符號在傳輸期間皆被攻擊者改變，則鑑認失敗。舉例而言，若C*n*'被攻擊者自"8"修改為"4"，則接收符號C*n*'及C*n*="47"之接受者將發現C*n*="7"應意謂C*n*'="8"，而非"4"。

即使在第一明文符號與第二明文符號相同的情況下，第二明文符號P*(n+1)*仍可具有完全不同的轉譯表。舉例而言，對於第二明文符號P*(n+1)*="5"，第一轉譯表B1 1506提供第三輸出符號C*(n+1)*'="*"(亦即，"5"轉譯為"*")。第三輸出符號C*(n+1)*'="*"可接著用作至第二轉譯表B2 1508之輸入以獲得第四輸出符號C*(n+1)*="1"(亦即，"*"轉譯為"1")。如前文，符號對C*(n+1)*'及C*(n+1)*之冗餘使用可用作鑑認形式。

圖16說明根據一實例之用於執行明文加密之方法。獲得在n個符號之集合內所界定的複數個輸入符號1602。自界定不同符號至符號排列之複數個轉譯表獲得用於待加密之輸入符號中之每一者的偽隨機選定轉譯表1604。使用輸入符號之用於輸入符號中之每一者的相應轉譯表而將輸入符

號轉譯為相應輸出符號以個別地加密每一輸入符號1606。可接著將輸出符號傳輸至解密裝置1608。

在此方法之一實例中，獲得第一明文符號，其中第一明文符號可為集合中之n個符號中的一者。獲得將n個符號轉譯為n個符號之不同排列的第一轉譯表。可藉由使用偽隨機數以混洗n個符號來偽隨機地產生第一轉譯表。接著使用第一轉譯表而將第一明文符號轉譯為第一輸出符號。

可獲得將n個符號轉譯為不同於第一轉譯表之n個符號之排列的第二轉譯表。使用第二轉譯表而將第一輸出符號轉譯為第二輸出符號。接著基於第一輸出符號及/或第二輸出符號來傳輸加密符號。

圖17為說明可如何藉由使用一或多個反向轉譯表來解密加密符號C*i*以獲得單一明文符號之方塊圖。亦即，加密輸入符號C*i* 1702可由第一反向轉譯表A1 1704解密以獲得第一解密輸出符號C*i*' 1710，第一反向轉譯表A1 1704可基於自第一密碼產生器1708所獲得之第一密鑰流S*i*' 1706而被產生或選擇。第一解密輸出符號C*i*' 1710接著用作至第二反向轉譯表A2 1712之輸入以用於獲得明文輸出符號P*i* 1718，第二反向轉譯表A2 1712可基於自第二密碼產生器1716所獲得之第二密鑰流S*i* 1714而被產生或選擇。

在(例如)C*i*=(x,y)之替代組態中，加密符號x及y可以反序被解密，其中其經加密以獲得明文輸出符號P*i*。

圖18說明根據一實例之用於執行符號解密之方法。獲得在n個符號之集合內所界定的複數個(加密)輸入符號1802。

自界定不同符號至符號排列之複數個反向轉譯表獲得用於待解密之輸入符號中之每一者的偽隨機選定反向轉譯表1804。使用輸入符號之用於輸入符號中之每一者的相應反向轉譯表而將輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號1806。

在此方法之一實例中，獲得第一加密符號(輸入符號)，其中第一加密符號為集合中之n個符號中的一者。亦獲得將n個符號轉譯為n個符號之不同排列的第一反向轉譯表。可藉由使用偽隨機數以混洗n個符號來偽隨機地產生第一反向轉譯表。使用第一反向轉譯表而將第一加密符號轉譯為第一輸出符號。獲得將n個符號轉譯為不同於第一轉譯表之n個符號之排列的第二反向轉譯表。使用第二反向轉譯表而將第一輸出符號轉譯為第二輸出符號。可接著基於第一輸出符號及/或第二輸出符號來獲得明文符號。

圖19為說明根據一實例之加密模組的方塊圖。加密模組1902可包括經組態以將種值提供至密鑰流產生器1906之處理電路1904。密鑰流產生器1906產生被發送至處理電路1904之偽隨機數或符號密鑰流。耦接至處理電路1904之輸入介面1908可接收明文符號流。為了加密明文符號流，處理電路1904可經組態以使用自密鑰流所獲得之偽隨機數以自轉譯表產生器1910獲得轉譯表。轉譯表產生器1910可經組態以使用偽隨機數以便(例如)以偽隨機無偏差之方式來混洗及/或合併基本表之符號以提供轉譯表。處理電路1904接著使用轉譯表一次以將第一明文符號轉譯為加密符

號流之第一加密符號。加密符號流可經由耦接至處理電路1904之輸出介面1912而傳輸。對於明文符號流中之每一明文符號，不同轉譯表可被產生且用於轉譯彼符號。

圖20為說明根據一實例之解密模組的方塊圖。解密模組2002可包括經組態以將種值提供至密鑰流產生器2006之處理電路2004。密鑰流產生器2006產生被發送至處理電路2004之偽隨機數或符號密鑰流。耦接至處理電路2004之輸入介面2008可接收加密符號流。為瞭解密加密符號流，處理電路2004可經組態以使用自密鑰流所獲得之偽隨機數以自反向轉譯表產生器2010獲得轉譯表。反向轉譯表產生器2010可經組態以使用偽隨機數以便(例如)以偽隨機無偏差之方式來混洗及/或合併基本表之符號以提供轉譯表。處理電路2004接著使用反向轉譯表一次以將第一加密符號轉譯為明文符號流之第一明文符號。明文符號流可經由耦接至處理電路2004之輸出介面2012而傳輸。

為了使加密模組1902及解密模組2002分別適當地加密及解密符號，其可具有相同密鑰流產生器且具有互補轉譯表產生器。為了使密鑰流產生器1906及2006同步，可建立共同種值(例如，藉由安全鑑認機制)以用於加密模組與解密模組之間的特定通信會話。舉例而言，會話密鑰可用作密鑰流產生器1906及2006之種值。

雖然本文中所描述之一些實例指代DTMF載頻調之加密，但本文中所描述之加密方法可以用以保全所傳輸資訊之許多其他類型的通信系統來實施。

圖1至圖18中所說明之組件、步驟及/或功能中的一或多者可在不偏離本發明之情況下被重新配置及/或合併為單一組件、步驟及/或功能或分離為若干組件、步驟及/或功能。在不偏離本發明之情況下，亦可添加額外元件、組件、步驟及/或功能。圖1、圖2、圖3、圖5、圖7、圖9、圖13、圖17、圖19及/或圖20中所說明之設備、裝置及/或組件可經組態以執行圖2、圖4、圖6、圖8、圖10、圖11、圖12、圖14、圖15、圖16及/或圖18中所描述之方法、特徵或步驟中的一或多者。

熟習此項技術者將進一步瞭解，結合本文中所揭示之實例而描述之各種說明性邏輯區塊、模組、電路及演算法步驟可被實施為電子硬體、電腦軟體或兩者之組合。為了清晰地說明硬體與軟體之此互換性，上文通常已依據功能性來描述各種說明性組件、區塊、模組、電路及步驟。此功能性被實施為硬體還是軟體視強加於整個系統上之特定應用及設計約束而定。

應注意，前述組態僅為實例且不應被解釋為限制本發明。預期此等實例之描述為說明性的且不限制申請專利範圍之範疇。如此，本教示可被容易地應用於其他類型之設備，且許多替代例、修改及變化對於熟習此項技術者而言將為明顯的。

【圖式簡單說明】

圖1說明安全裝置可沿通信線而耦接至電話以保全電話與安全伺服器之間的特定通信之系統。

圖2為說明用於保全電話與屬於圖1之發行機構之安全伺服器之間的特定通信之方法的流程圖。

圖3說明可使得能夠在傳輸期間保全DTMF載頻調之電話服務安全伺服器之一實例的方塊圖。

圖4說明在安全伺服器上操作以用於保全來自電話裝置之DTMF載頻調的方法。

圖5說明可經組態以在傳輸期間保護DTMF載頻調之安全裝置之一實例的方塊圖。

圖6說明在安全裝置上操作以用於保全來自電話裝置之DTMF載頻調的方法。

圖7為經組態以利用安全伺服器來鑑認自身之行動通信裝置的方塊圖。

圖8為說明用於鑑認經由通信網路至電話服務臺之行動通信裝置之方法的流程圖。

圖9說明用於藉由偽隨機地選擇用於待加密之每一符號之轉譯表來保全明文符號之合併組合器的方塊圖。

圖10說明用於將明文符號轉譯為加密符號之符號至符號轉譯表的實例。

圖11說明可如何使用不同轉譯表來加密明文符號以獲得加密符號之一實例。

圖12說明用於自n個符號之集合的複數個可能排列選擇轉譯表之演算法，其中n為正整數。

圖13為說明可藉由使用多個轉譯表以加密單一明文符號來達成符號鑑認之另一加密機制的方塊圖。

圖14說明多個轉譯表可如何用於加密每一明文符號以獲得相應加密符號。

圖15說明兩個轉譯表可如何用於將明文符號轉譯或加密為加密符號之實例。

圖16說明根據一實例之用於執行明文加密之方法。

圖17為說明可如何藉由使用一或多個反向轉譯表來解密加密符號以獲得單一明文符號之方塊圖。

圖18說明根據一實例之用於執行明文加密之方法。

圖19為說明根據一實例之加密模組的方塊圖。

圖20為說明根據一實例之解密模組的方塊圖。

【主要元件符號說明】

| | |
|---|---|
| 102 | 安全裝置 |
| 104 | 電話 |
| 106 | 通信網路 |
| 108 | 發行機構 |
| 110 | 安全伺服器 |
| 302 | 安全伺服器 |
| 304 | 處理電路 |
| 306 | 第一通信模組 |
| 308 | 鑑認模組 |
| 310 | DTMF解密模組 |
| 502 | 安全裝置 |
| 504 | 處理電路 |
| 506 | 第一通信介面A |

| | |
|---|---|
| 508 | 第二通信介面B |
| 510 | DTMF偵測器 |
| 512 | DTMF加密模組 |
| 702 | 行動通信裝置 |
| 704 | 處理電路 |
| 706 | 通信模組 |
| 708 | 使用者輸入介面 |
| 802 | 行動通信裝置 |
| 804 | 電話服務臺 |
| 902 | 密碼產生器 |
| 904 | 密鑰流S*i* |
| 906 | 轉譯表 |
| 908 | 明文輸入符號P*i* |
| 910 | 加密輸出符號C*i* |
| 1002 | 符號至符號轉譯表 |
| 1102 | 明文符號 |
| 1104 | 轉譯表 |
| 1106 | 加密符號 |
| 1302 | 明文輸入符號P*i* |
| 1304 | 轉譯表A1 |
| 1306 | 第一密鑰流S*i*' |
| 1308 | 第一密碼產生器 |
| 1310 | 第一加密輸出符號C*i*' |
| 1312 | 第二轉譯表A2 |

