201626752

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201626752 A

(43)公開日： 中華民國 105 (2016) 年 07 月 16 日

(21)申請案號：104133308 (22)申請日： 中華民國 104 (2015) 年 10 月 08 日

(51)Int. Cl.： *H04L9/08 (2006.01)*

(30)優先權：2014/10/09 瑞典 1451210-7

(71)申請人：凱利塞克股份有限公司 (瑞典) KELISEC AB (SE)
瑞典

(72)發明人：勒斐爾伊莉絲 REVELL, ELISE (SE)

(74)代理人：李世章；彭國洋

申請實體審查：無 申請專利範圍項數：13 項 圖式數：15 共 67 頁

(54)名稱

產生對稱加密密鑰

GENERATING A SYMMETRIC ENCRYPTION KEY

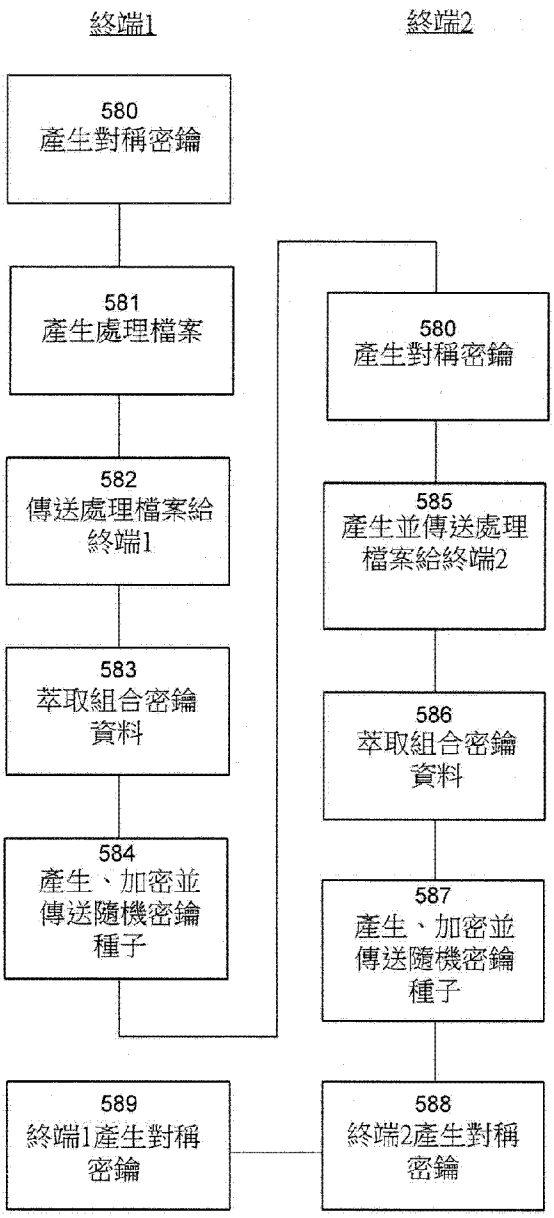
(57)摘要

本案係關於一種用於產生一對稱加密密鑰的系統，該系統包含一第一終端、一第二終端及一伺服器，其中該伺服器經配置以根據用於該第一終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第一終端產生一第一處理檔案；根據用於該第二終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第二終端產生一第二處理檔案；並傳送該第一處理檔案給該第一終端，以及傳送該第二處理檔案給該第二終端；其中該第一終端經配置以接收該第一處理檔案；從該第一處理檔案萃取經組合的密鑰生成資料；產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端；從該第二終端接收一第二隨機密鑰種子；其中該第二終端經配置以接收該第二處理檔案；從該第二處理檔案萃取經組合的密鑰生成資料；產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端；從該第一終端接收該第一隨機密鑰種子；由此該第一終端及該第二終端各經配置以進行下列步驟：將該經組合的密鑰生成資料及該第一隨機種子輸入到一函數中；將該經組合的密鑰生成資料及該第二隨機種子輸入到該相同函數中；以及將該些 函數的結果串連到該對稱加密密鑰中，各終端藉以產生該對稱加密密鑰的各個複本。

A system for generating a symmetric encryption key, said system comprising a first terminal, a second terminal and a server, wherein the server is configured to generate a first processing file for the first terminal based on a combination of key data for the first terminal and key data for the second terminal and the key data for the first terminal; generate a second processing file for the second terminal based on a combination of key data for the first terminal and key data for the second terminal and the key data for the second terminal; and send the first processing file to the first terminal and the second processing file to the second terminal; wherein the first terminal is configured to receive the first processing file; extract the combined key data; generate a first random key seed and send it to the second terminal; receive a second random key seed from the second terminal; wherein the second terminal is configured to receive the second processing file; extract the combined key data; generate the second random key seed and send it to the first terminal; receive the first random key seed from the first terminal; whereby the first terminal and the second terminal are each configured to: input the combined key data and the first random seed into a function; input the combined

key data and the second random seed into the same function; concatenate the results of the functions into the symmetric encryption key, each terminal thereby generating each copy of the symmetric encryption key.

指定代表圖：



第11圖

符號簡單說明：

580・・・產生對稱密鑰

581・・・產生處理檔案

582・・・傳送處理檔案給終端 1

583・・・萃取組合密鑰資料

584・・・產生、加密並傳送隨機密鑰種子

585・・・產生並傳送處理檔案給終端 2

586・・・萃取組合密鑰資料

587・・・產生、加密並傳送隨機密鑰種子

588・・・終端 2 產生對稱密鑰

589・・・終端 1 產生對稱密鑰

201626752
申請案號：104133308
申請日：2015年10月08日
IPC分類：

201626752

【發明摘要】

H04L 9/08 (2006.01)

【中文發明名稱】產生對稱加密密鑰

【英文發明名稱】GENERATING A SYMMETRIC ENCRYPTION KEY

【中文】

本案係關於一種用於產生一對稱加密密鑰的系統，該系統包含一第一終端、一第二終端及一伺服器，其中該伺服器經配置以根據用於該第一終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第一終端產生一第一處理檔案；根據用於該第二終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第二終端產生一第二處理檔案；並傳送該第一處理檔案給該第一終端，以及傳送該第二處理檔案給該第二終端；其中該第一終端經配置以接收該第一處理檔案；從該第一處理檔案萃取經組合的密鑰生成資料；產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端；從該第二終端接收一第二隨機密鑰種子；其中該第二終端經配置以接收該第二處理檔案；從該第二處理檔案萃取經組合的密鑰生成資料；產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端；從該第一終端接收該第一隨機密鑰種子；由此該第一終端及該第二終端各經配置以進行下列步驟：將該經組合的密鑰生成資料及該第一隨機種子輸入到一函數中；將該經組合的密鑰生成資料及該第二隨機種子輸入到該相同函數中；以及將該些

函數的結果串連到該對稱加密密鑰中，各終端藉以產生該對稱加密密鑰的各個複本。

【英文】

A system for generating a symmetric encryption key, said system comprising a first terminal, a second terminal and a server, wherein the server is configured to generate a first processing file for the first terminal based on a combination of key data for the first terminal and key data for the second terminal and the key data for the first terminal; generate a second processing file for the second terminal based on a combination of key data for the first terminal and key data for the second terminal and the key data for the second terminal; and send the first processing file to the first terminal and the second processing file to the second terminal; wherein the first terminal is configured to receive the first processing file; extract the combined key data; generate a first random key seed and send it to the second terminal; receive a second random key seed from the second terminal; wherein the second terminal is configured to receive the second processing file; extract the combined key data; generate the second random key seed and send it to the first terminal; receive the first random key seed from the first terminal; whereby the first terminal and the second terminal are each configured to: input the combined key data and the first random seed into a function; input the combined key data and the second random seed into the same function; concatenate the results of the functions into the symmetric encryption key, each terminal thereby generating each copy of the symmetric encryption key.