1314 第二密鑰流 $S_i$

1316 第二密碼產生器

1318 第二加密輸出符號 $C_i$

1402 明文符號

1404 轉譯表

1406 轉譯表

1408 加密符號對

1502 第一轉譯表 A1

1504 第二轉譯表 A2

1506 第一轉譯表 B1

1508 第二轉譯表 B2

1702 加密輸入符號 $C_i$

1704 第一反向轉譯表 A1

1706 第一密鑰流 $S_i'$

1708 第一密碼產生器

1710 第一解密輸出符號 $C_i'$

1712 第二反向轉譯表 A2

1714 第二密鑰流 $S_i$

1716 第二密碼產生器

1718 明文輸出符號 $P_i$

1902 加密模組

1904 處理電路

1906 密鑰流產生器

1908 輸入介面

| | |
|---|---|
| 1910 | 轉譯表產生器 |
| 1912 | 輸出介面 |
| 2002 | 解密模組 |
| 2004 | 處理電路 |
| 2006 | 密鑰流產生器 |
| 2008 | 輸入介面 |
| 2010 | 反向轉譯表產生器 |
| 2012 | 輸出介面 |

## 五、中文發明摘要：

另一特徵提供一種防護加密符號之安全性的有效加密方法。藉由使用一獨立偽隨機選定轉譯表來加密每一明文符號。而非將符號之每一可能排列預儲存為轉譯表，可基於一偽隨機數及一符號混洗演算法而在運作中有效地產生該等轉譯表。一接收裝置可類似地在運作中產生反向轉譯表以解密所接收加密符號。

## 六、英文發明摘要：

Another feature provides an efficient encryption method that safeguards the security of encrypted symbols. Each plaintext symbol is encrypted by using a separate pseudorandomly selected translation table. Rather than pre-storing every possible permutation of symbols as translation tables, the translation tables may be efficiently generated on-the-fly based on a pseudorandom number and a symbol shuffling algorithm. A receiving device may similarly generate reverse translation tables on-the-fly to decrypt received encrypted symbols.

# 十、申請專利範圍：

1. 一種在一加密裝置上操作之方法，包含：

獲得複數個輸入符號；

自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者的偽隨機選定轉譯表；及

使用該等輸入符號之用於該等輸入符號中之每一者的相應轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號。

2. 如請求項1之方法，其中獲得用於待加密之該等輸入符號中之每一者的該偽隨機選定轉譯表包括：

獲得一用於一第一輸入符號之偽隨機選定第一轉譯表；及

獲得一用於一第二輸入符號之偽隨機選定第二轉譯表；

且其中使用該等輸入符號之用於該等輸入符號中之每一者的相應轉譯表而將該等輸入符號轉譯為相應輸出符號包括：

使用該第一轉譯表而將該第一輸入符號轉譯為一第一輸出符號；及

使用該第二轉譯表而將該第二輸入符號轉譯為一第二輸出符號。

3. 如請求項1之方法，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一轉譯表為該N個符號

之一排列。

4. 如請求項3之方法，其中獲得用於待加密之該等輸入符號中之每一者的該偽隨機選定轉譯表包括：

獲得一用於待加密之一第一輸入符號的第一偽隨機數；及

混洗N個符號之該集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該轉譯表。

5. 如請求項4之方法，其中該第一偽隨機數藉由以下各項來獲得：

產生一用於該第一輸入符號之偽隨機數，其中該偽隨機數為k個位元長且k為一正整數；

判定該偽隨機數是否在一最大數Pmax內，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

在該偽隨機數大於該最大數Pmax時廢除該偽隨機數；

獲得用於該第一輸入符號之不同偽隨機數，直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止；及

以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數。

6. 如請求項4之方法，其中混洗N個符號之該集合包括：

以N個符號之該集合的所有符號來初始化一排列向量P；及

基於該第一偽隨機數來混洗該排列向量中之該等符號。

7. 如請求項1之方法，進一步包含：

將該等輸出符號傳輸至一解密裝置。

8. 如請求項1之方法，進一步包含：

自界定不同符號至符號排列之該複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者的第二偽隨機選定轉譯表；及

使用該等輸出符號之用於該等輸出符號中之每一者的相應第二轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地加密每一輸入符號。

9. 一種加密裝置，包含：

用於獲得複數個輸入符號之構件；

用於自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者之偽隨機選定轉譯表的構件；及

用於使用該等輸入符號之用於該等輸入符號中之每一者的相應轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號之構件。

10. 如請求項9之裝置，進一步包含：

用於獲得一用於一第一輸入符號之偽隨機選定第一轉譯表的構件；

用於獲得一用於一第二輸入符號之偽隨機選定第二轉譯表的構件；

用於使用該第一轉譯表而將該第一輸入符號轉譯為一第一輸出符號之構件；及

用於使用該第二轉譯表而將該第二輸入符號轉譯為一第二輸出符號之構件。

11. 如請求項9之裝置，進一步包含：

用於獲得一用於待加密之一第一輸入符號之第一偽隨機數的構件；及

用於混洗N個符號之集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該轉譯表的構件。

12. 如請求項11之裝置，進一步包含：

用於產生一用於該第一輸入符號之偽隨機數的構件，其中該偽隨機數為k個位元長且k為一正整數；

用於判定該偽隨機數是否在一最大數Pmax內之構件，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

用於在該偽隨機數大於該最大數Pmax時廢除該偽隨機數之構件；

用於獲得用於該第一輸入符號之不同偽隨機數直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止的構件；及

用於以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數之構件。

13. 如請求項9之裝置，進一步包含：

用於將該等輸出符號傳輸至一解密裝置之構件。

14. 如請求項9之裝置，進一步包含：

用於自界定不同符號至符號排列之該複數個轉譯表獲

得一用於待加密之該等輸入符號中之每一者之第二偽隨機選定轉譯表的構件；及

用於使用該等輸出符號之用於該等輸出符號中之每一者的相應第二轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地加密每一輸入符號之構件。

15. 一種加密裝置，包含：

一輸入介面，其用於接收一輸入符號流；及

一處理電路，其耦接至該輸入介面，該處理電路經組態以：

自該輸入介面獲得複數個輸入符號；

自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者的偽隨機選定轉譯表；及

使用該等輸入符號之用於該等輸入符號中之每一者的相應轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號。

16. 如請求項15之裝置，進一步包含：

一輸出介面，其耦接至該處理電路以用於傳輸該等輸出符號。

17. 如請求項15之裝置，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一轉譯表為該N個符號之一排列。

18. 如請求項17之裝置，進一步包含：

一耦接至該處理電路之密鑰流產生器，該密鑰流產生

器經組態以自該密鑰流產生器獲得一用於待加密之一第一輸入符號的第一偽隨機數；及

一耦接至該處理電路之轉譯表產生器，該轉譯表產生器經組態以混洗N個符號之該集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該轉譯表。

19. 如請求項17之裝置，其中該處理電路進一步經組態以：

產生一用於該第一輸入符號之偽隨機數，其中該偽隨機數為k個位元長且k為一正整數；

判定該偽隨機數是否在一最大數Pmax內，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

在該偽隨機數大於該最大數Pmax時廢除該偽隨機數；

獲得用於該第一輸入符號之不同偽隨機數，直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止；及

以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數。

20. 如請求項17之裝置，其中該處理電路進一步經組態以：

自界定不同符號至符號排列之該複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者的第二偽隨機選定轉譯表；及

使用該等輸出符號之用於該等輸出符號中之每一者的相應第二轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地加密每一輸入符號。

21. 一種機器可讀媒體，其具有操作以用於加密符號之一或

多個指令，該指令在由一處理器執行時使該處理器：

獲得複數個輸入符號；

自界定不同符號至符號排列之複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者的偽隨機選定轉譯表；及

使用該等輸入符號之用於該等輸入符號中之每一者的相應轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號。

22. 如請求項21之機器可讀媒體，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一轉譯表為該N個符號之一排列。

23. 如請求項22之機器可讀媒體，其具有一或多個指令，該指令在由一處理器執行時使該處理器進一步：

獲得一用於待加密之一第一輸入符號的第一偽隨機數；及

混洗N個符號之該集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該轉譯表。

24. 如請求項22之機器可讀媒體，其具有一或多個指令，該指令在由一處理器執行時使該處理器進一步：

產生一用於該第一輸入符號之偽隨機數，其中該偽隨機數為k個位元長且k為一正整數；

判定該偽隨機數是否在一最大數Pmax內，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

在該偽隨機數大於該最大數Pmax時廢除該偽隨機數；

獲得用於該第一輸入符號之不同偽隨機數，直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止；及

以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數。

25. 如請求項21之機器可讀媒體，其具有一或多個指令，該指令在由一處理器執行時使該處理器進一步：

自界定不同符號至符號排列之該複數個轉譯表獲得一用於待加密之該等輸入符號中之每一者的第二偽隨機選定轉譯表；及

使用該等輸出符號之用於該等輸出符號中之每一者的相應第二轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地加密每一輸入符號。

26. 一種用於解密符號之方法，包含：

獲得在n個符號之一集合內所界定的複數個輸入符號；

自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者的偽隨機選定反向轉譯表；及

使用該等輸入符號之用於該等輸入符號中之每一者的相應反向轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號。

27. 如請求項26之方法，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一反向轉譯表為該N

個符號之一排列，且進一步包含：

獲得一用於待解密之一第一輸入符號的第一偽隨機數；及

混洗N個符號之該集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該反向轉譯表。

28. 如請求項27之方法，其中該第一偽隨機數藉由以下各項來獲得：

產生一用於該第一輸入符號之偽隨機數，其中該偽隨機數為k個位元長且k為一正整數；

判定該偽隨機數是否在一最大數Pmax內，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

在該偽隨機數大於該最大數Pmax時廢除該偽隨機數；

獲得用於該第一輸入符號之不同偽隨機數，直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止；及

以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數。

29. 如請求項26之方法，進一步包含：

自界定不同符號至符號排列之該複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者的第二偽隨機選定反向轉譯表；及

使用該等輸出符號之用於該等輸出符號中之每一者的相應第二反向轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地解密每一輸入符號。

30. 一種解密裝置，包含：

用於獲得在n個符號之一集合內所界定之複數個輸入符號的構件；

用於自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者之偽隨機選定反向轉譯表的構件；及

用於使用該等輸入符號之用於該等輸入符號中之每一者的相應反向轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號之構件。

31. 如請求項30之裝置，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一反向轉譯表為該N個符號之一排列，且進一步包含：

用於獲得一用於待解密之一第一輸入符號之第一偽隨機數的構件；及

用於混洗N個符號之該集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該反向轉譯表的構件。

32. 如請求項31之裝置，其中該第一偽隨機數藉由以下各項來獲得：

用於產生一用於該第一輸入符號之偽隨機數的構件，其中該偽隨機數為k個位元長且k為一正整數；

用於判定該偽隨機數是否在一最大數Pmax內之構件，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

用於在該偽隨機數大於該最大數Pmax時廢除該偽隨機

數之構件；

用於獲得用於該第一輸入符號之不同偽隨機數直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止的構件；及

用於以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數之構件。

33. 如請求項30之裝置，進一步包含：

用於自界定不同符號至符號排列之該複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者之第二偽隨機選定反向轉譯表的構件；及

用於使用該等輸出符號之用於該等輸出符號中之每一者的相應第二反向轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地解密每一輸入符號之構件。

34. 一種解密裝置，包含：

一輸入介面，其用於接收一輸入符號流；及

一處理電路，其耦接至該輸入介面，該處理電路經組態以：

獲得在n個符號之一集合內所界定的複數個輸入符號；

自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者的偽隨機選定反向轉譯表；及

使用該等輸入符號之用於該等輸入符號中之每一者

的相應反向轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號。

35. 如請求項34之裝置，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一反向轉譯表為該N個符號之一排列，且進一步包含：

一耦接至該處理電路之密鑰流產生器，經組態之該密鑰流產生器自該密鑰流產生器獲得一用於待解密之一第一輸入符號的第一偽隨機數；及

一耦接至該處理電路之反向轉譯表產生器，該反向轉譯表產生器經組態以混洗N個符號之該集合以獲得N個符號之該集合的一不同排列且使用彼排列作為用於該第一輸入符號之該反向轉譯表。

36. 如請求項34之裝置，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一反向轉譯表為該N個符號之一排列，且該處理電路進一步經組態以：

產生一用於該第一輸入符號之偽隨機數，其中該偽隨機數為k個位元長且k為一正整數；

判定該偽隨機數是否在一最大數Pmax內，其中Pmax為小於一最大臨限值$2^k$之N階乘的最大倍數；

在該偽隨機數大於該最大數Pmax時廢除該偽隨機數；

獲得用於該第一輸入符號之不同偽隨機數，直至獲得一小於或等於該最大數Pmax之可接受偽隨機數為止；及

以N階乘為模數來除該可接受偽隨機數以獲得該第一偽隨機數。

37. 如請求項34之裝置，其中該處理電路進一步經組態以：

自界定不同符號至符號排列之該複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者的第二偽隨機選定反向轉譯表；及

使用該等輸出符號之用於該等輸出符號中之每一者的相應第二反向轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地解密每一輸入符號。

38. 一種機器可讀媒體，其具有用於解密符號之一或多個指令，該指令在由一處理器執行時使該處理器：

獲得在n個符號之一集合內所界定的複數個輸入符號；

自界定不同符號至符號排列之複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者的偽隨機選定反向轉譯表；及

使用該等輸入符號之用於該等輸入符號中之每一者的相應反向轉譯表而將該等輸入符號轉譯為相應輸出符號以個別地解密每一輸入符號。

39. 如請求項38之機器可讀媒體，其中該複數個輸入符號由N個符號之一集合界定，其中N為一正整數且一反向轉譯表為該N個符號之一排列，且進一步包含一或多個指令，該指令在由一處理器執行時使該處理器進一步：

獲得一用於待解密之一第一輸入符號的第一偽隨機數；及

混洗N個符號之該集合以獲得N個符號之該集合的一不

同排列且使用彼排列作為用於該第一輸入符號之該反向轉譯表。

40. 如請求項38之機器可讀媒體，其具有一或多個指令，該指令在由一處理器執行時使該處理器進一步：

自界定不同符號至符號排列之該複數個反向轉譯表獲得一用於待解密之該等輸入符號中之每一者的第二偽隨機選定反向轉譯表；及

使用該等輸出符號之用於該等輸出符號中之每一者的相應第二反向轉譯表而將該等輸出符號轉譯為相應第二輸出符號以進一步個別地解密每一輸入符號。

十一、圖式：

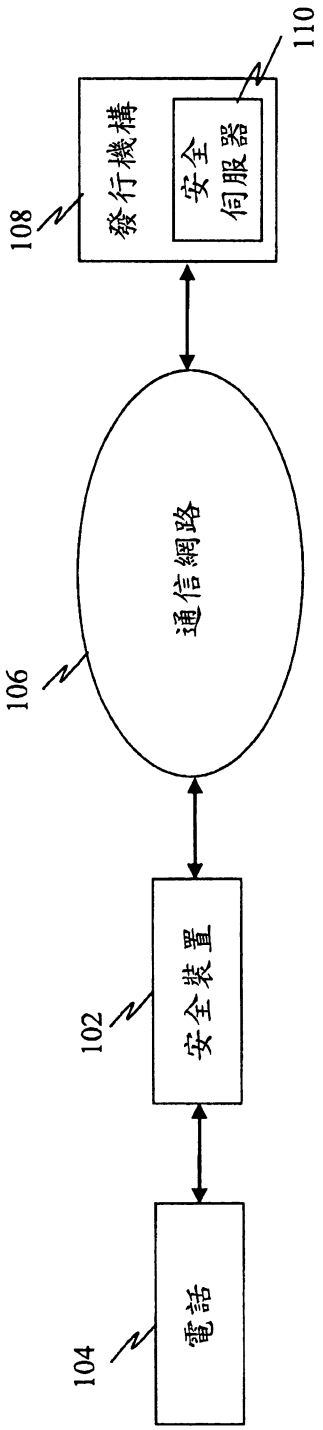


圖1

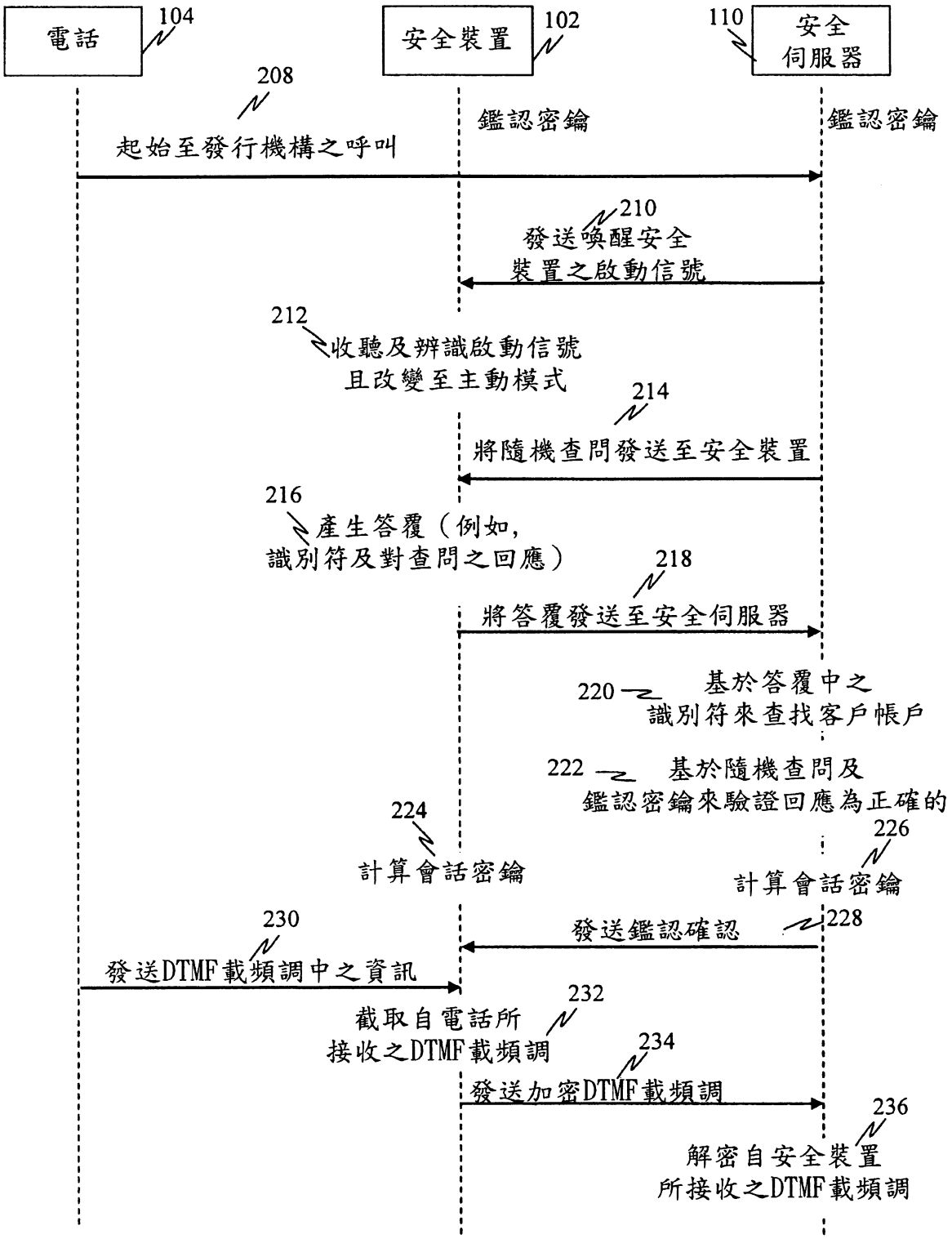
電話
104
安全裝置
102
110
安全伺服器
208
起始至發行機構之呼叫
鑑認密鑰
鑑認密鑰
210
發送喚醒安全裝置之啟動信號
212
收聽及辨識啟動信號且改變至主動模式
214
將隨機查問發送至安全裝置
216
產生答覆（例如，識別符及對查問之回應）
218
將答覆發送至安全伺服器
220
基於答覆中之識別符來查找客戶帳戶
222
基於隨機查問及鑑認密鑰來驗證回應為正確的
224
計算會話密鑰
226
計算會話密鑰
228
發送鑑認確認
230
發送DTMF載頻調中之資訊
232
截取自電話所接收之DTMF載頻調
234
發送加密DTMF載頻調
236
解密自安全裝置所接收之DTMF載頻調