【指定代表圖】第（ 11 ）圖。

【代表圖之符號簡單說明】

580 產生對稱密鑰

581 產生處理檔案

582 傳送處理檔案給終端 1

583 萃取組合密鑰資料

584 產生、加密並傳送隨機密鑰種子

585 產生並傳送處理檔案給終端 2

586 萃取組合密鑰資料

587 產生、加密並傳送隨機密鑰種子

588 終端 2 產生對稱密鑰

589 終端 1 產生對稱密鑰

【特徵化學式】

無

【發明說明書】

【中文發明名稱】產生對稱加密密鑰

【英文發明名稱】GENERATING A SYMMETRIC ENCRYPTION KEY

【技術領域】

【0001】 本申請案關於用於改良式保障及安全的系統、方法、設備及電腦可讀取儲存媒體，特定言之乃關於用於建立一安全通訊通道的系統、方法、設備及電腦可讀取儲存媒體。

【先前技術】

【0002】 數位通訊在今日的社會中正逐漸增加，且大部分人們覺得自在地利用網際網路進行像是管理銀行帳戶、申報所得、或者交換其他機密資訊等事務。為了在進行此類事務的同時維持令人滿意的安全層級，已經被提出許多種基於加密的不同安全性解決方案。大部分的此類解決方案牽涉某種公開密鑰（public key）及私人密鑰（private key），而使用者必須在與另一方建立安全通訊前將他的公開密鑰分享出來。在密碼學中，密鑰（key）可被視為一資訊片段，其決定一密碼學演算法的函數輸出。

【0003】 通常被認為在設計安全性系統中假設駭客已經可取得密碼學演算法的細節是明智的。此原則被稱為Kerckhoffs原則，且因此僅有密鑰的機密性才提供了安全性。此原則所依據的事實是，要保密一廣泛使用之演算法的細節是困難的。密鑰通常較容易保護，因為比較起加

密演算法，密鑰往往是一小片資訊。然而，要保密密鑰也可能是困難的。如果駭客以某種方式獲得密鑰，他（她）可能從經加密資料回復原始的訊息。

【0004】 針對加密及解密都用相同密鑰的加密演算法被稱為對稱加密密鑰演算法。也有非對稱加密密鑰演算法，其使用一對密鑰，一個用以加密而一個用以解密。這些非對稱加密密鑰演算法允許在將私人密鑰保留在僅一處的同時公開一密鑰。非對稱加密密鑰經過設計，使得就算已經知道對應的公開密鑰，要找出私人密鑰仍極度困難。使用者在將私人密鑰保密的同時能公開他（她）的公開密鑰，允許任何人傳送給他們經加密的訊息。

【0005】 要讓關聯於對稱加密演算法的密鑰「安全」，通常認為80位元的長度是最小值，廣泛使用且被認為非常強大的是128位元的密鑰。公開密鑰密碼學中使用的密鑰具有某種數學性結構。例如，RSA系統中使用的公開密鑰是二個質數的乘積。因此公開密鑰系統需要比對稱系統更長的密鑰長度，以得到相同的安全性層級。對於根據因數分解及整數離散對數的系統，建議的密鑰長度是3072位元，其目標在於具有等同於一128位元對稱密碼的安全性。

【0006】 如上所提，如果對於根據對稱及非對稱演算法兩者的密鑰而言都足夠長的話，有可能產生具有高度安全性的密鑰。然而，有個問題在於密鑰的分發。如果，例如有兩方想要利用對稱密碼學來通訊，他們首先必須決定要

使用的密鑰，然後安全地從一方將該密鑰分發到另一方。此外，該密鑰必須由雙方保密。侵入者可能找出密鑰的風險隨密鑰被使用的時間增加。因此，正常地一密鑰僅在一有限時間期間有效，例如六或十二個月。經過此時間後必須分發一個新的密鑰。

【0007】 還有，對於非對稱密碼加密的密鑰分發，在兩方想彼此溝通時遭遇到密鑰分發的麻煩。為了雙向地傳送資訊，他們通常需要彼此交換公開密鑰。還有，在此情況中通常該些密鑰有效的時間區間是有限的。對於想與不同的多方通訊的一方來說，有效的公開密鑰的管理及分發可能是擾人的。一個典型的例子是當一密鑰的有效性已經過期時，當你需要緊急地傳送某些秘密資訊給另一方時，或者你還沒有交換公開金鑰時。

【0008】 WO 2011/002412揭露一種用於產生加密/解密密鑰的方法，特別是用於產生用於對稱加密之一次性加密/解密密鑰（也就是相同的密鑰同時被用來加密及解密），提供了一個解決方案。為了開始密鑰的生成，一第一終端(A)向一中央伺服器(2)傳送一請求以設定與一第二終端(B)的通訊。中央伺服器(2)傳送一密鑰產生檔案到兩個終端（也就是終端A及終端B）。各終端產生一個不同的中間資料集合，也就是第一資料集合及第二資料集合。由第一終端(A)產生的第一資料集合被傳送到第二終端(B)，第二終端(B)根據該資料集合來產生一第三資料集合，第三資料集合被傳送回第一終端。在終端(A)中第

一密碼學密鑰的生成是基於在第三及第一中間資料集合之間逐一位元的比較，而第二密碼學密鑰的生成是基於在第一及第二中間資料集合之間逐一位元的比較。第一及第二密碼學密鑰是相同的。

【0009】 雖然這種作法有許多優點，這在被實施在有防火牆或其他類似安全性措施的系統中可能提出挑戰。已知上述的挑戰下，本案發明人理解到需要一種方法能讓雙方彼此以安全的方式通訊而不一定需要事先彼此交換密鑰，且該方法可以被用在採用防火牆或其他類似安全性措施的系統中。

【0010】 因此，需要對加密密鑰有改良式的處理。

【發明內容】

【0011】 本案之教示的一個目的是藉由提供一種用於產生對稱加密密鑰的系統來克服上列的問題，該系統包含一第一終端、一第二終端及一伺服器，其中該伺服器經配置以根據用於該第一終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第一終端產生一第一處理檔案；根據用於該第二終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第二終端產生一第二處理檔案；並傳送該第一處理檔案給該第一終端，以及傳送該第二處理檔案給該第二終端；其中該第一終端經配置以接收該第一處理檔案；從該第一處理檔案萃取經組合的密鑰生成資料；產生一第一隨

機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端；從該第二終端接收一第二隨機密鑰種子；其中該第二終端經配置以接收該第二處理檔案；從該第二處理檔案萃取經組合的密鑰生成資料；產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端；從該第一終端接收該第一隨機密鑰種子；由此該第一終端及該第二終端各經配置以進行下列步驟：將該經組合的密鑰生成資料及該第一隨機種子輸入到一函數中；將該經組合的密鑰生成資料及該第二隨機種子輸入到該相同函數中；以及將該些函數的結果串連到該對稱加密密鑰中，各終端藉以產生該對稱加密密鑰的各個複本。

【0012】 本案之教示的一個目的是藉由提供一種伺服器來克服上列的問題，該伺服器供用於一系統中來產生一對稱加密密鑰，該系統包含一第一終端及一第二終端，該第一終端及該第二終端包含密鑰生成資料，其中該伺服器經配置以進行下列步驟：根據用於該第一終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第一終端產生一第一處理檔案；根據用於該第二終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第二終端產生一第二處理檔案；及傳送該第一處理檔案給該第一終端以及傳送該第二處理檔案給該第二終端。