圖2

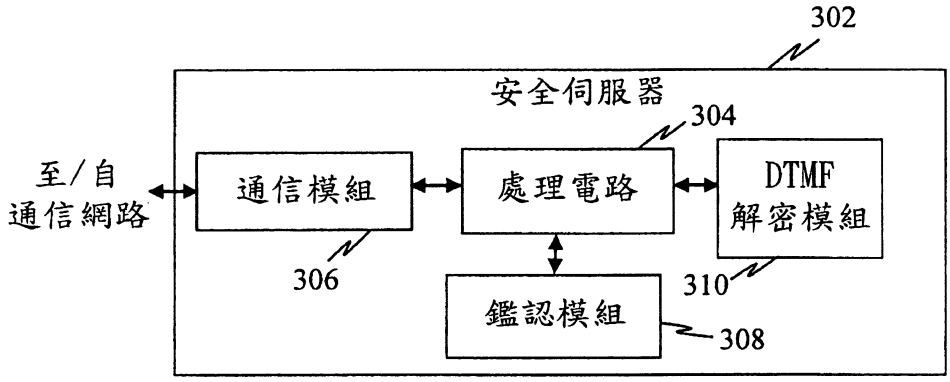
302
安全伺服器
304
至/自
通信網路
通信模組
處理電路
DTMF
解密模組
306
310
鑑認模組
308

圖3

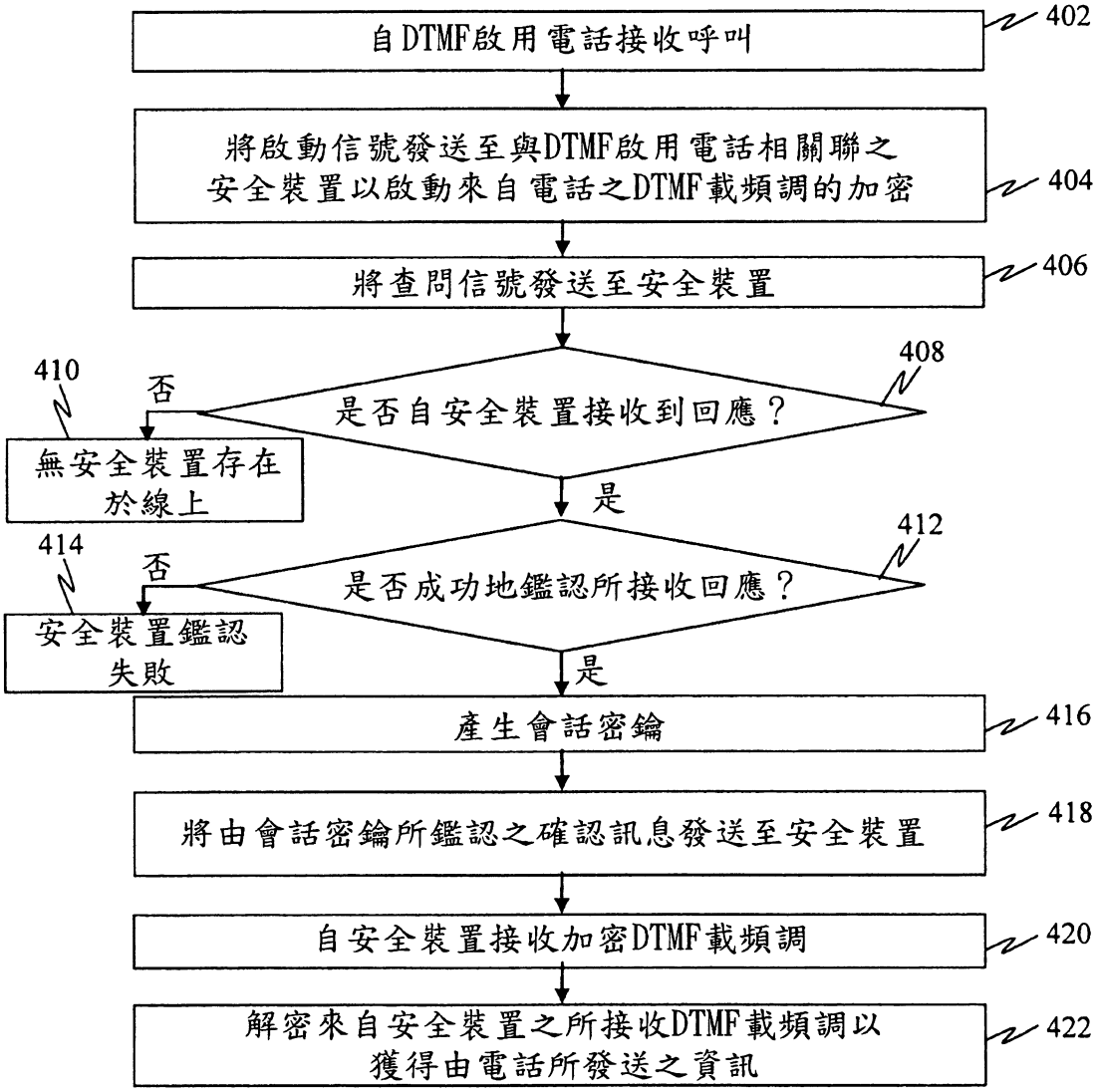
自DTMF啟用電話接收呼叫
402
將啟動信號發送至與DTMF啟用電話相關聯之
安全裝置以啟動來自電話之DTMF載頻調的加密
404
將查問信號發送至安全裝置
406
408
是否自安全裝置接收到回應？
否
410
無安全裝置存在
於線上
是
412
是否成功地鑑認所接收回應？
414
否
安全裝置鑑認
失敗
是
產生會話密鑰
416
將由會話密鑰所鑑認之確認訊息發送至安全裝置
418
自安全裝置接收加密DTMF載頻調
420
解密來自安全裝置之所接收DTMF載頻調以
獲得由電話所發送之資訊
422

圖4

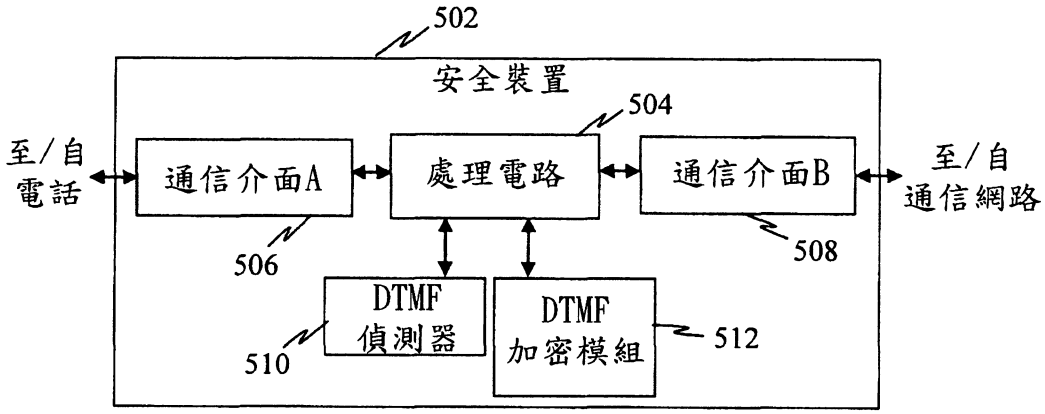
502
安全裝置
504
至/自
電話
通信介面A
處理電路
通信介面B
至/自
通信網路
506
508
DTMF
偵測器
DTMF
加密模組
510
512

圖5

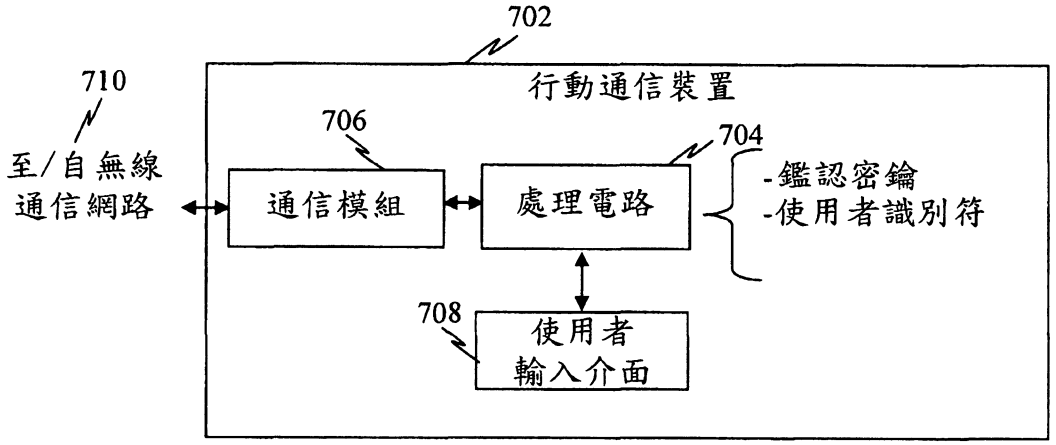
702
行動通信裝置
710
至/自無線
通信網路
706
704
通信模組
處理電路
-鑑認密鑰
-使用者識別符
708
使用者
輸入介面