【0013】 本案之教示的一個目的是藉由提供一種終端來克服上列的問題，該終端用於在一系統中產生一對稱加密密鑰，該系統包含一第二終端及一伺服器，其中該終端經配置以進行下列步驟：接收一第一處理檔案；從該第一處理檔案萃取經組合的密鑰生成資料；產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端；從該第二終端接收一第二隨機密鑰種子；將該經組合的密鑰生成資料及該第一隨機種子輸入到一函數中；將該經組合的密鑰生成資料及該第二隨機種子輸入到該相同函數中；以及將該些函數的結果串連到該對稱加密密鑰中。

【0014】 本案之教示的一個目的也是藉由提供一種用於在一系統中產生對稱加密密鑰的方法來克服上列的問題，該系統包含一第一終端、一第二終端及一伺服器，其中該方法包含下列步驟：該伺服器根據用於該第一終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第一終端產生一第一處理檔案；該伺服器根據用於該第二終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第二終端產生一第二處理檔案；該伺服器傳送該第一處理檔案給該第一終端，以及傳送該第二處理檔案給該第二終端；該第一終端接收該第一處理檔案；該第一終端從該第一處理檔案萃取經組合的密鑰生成資料；該第一終端產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端；該第一

終端從該第二終端接收一第二隨機密鑰種子；該第二終端接收該第二處理檔案；該第二終端從該第二處理檔案萃取經組合的密鑰生成資料；該第二終端產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端；該第二終端從該第一終端接收該第一隨機密鑰種子；該第一終端及該第二終端各自將該經組合的密鑰生成資料及該第一隨機種子輸入到一函數中；該第一終端及該第二終端各自將該經組合的密鑰生成資料及該第二隨機種子輸入到該相同函數中；以及該第一終端及該第二終端都將該些函數的結果串連到該對稱加密密鑰中。

【0015】 本案之教示的一個目的也是藉由提供一種用於在一系統的一伺服器中產生對稱加密密鑰的方法來克服上列的問題，該系統包含一第一終端及一第二終端，其中該方法包含下列步驟：根據用於該第一終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第一終端產生一第一處理檔案；根據用於該第二終端的密鑰生成資料、以及用於該第一終端的密鑰生成資料和用於該第二終端的密鑰生成資料的組合，針對該第二終端產生一第二處理檔案；及傳送該第一處理檔案給該第一終端以及傳送該第二處理檔案給該第二終端。

【0016】 本案之教示的一個目的也是藉由提供一種方法來克服上列的問題，該方法供一系統中的一終端用於產生一對稱加密密鑰，該系統包含一第二終端及一伺服器，

其中該方法包含下列步驟：接收一第一處理檔案；從該第一處理檔案萃取經組合的密鑰生成資料；產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端；從該第二終端接收一第二隨機密鑰種子；將該經組合的密鑰生成資料及該第一隨機種子輸入到一函數中；將該經組合的密鑰生成資料及該第二隨機種子輸入到該相同函數中；以及將該些函數的結果串連到該對稱加密密鑰中。

【0017】 本案之教示的一個目的也是藉由提供一種電腦可讀取儲存媒體來克服上列的問題，該電腦可讀取儲存媒體被編寫有指令，當該等指令在一處理器上執行時進行如上的方法。

【0018】 本案之教示可見於在確保安全連線之系統中的使用，像是金融交易應用程式，但也可見於其中一裝置需要向另一裝置進行驗證的系統中，像是被連接到電腦的外部記憶體。

【0019】 本案揭示之實施例的其他特徵及優點將從以下詳細的揭示內容、隨附申請專利範圍還有圖式中顯現。

【0020】 通常，在申請專利範圍中的全部用語應被按照其在本技術領域中通常的意義來解讀，除非在本說明書中有另外明確定義。對於「一/一個/該[元件、裝置、組件、構件、步驟、其他]」的指稱應被開放地解讀為指稱該元件、裝置、組件、構件、步驟、等等中至少一實例，除非有明確地相反說明。本說明書中揭露之任何方法的步驟並不需要以所揭露的確切順序來進行，除非經明確地說明。

【圖式簡單說明】

【0021】 以下將進一步參照隨附圖式來詳細描述本發明，該些圖式包括：

【0022】 第1圖是按照本案之教示的一終端的示意圖；

【0023】 第2圖是按照本案之教示的一終端的組件的示意圖；

【0024】 第3圖是按照本案之教示的電腦網路的示意概圖；

【0025】 第4圖顯示按照本案教示的實施例之電腦可讀取媒體的示意圖；

【0026】 第5圖顯示按照本案之教示的一方法的流程圖，該方法用於在一系統的第一終端及第二終端之間建立一通訊通道；

【0027】 第6圖顯示按照本案之教示的一方法的流程圖，該方法用於在一系統中安裝一終端；

【0028】 第7圖是是一概略方法的流程圖，該方法用於按照本案之教示來交互驗證一終端及一伺服器；

【0029】 第8圖是在按照本案之教示的交互驗證期間所進行之驗證傳輸的示意概視圖；

【0030】 第9圖顯示按照本案之教示的一實施例，一元資料字串及一相應的驗證符記的例子；

【0031】 第10A圖顯示按照本案之教示產生一驗證符記的概略流程圖；

【0032】 第10B圖顯示按照本案之教示驗證一驗證符記的概略流程圖；

【0033】 第11圖顯示按照本案之教示產生一對稱加密密鑰的方法的流程圖；

【0034】 第12圖是在按照本案之教示的對稱加密密鑰生成期間所進行之傳輸的示意概視圖；

【0035】 第13圖是按照本說明書之一概略方法的流程圖，該方法用於按照本案之教示從用於兩個終端之密鑰資料產生一處理檔案；

【0036】 第14圖是按照本案之教示產生對稱加密密鑰之方式的流程圖；以及

【0037】 第15圖顯示按照本案之教示之系統通訊的示意概視圖。

【實施方式】

【0038】 此後將參照隨附圖式來更完整地說明所揭示的實施例，在圖式中顯示了本發明的某些實施例。然而，本發明可能以不同的形式體現，而不應被解讀為限於本說明書中闡釋的實施例；相反地，這些實施例經提供做為例子，使得本揭示文件詳細而完整，且對本領域之技術人員而言將可完整傳達本發明之範疇。整體文件中相同的數字指稱相同的元件。

【0039】 第1圖顯示按照本案之實施例的一通訊設備100。在一實施例中，通訊設備100經配置用於無線的或有線的網路通訊。在一實施例中，通訊設備100經配置同

時用於無線的及有線的網路通訊。此種通訊設備100的例子為例如：個人電腦（桌上型或膝上型）、網路平板、行動電話、智慧型電話、個人數位助理、伺服器、電子密鑰、機器對機器裝置（M2M）及工作站。

【0040】 此後將以一個人電腦100的方式來例示及描述通訊設備100。個人電腦或終端100包含一顯示器110及一外殼120。該外殼包含一控制器或CPU（未圖示）及一或更多電腦可讀取儲存媒體（未圖示），像是儲存單元及內部記憶體。儲存單元的例子是磁碟機或硬碟機。終端100進一步包含至少一資料埠。資料埠能是有線的及/或無線的。資料埠的例子是USB（通用序列匯流排）埠、乙太網路埠或WiFi（按照IEEE標準802.11）埠。資料埠經配置以使終端100能夠與其他終端或一伺服器連接。

【0041】 終端100進一步包含至少一輸入單元，像是一鍵盤130。輸入單元的其他例子是電腦滑鼠、觸控板、觸控螢幕或搖桿，僅舉出其中幾例。

【0042】 第2圖顯示一計算裝置之概略結構的示意圖。該計算裝置可為如第1圖中的通訊設備，或是一伺服器。在一實施例中該計算裝置是一計算設備，以下將進一步詳細討論。在以下的說明中該計算裝置將以當作按照第1圖中之終端的方式來揭露。終端100包含一控制器210，該控制器負責終端100的整體操作，且該控制器最佳乃藉由任何市面可得之CPU（「中央處理單元」）、DSP（「數位信號處理器」）或任何其他電子可程式化

邏輯裝置來實施。可利用致能硬體功能的指令來實施控制器210，例如藉由在通用或特殊用途處理器中利用可執行電腦程式指令，該些指令可經儲存在一電腦可讀取儲存媒體（磁碟、記憶體等等）240上，以藉由此一處理器執行。控制器210經配置以自記憶體240讀取指令，並執行這些指令以控制終端100的操作。可利用任何用於電腦可讀取記憶體的公知技術來實施記憶體240，像是ROM、RAM、SRAM、DRAM、CMOS、FLASH、DDR、EEPROM記憶體、快閃記憶體、硬碟機、光學儲存器或以上之任意組合。

【0043】 終端100也可經連結至一外部裝置（像是外部記憶體）245，該外部裝置可能的形式是USB（通用序列匯流排）棒或外部硬碟機。在連接這樣的外部裝置到終端之後，馬上成為包含該終端及一外部終端或裝置245的一設備。任何需要實現以致使該外部裝置能與終端100合作的驅動程式更新或下載，可藉由在該控制器中、或是另一未圖示之控制器中所執行的一驅動程式應用程式來進行。

【0044】 終端100進一步包含一或更多應用程式250。該些應用程式是數組指令，當由控制器210執行該些組指令時控制終端100的操作。記憶體240由控制器210用於各種用途，其中一用途乃儲存用於終端100中各種軟體模組的應用程式資料及程式指令250。該些軟體模組包括一實時作業系統、用於人機介面220的驅動程式、

應用程式處理器、以及各種應用程式250。應用程式250能包括傳訊應用程式（像是電子郵件）、瀏覽應用程式、金融交易應用程式，以及各種其他應用程式250。

【0045】 終端100可進一步包含一使用者介面220，該使用者介面在第1圖之終端100中乃包含顯示器110、鍵盤130。顯示器110可為一觸控顯示器，在其上能顯示出及操作虛擬按鍵（未圖示）。此種虛擬按鍵可取代實體按鍵130中之任意者或全部，而在此若無明確指明，則虛擬按鍵及實體按鍵間將無差異。

【0046】 使用者介面（UI）220也包括一或更多硬體控制器，該一或更多硬體控制器連同UI驅動程式與顯示器110、鍵盤130、還有各種其他I/O裝置（像是音效系統、LED指示器、等等）協作。如眾所周知，使用者可通過如此形成的人機介面來操作終端100。

【0047】 終端100可進一步包含一射頻（RF）介面230，該射頻介面經調適以允許該終端通過不同射頻技術的運用，與其他裝置通過射頻頻帶來通訊。此種技術的例子有WIFI、藍牙（Bluetooth®）、W-CDMA、GSM、UTRAN、LTE、NMT，僅舉數例。

【0048】 終端100可進一步包含一有線介面235，該有線介面經調適以允許該終端通過不同網路技術的運用來與其他裝置通訊。此種技術的例子有USB、乙太網路、區域網路、TCP/IP（傳輸控制協定/網際網路協定），僅舉數例。

【0049】 控制器210經配置以利用儲存在記憶體240中的軟體，通過RF介面230及/或有線介面235，來可操作地執行應用程式250（像是網頁瀏覽或email應用程式），該些軟體包括為RF介面230及/或有線介面235提供通訊服務（像是傳輸、網路及連線）的各種模組、協定層疊（protocol stack）、驅動程式等等，以及用於區域性連線的選擇性的藍牙介面及/或IrDA介面。RF介面230包含內部或外部天線，還有合適的無線電電路系統，以供建立及維護往基地台的無線鏈結。如本領域中之技術人員所熟知者，無線電系統包含一系列的類比的及數位的電子組件，該些組件一起形成一無線電收發器。這些組件包括例如帶通濾波器、放大器、混合器、區域振盪器、低通濾波器、AD/DA轉換器、等等。

【0050】 第3圖顯示按照本案之實施例的一電腦網路300的示意概視圖。經由網際網路，二個終端100a、100b（像是第1或2圖之終端100）在一例子中經通過一網路或其他連線330而經連接。該二個終端可通過有線連線或無線連線、或任何已知連接方式的組合來連接，例如通過專屬網路或連線。在第3圖中有二個終端100a及100b，其中一者是桌上型電腦100a而另一者是智慧型手機100b。應注意任何終端可被連接至網際網路，而第3圖中終端100的數目及類型不應被理解為設定限制。電腦網路300進一步包含至少一伺服器340。在第3圖中僅圖示出一伺服器340，但應注意在電腦網路300中可實施任意

數目的伺服器340。通常伺服器是專門執行一或更多服務（作為一代管器）的一實體電腦（硬體系統），用以服務網路300上其他電腦或終端100a、100b的使用者的需要。依照所提供的計算服務而異，該伺服器可能是資料庫伺服器、檔案伺服器、郵件伺服器、列印伺服器、網站伺服器，或其他。

【0051】 在一實施例中伺服器340是一網站伺服器340。通常網站伺服器340可能指協助傳遞內容的硬體（電腦）或軟體（電腦應用程式），該內容能被通過一交互通訊網路（像是網際網路330）來存取。

【0052】 網際網路330是互連電腦網路的全球化系統，其利用標準網際網路協定組（TCP/IP—傳輸控制協定/網際網路協定）來服務全球數十億使用者。其為網路構成的網路，含有數百萬個從區域性到全球性之範疇的私人的、公開的、學術的、商業的、及政府的網路，該些網路藉由電子、無線、及光學網路技術的廣大陣列鏈結起來。網際網路承載廣大範圍的資訊資源及服務，像是全球資訊網（WWW）相互鏈結的超文字文件。

【0053】 如將對一具有技術之讀者將顯而易見者，網際網路對於如何連接二個終端充滿可能性及變異性，而本說明書中揭露的實施例僅為單純例示之目的，不應被解讀為設限。

【0054】 就算本說明書之揭示內容僅聚焦在終端及一伺服器之間的通訊網路，本說明書之教示也可被用在一個

用於在二裝置（像是被連接到一個人電腦的一外部記憶體）之間建立安全連線的設備300之內。參看第3圖，第一裝置100a接著被連接到第二裝置100b。如一技術人員已知者，通訊將建立在一資料匯流排或其他內部通訊網路上。在該些裝置100a及100b中一者（或兩者）中，或是替代地在未圖示的另一裝置（像是設備30的一控制器）中執行的伺服器應用程式，對應至第3圖的伺服器340。參看第2圖，這樣的設備300可被設想成將連接一外部裝置245所至的一終端100。按照本說明書之教示而建立的安全通訊通道可接著由該控制器所實現，該控制器可能通過正由控制器210（或由另一驅動控制器）執行中的伺服器應用程式來當作一伺服器之用。可能該伺服器是一外部安全性伺服器，其經通過一有線或無線通訊通道被接觸，以管理用於該區域匯流排或其他裝置內通訊硬體的通訊交換位址的建立。