圖7

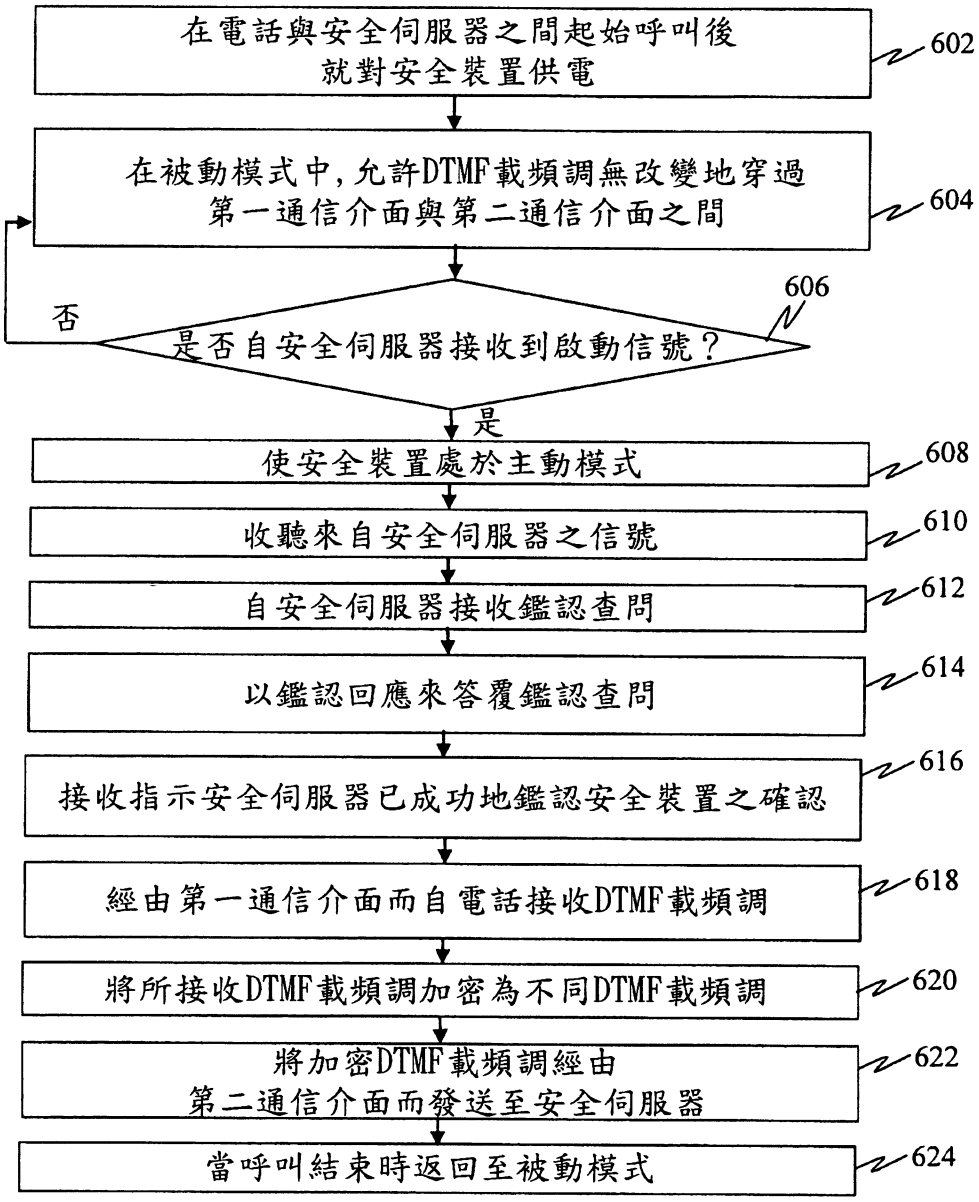
在電話與安全伺服器之間起始呼叫後
就對安全裝置供電
602
在被動模式中，允許DTMF載頻調無改變地穿過
第一通信介面與第二通信介面之間
604
606
否
是否自安全伺服器接收到啟動信號？
是
使安全裝置處於主動模式
608
收聽來自安全伺服器之信號
610
自安全伺服器接收鑑認查問
612
以鑑認回應來答覆鑑認查問
614
接收指示安全伺服器已成功地鑑認安全裝置之確認
616
經由第一通信介面而自電話接收DTMF載頻調
618
將所接收DTMF載頻調加密為不同DTMF載頻調
620
將加密DTMF載頻調經由
第二通信介面而發送至安全伺服器
622
當呼叫結束時返回至被動模式
624

圖6

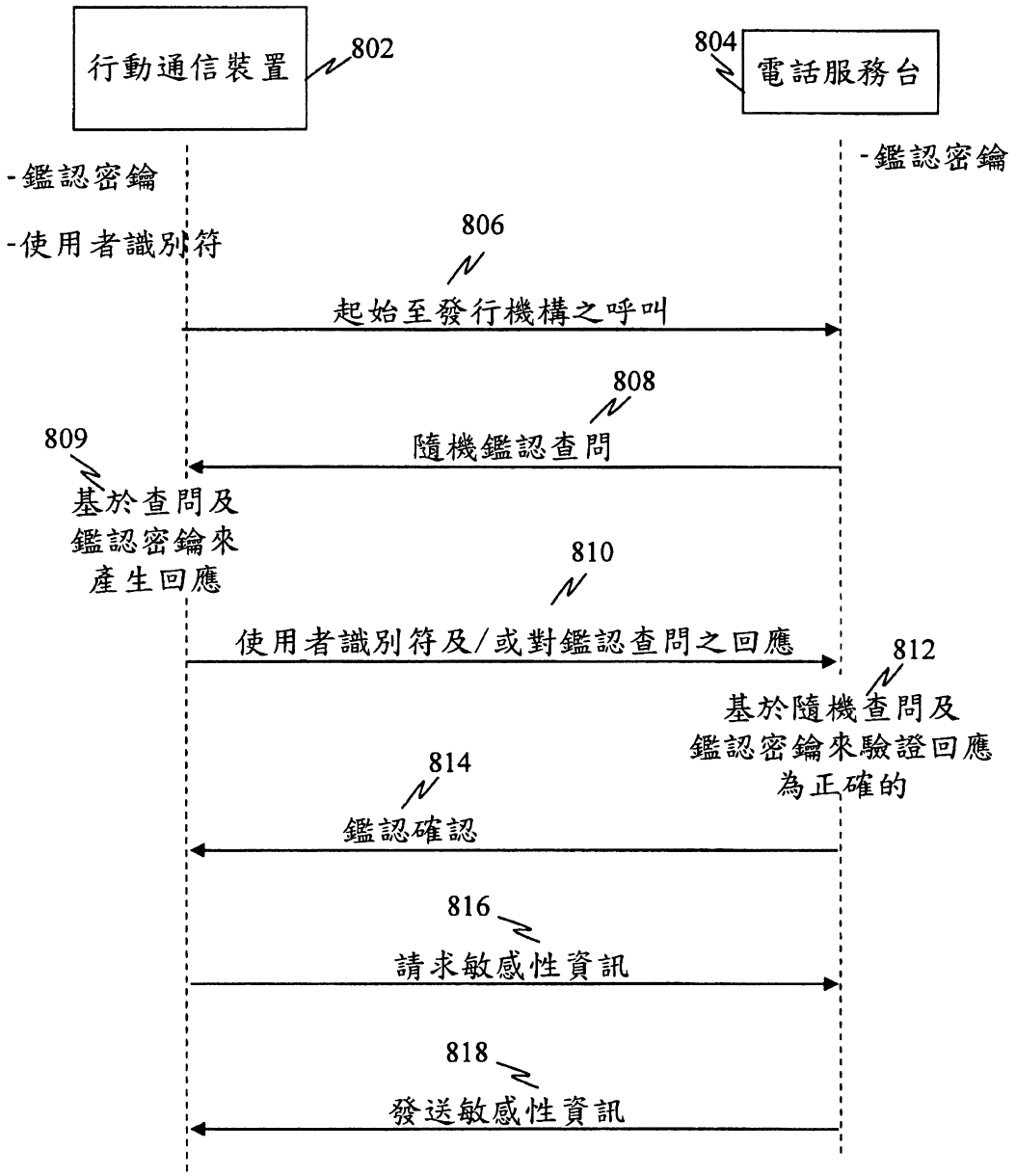
行動通信裝置
802
804
電話服務台
-鑑認密鑰
-使用者識別符
-鑑認密鑰
806
起始至發行機構之呼叫
808
隨機鑑認查問
809
基於查問及
鑑認密鑰來
產生回應
810
使用者識別符及/或對鑑認查問之回應
812
基於隨機查問及
鑑認密鑰來驗證回應
為正確的
814
鑑認確認
816
請求敏感性資訊
818
發送敏感性資訊

圖8

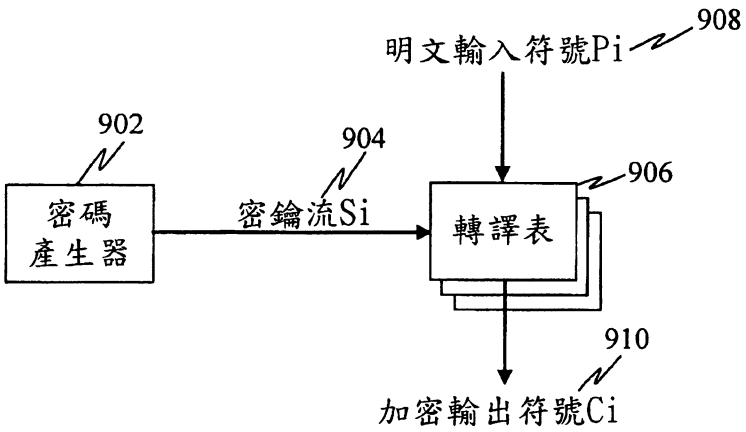


圖9

| 明文符號 | 二進位之明文符號 | 加密符號 | 二進位之加密符號 |
|---|---|---|---|
| 0 | 0000 | 5 | 0101 |
| 1 | 0001 | 9 | 1001 |
| 2 | 0010 | A | 1100 |
| 3 | 0011 | 0 | 0000 |
| 4 | 0100 | # | 1011 |
| 5 | 0101 | 1 | 0001 |
| 6 | 0110 | C | 1110 |
| 7 | 0111 | * | 1010 |
| 8 | 1000 | 7 | 0111 |
| 9 | 1001 | B | 1101 |
| * | 1010 | 4 | 0100 |
| # | 1011 | 6 | 0110 |
| A | 1100 | D | 1111 |
| B | 1101 | 2 | 0001 |
| C | 1110 | 8 | 1000 |
| D | 1111 | 3 | 0011 |

1002

圖10

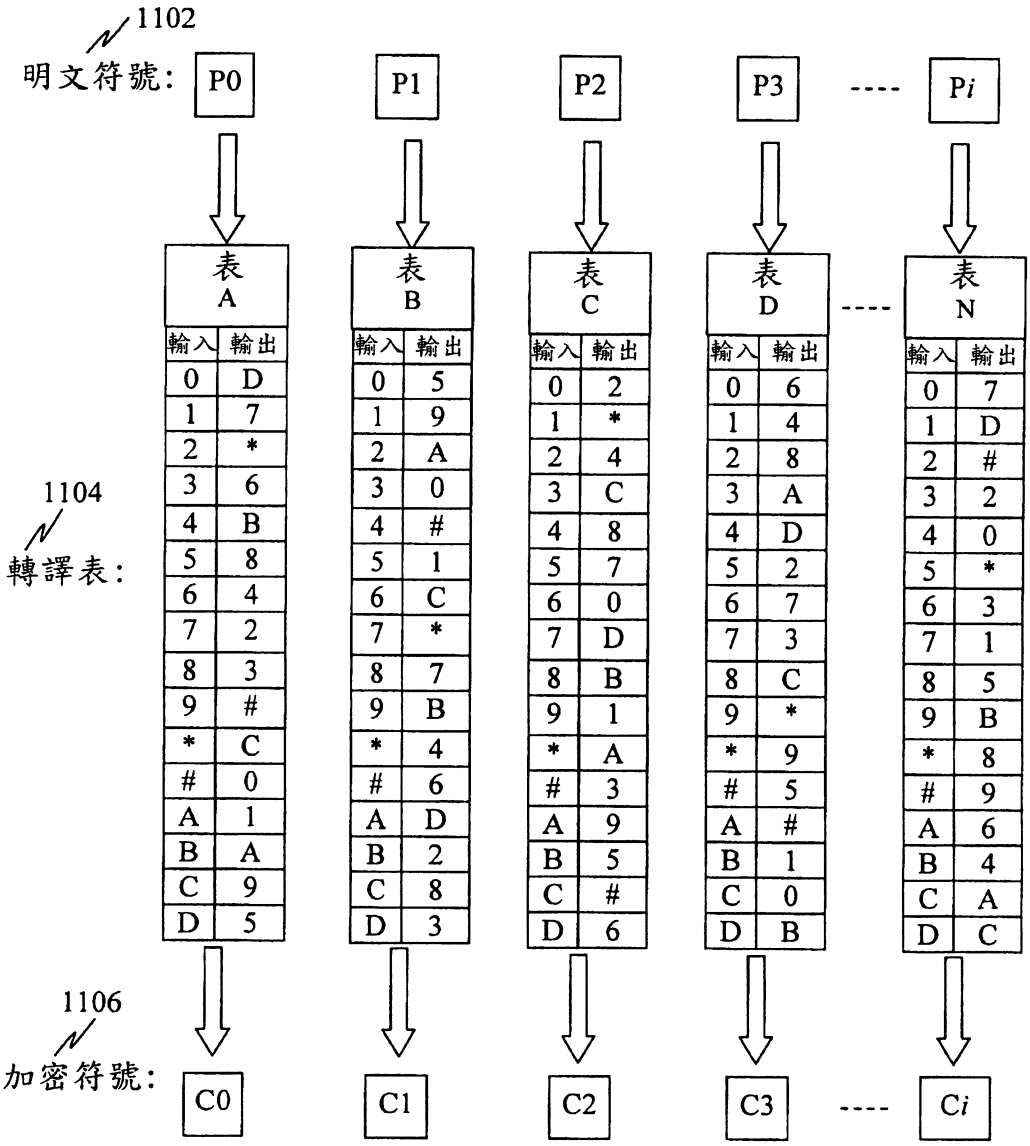
1102
明文符號:
P0
P1
P2
P3
----
Pi
1104
轉譯表:
表 A
表 B
表 C
表 D
----
表 N
輸入 輸出
0 D
1 7
2 *
3 6
4 B
5 8
6 4
7 2
8 3
9 #
* C
# 0
A 1
B A
C 9
D 5
輸入 輸出
0 5
1 9
2 A
3 0
4 #
5 1
6 C
7 *
8 7
9 B
* 4
# 6
A D
B 2
C 8
D 3
輸入 輸出
0 2
1 *
2 4
3 C
4 8
5 7
6 0
7 D
8 B
9 1
* A
# 3
A 9
B 5
C #
D 6
輸入 輸出
0 6
1 4
2 8
3 A
4 D
5 2
6 7
7 3
8 C
9 *
* 9
# 5
A #
B 1
C 0
D B
輸入 輸出
0 7
1 D
2 #
3 2
4 0
5 *
6 3
7 1
8 5
9 B
* 8
# 9
A 6
B 4
C A
D C
1106
加密符號:
C0
C1
C2
C3
----
Ci

圖11

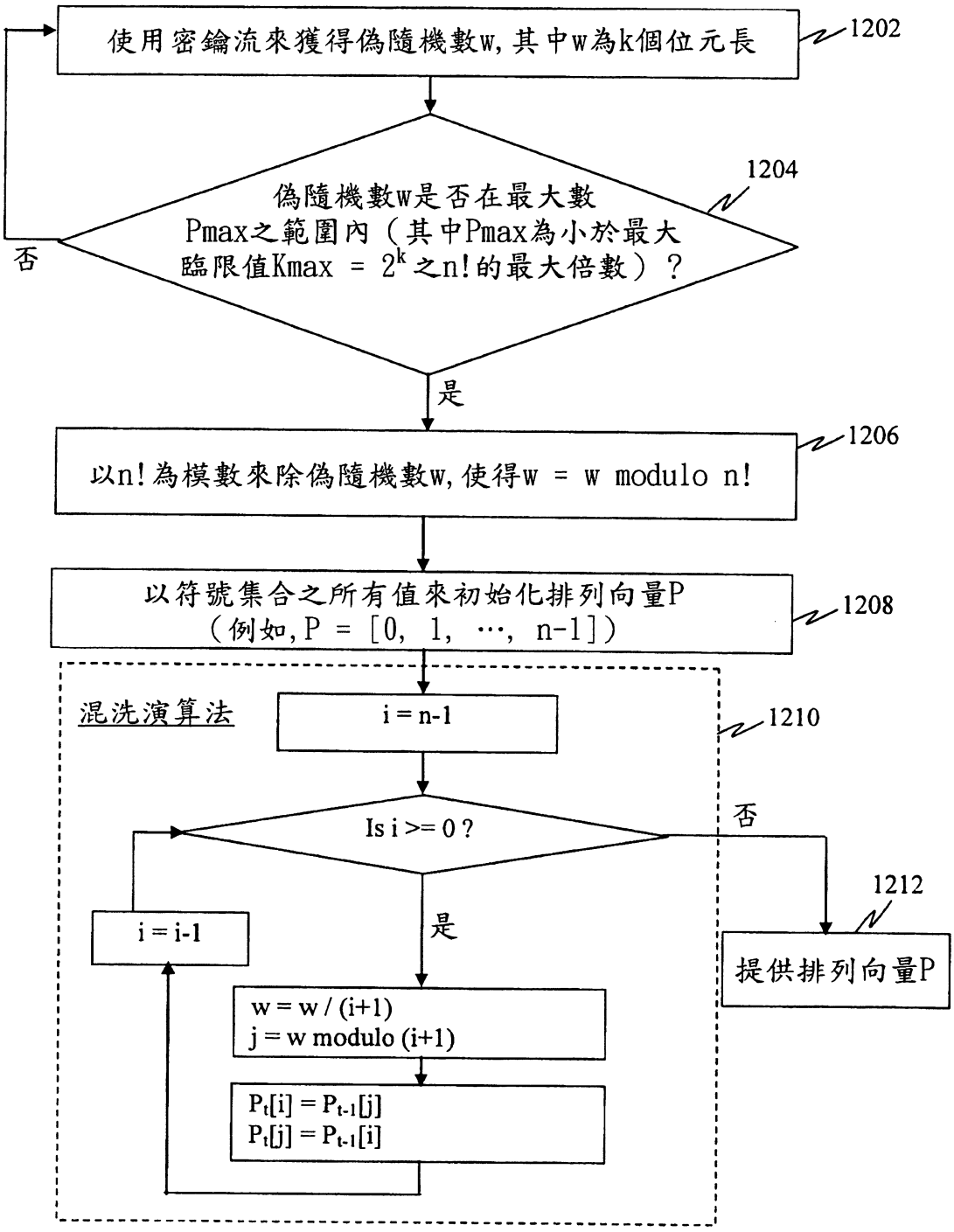
使用密鑰流來獲得偽隨機數w, 其中w為k個位元長
1202
偽隨機數w是否在最大數Pmax之範圍內（其中Pmax為小於最大臨限值Kmax = 2^k之n!的最大倍數）？
1204
否
是
以n!為模數來除偽隨機數w, 使得w = w modulo n!
1206
以符號集合之所有值來初始化排列向量P（例如, P = [0, 1, …, n-1]）
1208
混洗演算法
i = n-1
1210
Is i >= 0 ?
否
是
1212
提供排列向量P
i = i-1
w = w / (i+1)
j = w modulo (i+1)
Pt[i] = Pt-1[j]
Pt[j] = Pt-1[i]