【0055】 應注意，在此情境中的外部裝置，可在一實施例中被理解為將被連接至一終端的裝置。其在此後內容可被理解為終端100的一個或多或少永久性（也可能是內建的）組件。

【0056】 第4圖顯示如上內容中所述之電腦可讀取媒體的示意圖。此實施例中的電腦可讀取媒體40是一資料碟片40。在一實施例中，資料碟片40是一磁性資料儲存碟片。資料碟片40經配置以承載指令41，當指令41被載入到控制器（像是處理器）中時執行按照以上描述之實施

例的一方法或程序。資料碟片40經安排以被連接至一讀取裝置42或是經安排在讀取裝置42內，並由讀取裝置42讀取以將指令載入到該控制器中。此種讀取裝置42與一個（或數個）資料碟片40之結合的一例是硬碟機。應注意，電腦可讀取媒體也能是其他媒體，像是光碟、數位影音光碟、快閃記憶體或常見使用的其他記憶體技術。在這樣的實施例中資料碟片40是一種有形電腦可讀取媒體40。

【0057】 指令41也可被下載到一電腦資料讀取裝置44（像是能夠讀取在一電腦可讀取媒體上之電腦編寫資料的電腦或其他裝置）中，該下載動作是藉由將指令41包含在一電腦可讀取信號43中，該電腦可讀取信號經由無線（或有線）介面（例如經由網際網路）被傳輸給電腦資料讀取裝置44，以供載入指令41到一控制器中。在此一實施例中，電腦可讀取信號43是一種非有形電腦可讀取媒體40。

【0058】 該些指令可經儲存在電腦44的一記憶體中（在第4圖中未明確示出，但在第2圖中以240參照）。

【0059】 對於電腦程式、指令、代碼等等的參照應被理解為涵蓋用於可程式化處理器或韌體的軟體，像是(例如)一硬體裝置的可程式化內容，用於處理器的指令，或是用於一固定功能裝置、閘陣列、或可程式化邏輯裝置等等的組態設定。

【0060】本案發明人已理解到，類似於WO 2011/002412之作法如果經以聰明且有見地的方式來修改的話，也可被用在使用了像是防火牆之安全性措施的系統中。第5圖顯示這樣一種用於在二個終端之間建立一交互安全連線之方式的概要。

【0061】第5圖顯示按照本案之教示，在如第3圖之系統300中的第一終端100a及第二終端100b之間建立通訊通道之方法的流程圖。

【0062】在連線建立之前，針對相關的應用，一終端(像是第3圖的第一終端100a及/或第二終端100b中之一)經安裝或起始（510）在通訊網路300中。此一應用可能是金融交易應用、安全通訊應用、或需要識別出在通訊中之雙方的任何其他應用。在一實施例中，此一應用是當一裝置將被連接到一設備的另一裝置時。

【0063】此安裝步驟的進行是由一終端100傳送欲被安裝的請求到一伺服器340。伺服器340送回有關密鑰生成的資訊或資料給終端100作為回應，終端100接收該密鑰生成資料。此種密鑰生成資料因此被分發（515）。

【0064】將參照第6圖以提供更多有關將終端100安裝到系統300中的細節。

【0065】當已安裝了第一終端100a時，其可能希望與另一終端100b設立安全通訊。

【0066】在其中整體的應用是金融交易應用的一範例實施例中，第一終端100a代表客戶端而第二終端100b

代表銀行。伺服器340可由一互助銀行公司、該銀行本身或一安全連線提供者所管理。

【0067】 為了設立這樣的安全連線，第一終端100a藉由傳送一第一對話請求（520）到伺服器340來起始該設立步驟。該第一對話請求包括用於第二終端100b（該第一終端想要與其設立通訊）的一識別符。用於通道資料的識別符在一實施例中可能是對一網際網路協定通訊通道的一位址（像是一致資源定位位址(URL)或網際網路協定(IP)位址）。

【0068】 伺服器340起始或建立一對話通道（530）並以一第一對話回應來回應（535），由第一終端100a所接收的該第一對話回應指示了用於該對話通道的一識別符以及用於第二終端100b的密鑰資料。第一終端100a接著傳送一第二對話請求到第二終端100b。該第二對話請求包括第一終端100a的識別及用於第一終端100a的一密鑰加密種子。

【0069】 隨著第二終端100b接收來自第一終端100a的該第二對話請求，第二終端100b傳送一第三對話請求（550）給伺服器340。該第三對話請求包括用於第一終端100a的一識別符及/或用於目前對話的一識別符。伺服器340決定是否第一終端100a被允許與第二終端100b連接，如果是則傳送一第二對話回應（560）給第二終端100b，其中該第二對話回應包括用於該對話通道的識別符以及有關第一終端100a之密鑰產生的資料。

【0070】 隨著第二終端100b接收該第二對話回應，第二終端100b可確定該第一終端被允許與第二終端100b建立連線。第二終端100b此後傳送一第三對話回應（570）至第一終端100a，該第三對話回應包括密鑰資料及用於終端100b的一密鑰加密種子。

【0071】 第二終端100b及第一終端100a因此兩者都已從伺服器340接收到密鑰資料以及對方的密鑰加密種子。據此，該第一終端及該第二終端產生（580）用於加密資料的一對稱加密密鑰，該對稱加密密鑰將在經起始之對話通道上傳送而藉以建立（590）一通道。

【0072】 有關如何產生該對稱加密密鑰的細節將參看第12、13及14圖來提供。

【0073】 產生此一對稱加密密鑰的替代方式可在WO 2011/002412之教示中找到。

【0074】 以這種方式，由於兩終端都已由伺服器340所驗證，第一終端100a及第二終端100b兩者都能確定另一終端的身分及可信度。該些終端也經致使能產生一對稱加密密鑰，而無須彼此交換完整的密鑰，也無須與伺服器340交換完整的密鑰（像是對稱密鑰）。

【0075】 此外，由兩個終端100a及100b驗證了該伺服器。在先前技術的例子中只有伺服器驗證終端，而不像本案之教示般由終端驗證伺服器。

【0076】 此種交互驗證的更多細節將參照第6及7圖於**交互驗證**一節底下提供。

【0077】 應注意安全通訊通道的整體設定乃由來自一終端的主動提示所進行，對該些主動提示提供了一回應，以致使該通訊系統設定被用在採用安全性措施(像是防火牆）的系統中。

終端的安裝

【0078】 為了確保將被安裝在系統300中的一終端可被信任，以及為了確保任何在該終端及該伺服器之間傳送的安裝資料不會被第三方濫用，本申請案之作者設計出一種方式來用於安全的安裝，其中密鑰資料不會完整的被傳送，藉此使該密鑰資料對於偵聽通訊的任何第三方而言是無用的。第6圖顯示按照本案之教示之一概略方法的流程圖，該方法用於在如第3圖中之系統300中安裝一終端100。

【0079】 由於一終端100將被安裝在該系統中(像是在第5圖中參考符號510所指的安裝一終端時），該伺服器設立用於終端100的一帳號，該設立動作是藉由產生一隨機識別碼NodeID（511）及產生一隨機加密密鑰Y（512）。

【0080】 該隨機識別碼及該隨機加密密鑰接著以安全的方式被分發到要被安裝的終端100。可藉由普通郵件、email、文字訊息（像是簡訊服務(SMS)傳訊），或其他安全通道來分發該隨機識別碼及該隨機加密密鑰。