圖12

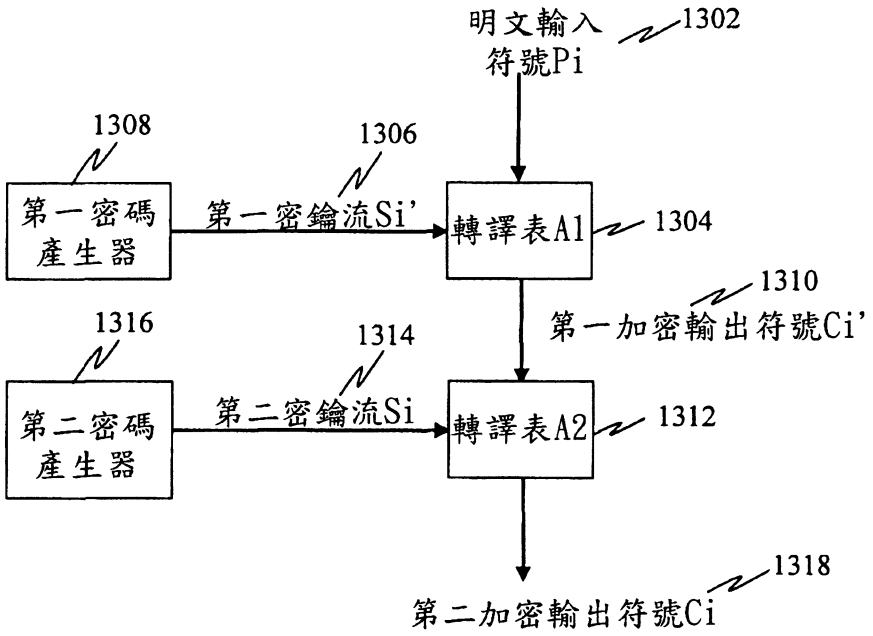
明文輸入
符號Pi
1302
1308
1306
第一密碼
產生器
第一密鑰流Si'
轉譯表A1
1304
1310
第一加密輸出符號Ci'
1316
1314
第二密碼
產生器
第二密鑰流Si
轉譯表A2
1312
1318
第二加密輸出符號Ci

圖13

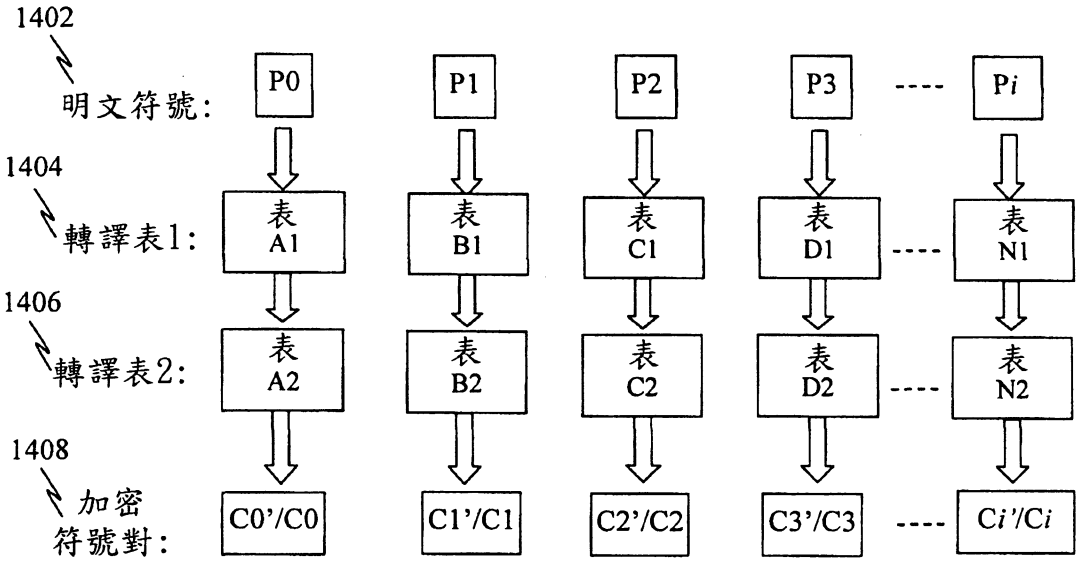
1402
明文符號:
P0
P1
P2
P3
----
Pi
1404
轉譯表1:
表
A1
表
B1
表
C1
表
D1
----
表
N1
1406
轉譯表2:
表
A2
表
B2
表
C2
表
D2
----
表
N2
1408
加密
符號對:
C0'/C0
C1'/C1
C2'/C2
C3'/C3
----
Ci'/Ci

圖14

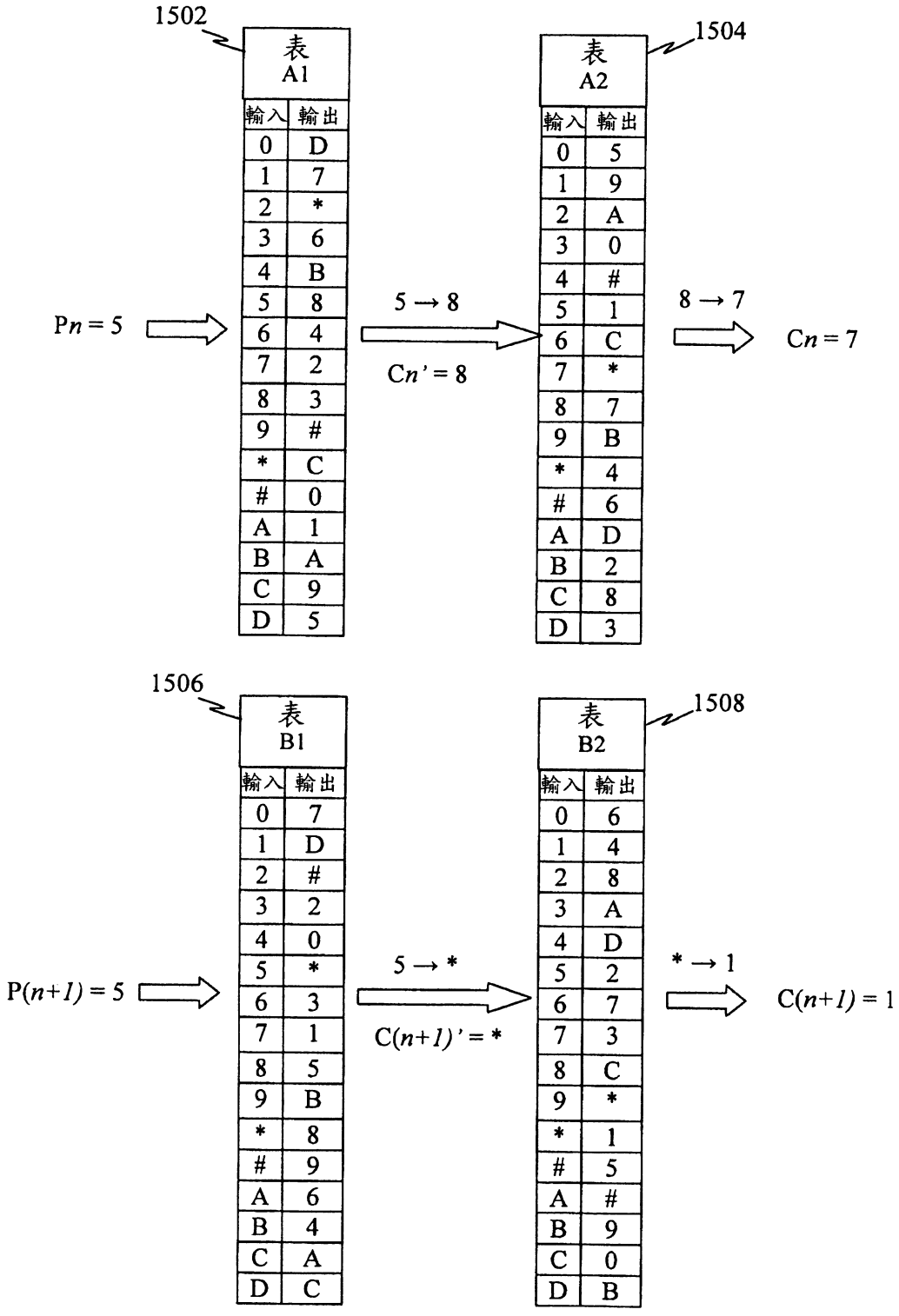
1502
表
A1
輸入 輸出
0 D
1 7
2 *
3 6
4 B
5 8
6 4
7 2
8 3
9 #
* C
# 0
A 1
B A
C 9
D 5
1504
表
A2
輸入 輸出
0 5
1 9
2 A
3 0
4 #
5 1
6 C
7 *
8 7
9 B
* 4
# 6
A D
B 2
C 8
D 3
Pn = 5
5 → 8
Cn' = 8
8 → 7
Cn = 7
1506
表
B1
輸入 輸出
0 7
1 D
2 #
3 2
4 0
5 *
6 3
7 1
8 5
9 B
* 8
# 9
A 6
B 4
C A
D C
1508
表
B2
輸入 輸出
0 6
1 4
2 8
3 A
4 D
5 2
6 7
7 3
8 C
9 *
* 1
# 5
A #
B 9
C 0
D B
P(n+1) = 5
5 → *
C(n+1)' = *
* → 1
C(n+1) = 1

圖15

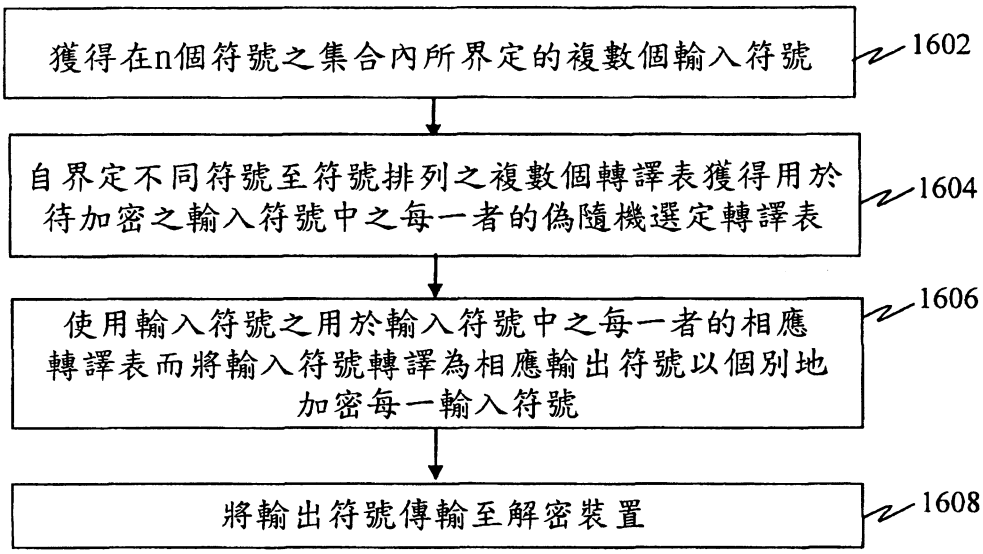
獲得在n個符號之集合內所界定的複數個輸入符號
1602
自界定不同符號至符號排列之複數個轉譯表獲得用於待加密之輸入符號中之每一者的偽隨機選定轉譯表
1604
使用輸入符號之用於輸入符號中之每一者的相應轉譯表而將輸入符號轉譯為相應輸出符號以個別地加密每一輸入符號
1606
將輸出符號傳輸至解密裝置
1608

圖16

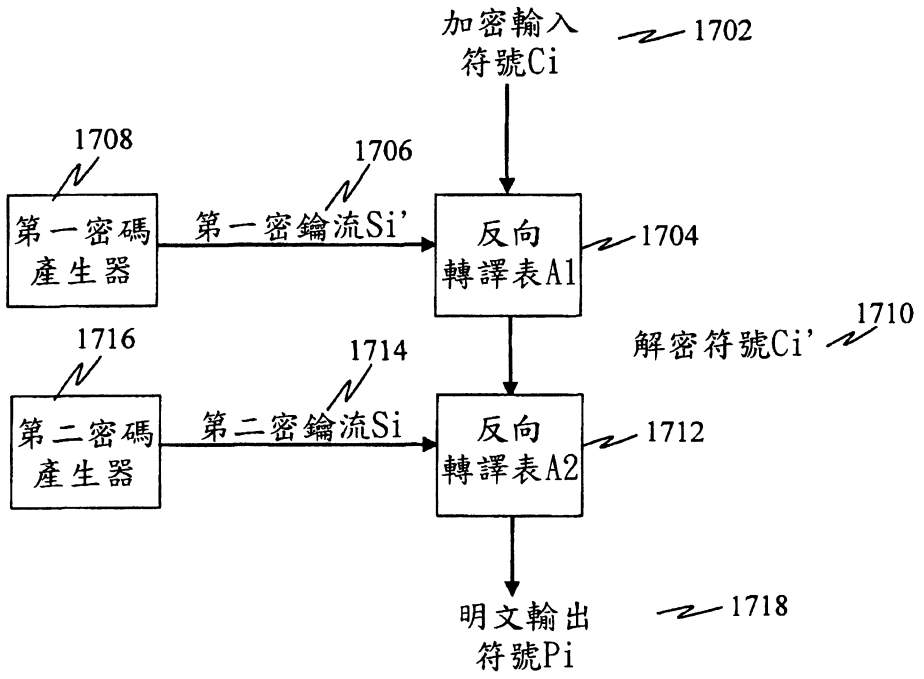
加密輸入
符號Ci
1702
1708
1706
第一密碼
產生器
第一密鑰流Si'
反向
轉譯表A1
1704
1710
解密符號Ci'
1716
1714
第二密碼
產生器
第二密鑰流Si
反向
轉譯表A2
1712
明文輸出
符號Pi
1718

圖17

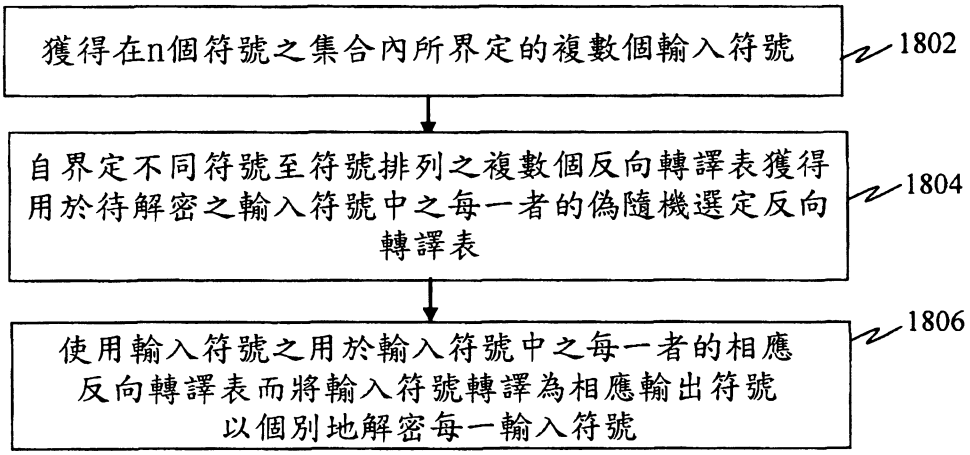
獲得在n個符號之集合內所界定的複數個輸入符號
1802
自界定不同符號至符號排列之複數個反向轉譯表獲得
用於待解密之輸入符號中之每一者的偽隨機選定反向
轉譯表
1804
使用輸入符號之用於輸入符號中之每一者的相應
反向轉譯表而將輸入符號轉譯為相應輸出符號
以個別地解密每一輸入符號
1806

圖18

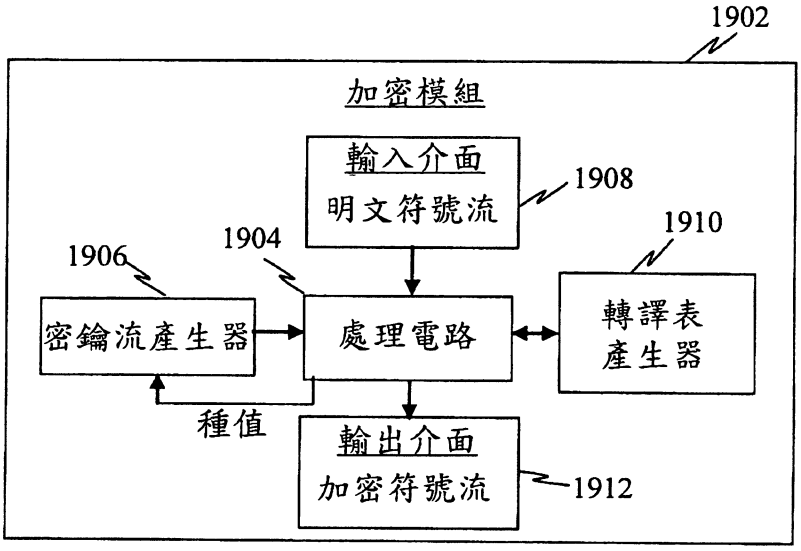
1902
加密模組
輸入介面
明文符號流
1908
1910
1904
1906
密鑰流產生器
處理電路
轉譯表
產生器
種值
輸出介面
加密符號流
1912

圖19

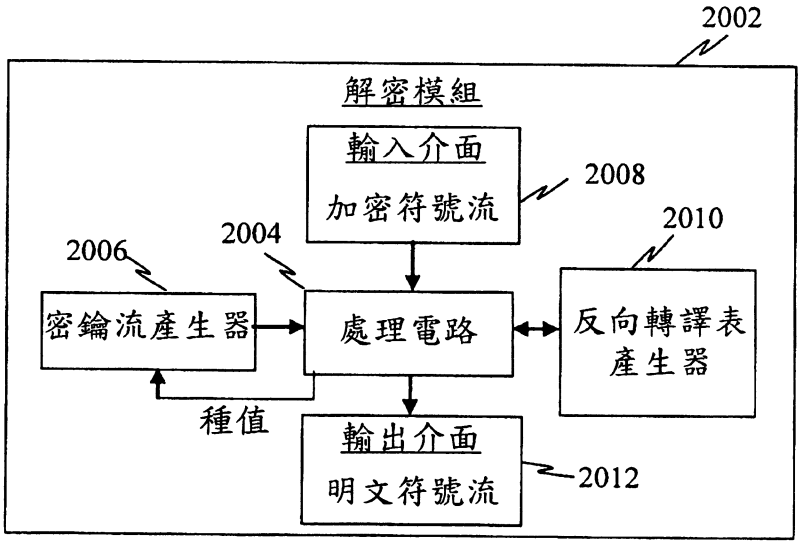
2002
解密模組
輸入介面
加密符號流
2008
2010
2004
2006
密鑰流產生器
處理電路
反向轉譯表
產生器
種值
輸出介面
明文符號流
2012

圖20

## 七、指定代表圖：

(一)本案指定代表圖為：第（ 16 ）圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

## 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)