【0081】 該隨機識別碼及該隨機加密密鑰被輸入（513）到終端100中，該輸入動作可能是由一使用者、

或由（另一）安全應用程式可能地通過屬於該隨機識別碼及該隨機加密密鑰的一檢查總和的使用而進行，該隨機識別碼及該隨機加密密鑰將被檢查看是否其為正確的。

【0082】 終端100接著通過該隨機識別符（NodeID）來向伺服器300識別（514）自身，且因此由伺服器340所識別。

【0083】 該伺服器接著產生二個隨機加密密鑰種子、一密鑰資料種子及一元資料種子，統稱為資料種子。

【0084】 該密鑰資料種子可具有長度為例如128或256位元。該元資料種子可具有的長度為例如128或256位元。

【0085】 利用這些種子，該伺服器產生密鑰資料及元資料。該密鑰資料是被用來產生對稱加密密鑰的資料，而該元資料被用來在與該密鑰資料一起或沒有該密鑰資料之下產生一驗證符記（以下將進一步描述）。

【0086】 該密鑰資料所具長度可為128、256、512或1024位元。該元資料所具長度可為8192位元。

【0087】 為了保護而免遭竊聽，伺服器340僅分發（515）該產生密鑰之種子到終端100，也就是說僅該密鑰資料種子及該元資料種子被分發到終端100。這樣確保了真正的密鑰資料及元資料被保密在伺服器340中。

【0088】 在該密鑰資料及該元資料被分發到終端100前，利用該隨機加密密鑰來加密該密鑰資料及該元資料。

而終端100利用該隨機加密密鑰來解密該密鑰資料及該元資料。

【0089】 終端100接著藉由利用伺服器340所用的相同函數來產生該密鑰資料及該元資料。該函數可連同該隨機識別符及該隨機加密密鑰被分發，或者該函數可被獨立地分發，其中該隨機識別符及/或該隨機加密密鑰是該函數的參數，及/或該函數可經實施在該終端及/或伺服器中。在一實施例中該函數是一密碼學雜湊函數，像是Feistel網路。

【0090】 已知有數種用於產生數字的函數，而在本說明書中將不進一步詳細討論。對該函數而言唯一具重要性的特點在於終端100使用伺服器340所用的相同函數。

【0091】 該些種子因為比所要產生的相應資料小得多，因此伺服器340僅需傳送較小的種子到該終端，如此節省了頻寬也增加了安全性，因為種子在沒有函數的情況下是無價值的。

【0092】 由伺服器340及終端100兩者如此產生（516）該密鑰資料及該元資料。

【0093】 終端100根據該密鑰資料及/或該元資料而產生（517）一驗證符記，而該驗證符記被傳送到伺服器340，伺服器340驗證（518）該驗證符記，該伺服器可取得該驗證符記所根據的該密鑰資料及該元資料。

【0094】 有關如何產生及驗證一驗證符記的更多細節將在以下參照第10A及10B圖而提供。

【0095】 如果驗證了該驗證符記，則用於終端100的一身分（像是一識別）被儲存在伺服器340中。在一實施例中，用於終端100的識別是NodeID。在一實施例中，用於終端100的識別是IMSI（國際行動訂戶識別）、IMEI（國際行動裝備識別符）及/或終端100的序號。在一實施例中，用於終端100的識別是一應用程式識別符，其係與運用如本說明書所教示之安全通訊通道的應用程式一起提供。

【0096】 對於其中終端是一外部裝置的實施例來說，用於該外部裝置的NodeID可連同該外部裝置一起供應，或者該外部裝置的NodeID可在登錄該外部裝置245之後即被傳送給使用者或給該外部裝置。

交互驗證

【0097】 隨著終端100a已被安裝而嘗試與第二終端100b（像是金融交易應用程式伺服器）設立一通訊通道，其中該通訊通道是由安全性伺服器340所主控，可能是相同銀行伺服器之部分或是被實施在相同銀行伺服器中，終端100a將由安全性伺服器340（此後將如上稱為伺服器340）所驗證。在伺服器340驗證終端100a之後，伺服器340被提供以用來建立與第二終端100b之安全通訊的必要的密鑰資料。

【0098】 然而，現今的社會中網際網路上流通許多詐騙，正因此我們需要安全通訊通道。然而，發明人已察覺全部此類安全通訊系統本質上有一根本的問題，在於：利

用今日進步的技術，連第一終端100a（還有第二終端100b）都無法確定伺服器340是真正可以信任的。伺服器340的位址其實可能已經被惡意的詐騙操縱者所挾制，該詐騙操縱者可能提供的密鑰資料導向一個該詐騙操縱者可在之後解密的加密結果。

【0099】 瞭解到這個問題的存在，而通過有見地的歸因與創造性的思考，本案發明人設計出一種做法，其中伺服器340也經過驗證。

【0100】 對於在一設備300（像是終端100）中安裝一外部裝置245的實施例，這樣的驗證用以保護使敏感性資料不被屬於設備300或是後來被連接至設備300的另一裝置、或是被一經替換之作業軟體所讀取。因此交互驗證用以保護免於簡單地藉由取代某些組件（帶有軟體碼的記憶體）或其他裝置而得到對一受保護裝置之存取。

【0101】 第7圖是用以按照本案之教示來交互驗證終端100及伺服器340之概略方法的流程圖，而第8圖是在此種交互驗證所進行之驗證傳輸的示意概視圖。此種驗證的詳細說明將在以下同時參照第7及8圖來提供。

【0102】 第一終端100a藉由產生一驗證符記AT 1-S（此參考符號顯示出其為從終端1到伺服器S的驗證符記），及可能連同一對話請求來傳送（710）該驗證符記到伺服器340，以起始該驗證。或者，在已成功地完成該驗證後傳送該對話請求。應注意終端100a、100b中任意者可起始驗證動作。伺服器340也可起始驗證動作。該伺

服器可藉由提示第一終端100a（或第二終端）去提供一驗證符記以起始驗證動作。

【0103】 伺服器340接收驗證符記AT 1-S並予以驗證（715）。

【0104】 該驗證符記可為用於該終端的一識別符(像是NodeID），其可能經用先前所接收之隨機加密數字所加密，該隨機加密數字僅被第一終端100a及伺服器340所知。該驗證符記也可是僅被伺服器340及終端100a所知的另一字串或數字，該字串或數字可能通過一已知協定或演算法所決定，且也可經該隨機加密數字所加密。

【0105】 由於能確保驗證是安全的，使用一個大型字串是有益的，因為其更難以猜測。這樣的字串是僅被伺服器340及終端100所知的元資料。這有一個問題在於每次要進行驗證時必須傳送一個大檔案，以及如以下將揭露的，該元資料將也與該第二終端共享，因此洩露了該元資料給該第二終端，而後者不應該得知用於第一終端100a的元資料。然而，利用元資料是有益處的，因為其是難以惡意地推導出的大型字串，也僅為伺服器340及終端100所知。

【0106】 發明人因此已設計出聰明且簡單的作法來從該元資料制定出驗證符記，其中從該元資料隨機地選擇複數個區塊或部分。

驗證符記

【0107】 第9圖顯示一元資料字串MTS及一相應的驗證符記AT的例子。在第9圖的例子中，該元資料字串包含了僅40個字母，然而應注意一元資料字串MTS的確切長度較佳地為更長。在一實施例中其長度是8192位元。此外，此例中該些部分的個數是四個且各部分的長度是2，但在真實的實施例中一部分的長度應為64～128位元，而在一實施例中該部分長度是96位元。應注意在一驗證符記內一部分的長度也可有差異，該些部分的個數也是如此。在該些部分的個數有差異的實施例中，該驗證符記的標頭可被用來指示出該些部分的個數。在一或更多部分的長度有差異的實施例中，該驗證符記的標頭可被用來指示出該些部分的長度，或者各部分可由該個部分的長度做起始。

【0108】 該等四個部分由指數（index）來參照。可隨機選擇該些指數，或者通過一已知函數（像是隨機數產生器），例如使用一種子。在以上有關如何在系統中安裝終端的揭示內容中已提供了此種函數的例子。

【0109】 在使用一種子供一函數產生指數的實施例中，只有種子是必要在該驗證符記中傳輸的。

【0110】 一指數應該具備的長度要足以正確地定址較大的資料集合，也就是元資料字串（MTS）。對於8192位元的元資料，指數必須有13位元的長度。也可用距離下一部分的步數來指定指數，其中該指數長度能被減少一位元，假設下一部分至少在該元資料的下半之內。

【0111】 該些指數或該種子可被提供在該驗證符記的標頭中。該些指數也可被當作各部分的標頭來提供。第9圖顯示此種驗證符記的三個例子，其中有一種子被提供在標頭中，有四個指數被提供在標頭中，以及有四個指數被提供為各部分的標頭。在這全部三個例子中，該種子是24，而該些指數是3、7、13及16，而其相應部分分別是「as」、「or」、「lp」及「it」。

【0112】 應注意，同上所述，該些範例指數及部分長度還有元資料字串MTS的長度被造的短，以更容易闡釋本案之教示。

【0113】 藉著僅傳送元資料的部分，確保了可在不浪費頻寬也不洩露敏感資料之下驗證終端100及伺服器340，因為僅有元資料的部分被傳輸。

【0114】 一驗證符記AT可接著藉由僅比較該些部分與元資料中的相應部分而經驗證。該些相應部分通過指數被擷取，該些指數不是當作該驗證符記的部分被接收，就是以屬於該驗證符記之該種子的一函數被擷取。

【0115】 該些指數也可根據一計時函數來提供，計時函數像是一天中的時間或計數器。必須在產生、傳送及接收驗證符記的時間期間遞增該計數器。

【0116】 第10A圖顯示用於按照本案之教示產生驗證符記的概略流程圖，而第10B圖顯示用於按照本案之教示辨別一驗證符記真偽的概略流程圖。

【0117】 驗證符記AT的產生是藉由產生至少一個指數（1010）。如以上討論，在一實施例內指數的個數可有變化，也可能在實施例之間有所變化。在一實施例中指數的個數是4。

【0118】 該些指數可經產生為隨機地選擇的數字，或者通過一隨機地選擇的種子以一函數來使用。

【0119】 此後至少一個部分被擷取（1020）自一較大資料集合，像是元資料（第9圖中的MTS），並連同該些指數（或該種子）經封裝在如第9圖中所示的一資料結構中（1030）。

【0120】 隨著接收（1040）到一驗證符記，該些指數被擷取（1050）（不是從該驗證符記，就是藉由利用基於一種子的一函數），且從一本地儲存的資料集合（像是元資料）擷取該（該等）相應部分（1060）。該（該等）相應部分接著被與該（該等）被接收部分做比較（1080），如果相符則該驗證符記經驗證為真。

【0121】 此比較動作可按位元進行，或者藉由任何其他已知的比較方式。按位元比較方式的優點在於執行快速。

【0122】 如果一指數被選擇離資料集合的結尾太近，而使得沒有剩下足夠的字元或位元來完成一部分，則進一步的或缺少的字元或位元可從該資料集合的開頭來取得，也就是說該資料集合是環形的。

【0123】 以上對於包含字元的資料集合及包含位元的資料集合並沒做出差別。如技術人士所將理解者，可在本案教示之範疇內輕易地替換此類實體。

【0124】 對於8192位元、有各具96位元之四個部分或區塊的元資料集合而言，驗證符記有4x96+4x13（一指數需要有至少13位元，以正確地定址8192位元）=436位元。所以，傳送僅只該驗證符記不只比傳送元資料更安全（因為該元資料被保密），且所需頻寬也減少了大約95 %。

【0125】 在一實施例中，該指數經選擇以使能定址超過該元資料，且接著藉由在該指數除以該元資料大小的餘數（該指數 mod 該元資料大小）處定址該元資料能輕易地找到該等相應部分。在元資料有8192位元的本例中，要擷取一部分的位址因此是在指數除以8192的餘數處。

【0126】 從以上說明可明顯知道，可藉由終端及伺服器兩者產生及驗證一驗證符記。事實上，驗證符記可由任何計算裝置產生，第1及2圖的終端以及第3圖的伺服器就是此種計算裝置的例子。外部裝置也可以是此種計算裝置。

【0127】 回到第7及8圖及交互驗證，隨著伺服器340已經驗證從第一終端100a所接收的驗證符記AT 1-S，該伺服器產生（720）一個針對第一終端100a的驗證符記ATS-1，以及一個針對第二終端100b的驗證符記ATS-2，並傳送（725）該等兩個驗證符記ATS-1、ATS-2給第一終端100a。

【0128】 在一實施例中，伺服器340將針對第二終端100b的驗證符記AT S-2加密。加密該驗證符記可利用用於第二終端100b之元資料的一部分，而在這樣的實施例中，該驗證符記可經配置以包含多一欄位，該欄位指示一加密指數，該加密指數只是了在元資料的何處可以找到用於加密該驗證符記的加密密鑰。因此該加密指數是在未加密之下被傳輸。如此避免任何惡意的攻擊者偽裝成第二終端100b去解密驗證符記AT S-2。

【0129】 隨著第一終端100a接收（730）該等二個驗證符記AT S-1及AT S-2，第一終端100a驗證（735）從伺服器340所接收的第一驗證符記AT S-1。

【0130】 由於第一終端100a無法取得第二終端100b的元資料，第一終端100a無法驗證從伺服器340接收的第二驗證符記AT S-2。然而，藉由伺服器340傳送目標是第二終端100b的驗證符記給第一終端100a，則通過第二終端100b達成了對伺服器340的額外驗證。

【0131】 如果對於從伺服器340接收的第一驗證符記AT S-1驗證成功，則第一終端100b繼續進行由第二終端100b實施的額外驗證。在這方面，該第一終端傳送（740）從伺服器340接收的第二驗證符記AT S-2給第二終端100b。第二終端100b接收並驗證（745）驗證符記AT S-2。如果驗證成功，則已經通過第一終端100a及第二終端100b兩者驗證了伺服器340。如此已經達成高度安全性的交互驗證。

【0132】 然而，由於理解到若惡意的詐騙操縱者已經能挾制第一終端100a及伺服器340之間的通訊通道，則針對第二終端2的驗證符記也可能被洩露。為了更進一步增加驗證的安全性，第二終端100b較佳地經配置也去驗證伺服器340。

【0133】 隨著第二終端100b已經驗證了從伺服器340通過第一終端100a所接收、且針對第二終端100b的驗證符記AT S-2，該第二終端繼續利用其對伺服器340的自有通訊通道來驗證伺服器340。

【0134】 該第二終端因此產生用於伺服器340的一驗證符記AT 2-S，並傳送（750）該驗證符記給伺服器340。伺服器340接收驗證符記AT 2-S並予以驗證（755）。如果驗證成功，則第二終端100b被伺服器340所驗證，且伺服器340產生（760）一個針對第一終端100a的驗證符記AT S-1以及一個針對第二終端100b的驗證符記AT S-2，並傳送（765）驗證符記AT S-1、AT S-2兩者至第二終端100b。

【0135】 隨著第二終端100b接收（770）二個驗證符記AT S-1及AT S-2，第二終端100b驗證從伺服器340接收的第二驗證符記AT S-2，如果成功則傳送（775）第二驗證符記AT S-1至第一終端100a，第一終端100a驗證（780）其從伺服器340通過第二終端100b所接收、並針對第一終端100a自身的驗證符記AT S-1。

【0136】 伺服器340不只是因此被第一終端100a所驗證，伺服器340也被第二終端100b代表第一終端100a所驗證。該二個終端因此彼此協助以驗證伺服器340。此外，由第一終端100通過從伺服器340經由第二終端100b所接收的該些驗證符記，第一終端100隱含地驗證了第二終端100b。另外，伺服器340被利用二個不同的通訊通道所驗證，藉以使得詐騙操縱者難以惡意地將自身識別為安全性伺服器340。

對稱加密密鑰的生成

【0137】 隨著二個終端100及伺服器340已被驗證，一個對稱加密密鑰被產生。參看第5圖，一終端100當被安裝時接收（515）密鑰生成資料，且該終端根據該密鑰生成資料產生（516）密鑰資料。該密鑰資料將被用來產生以下將揭露的對稱加密密鑰。該對稱加密密鑰將被用於第一終端100a及第二終端100b之間通訊的加密。第一終端100a可能是（如上所述）安全服務的客戶端，而第二終端100b可能是該服務的提供者。

【0138】 替代地，第一終端100a可為要被連接至一設備300的一外部裝置245，其中第二終端100b代表設備300。

【0139】 被產生的密鑰資料僅為第一終端100a及伺服器340所知，而第二終端100b不知道此密鑰資料。如此致使了增加的安全性，因為所要建立的通訊連線在沒有交

換個別終端之密鑰資料之下建立起來，使得惡意的詐騙操縱者難以截聽任何密鑰資料。

【0140】 為此目的，發明人已設計出簡單而聰明的方式來從個別終端之密鑰資料製造對稱加密密鑰，無須真正地分享密鑰資料。

【0141】 第11圖顯示產生這樣的對稱加密密鑰之方法流程圖，而第12圖是在按照本案之教示生成對稱加密密鑰期間所完成之傳輸的示意概視圖。

【0142】 第一終端100a從傳送針對所要產生（580）之對稱加密密鑰的一請求開始。該請求可按照第5圖般作為一對話設立請求的部分被傳送，或者該請求可自己被傳送。該請求也可隱含在先前請求中。伺服器340接著繼續產生（581）一第一處理檔案PF1，該第一處理檔案被傳回（582）到第一終端100a。

【0143】 第一終端100a接著從第一處理檔案PF1萃取（583）一組合密鑰資料。第一終端100a接著產生一第一隨機密鑰種子，該第一隨機密鑰種子被加密並被傳送（584）給該第二終端。第二終端100b也向伺服器340傳送（580）針對產生一對稱加密密鑰的一請求，而伺服器340產生並傳送（585）一第二處理檔案PF2給第二終端100b。

【0144】 第二終端100b接著從第二處理檔案PF2萃取（586）該組合密鑰資料，並產生一第二隨機密鑰種子，該第二隨機密鑰種子被傳送（587）給第一終端100a。

第一及第二終端100兩者都各自接著產生（588、589）對稱加密密鑰。

【0145】 第13圖是按照本說明書用於從用於二個終端之密鑰資料產生一處理檔案PF之概略方法的流程圖。用於第一終端的密鑰資料將稱為KD1，而用於第二終端的密鑰資料將稱為KD2。

【0146】 由於將要產生（581）一處理檔案，在各終端的密鑰資料上進行按位元AND運算而產生（5811）一組合密鑰資料（稱為CKD），也就是：

CKD = KD1 AND KD2

【0147】 接著產生（5812）針對相應終端之密鑰資料的相反數，也就是產生~KD，且~KD經過（5813）一函數F，其中以例如是10%、25%、50%的機率，或者是在10～80%、20～70%、或25～50%之範圍中任意者的機率，各個是1的位元被改成是0的位元。所產生經改變的位元字串可被稱為F(~KD)。在該組合密鑰資料及該所產生經改變的位元字串的邏輯OR就產生（5814）了該處理檔案。也就是說：

PF1 = CKD OR F(~KD1) = (KD1 AND KD2) OR F(~KD1)，以及

PF2 = CKD OR F(~KD2) = (KD1 AND KD2) OR F(~KD2)

【0148】 被產生的處理檔案PF因此與密鑰資料完全不同，也完全不同於該組合密鑰資料，而因此對應的密鑰資

料對另一終端保密，而組合密鑰資料及對應的密鑰資料兩者都對外界保密。

【0149】 隨著該處理檔案已被接收，則萃取（第11圖中的583/586）該組合密鑰資料，該萃取步驟僅簡單地在該處理檔案及該相應終端的密鑰資料上進行邏輯或按位元AND，也就是：

CKD = PF1 AND KD1，及

CKD = PF2 AND KD2

【0150】 為了例示以上內容，以下提出一例。應注意此例為闡釋之目的而被限制在8位元，而在真實生活的實施例中應使用更長的字串，例如128位元、256、512、1024位元，因為較多位元提供較高的安全性。

範例

KD1 10001110

KD2 01111101

CKD = KD1 AND KD2 00001100

~KD1 01110001

F(~KD1) 01010000

PF1 = CKD OR F(~KD1) 01011100

萃取結果

CKD = PF1 AND KD1 00001100

【0151】 隨著已經萃取了該組合密鑰資料，同時在傳輸期間保持其安全地隱藏在該處理檔案中，而將產生該對稱

加密密鑰。第14圖是用於按照本案之教示產生該對稱加密密鑰之範例方式的流程圖。

【0152】該對稱加密密鑰最終由兩終端100產生（588/589），該產生步驟係藉由針對各終端100在一函數（像是密碼學雜湊函數或互斥或函數(XOR)）（5801）中輸入該組合密鑰資料及先前針對各終端產生（第一終端在584，第二終端在587）而當作一函數中之種子的一隨機密鑰種子。在一實施例中，該函數將重複該隨機密鑰種子8次而成為具有例如512位元的加長隨機密鑰種子，並在該組合密鑰資料及該加長隨機密鑰種子上進行互斥OR函數。可能利用一modulo函數而從該經XOR之數值取得128位元的半個對稱密鑰。此步驟乃由先前已接收到另一終端之隨機密鑰種子的兩終端100來進行。在一實施例中，結果是用於各終端而具例如128位元的位元字串，而該等二個位元字串經串連（5802）成為藉以產生的對稱加密密鑰。

【0153】該對稱加密密鑰是對話設立的結果，且該對稱加密密鑰將被使用在第一終端100a及第二終端100b之通訊期間，以用於編碼及解碼該通訊。

【0154】應注意，儘管已將對於交互驗證及對於產生該對稱加密密鑰的流程揭露為個別流程，但它們可屬於相同的流程且在任一流程之傳輸中傳送的資料可被組合成唯一共同的傳輸，以減少頻寬並平行化驗證的流程。

密鑰資料的變異

【0155】 為了保護免於惡意的攻擊者企圖挾制密鑰資料或其他加密資料，本案發明人提出一種簡單的解決方式是使該密鑰資料變異或改變該密鑰資料。應注意，元資料、密鑰資料及對稱加密密鑰可全部被個別地變異或一起變異。

【0156】 在一實施例中，該元資料一天被變異一次，因為其主要用於驗證目的。

【0157】 在一實施例中，該密鑰資料在每次對話設立時被變異，或者在一對話期間每時間間隔處被變異或是當有來自第一終端的提示時被變異。

【0158】 在一實施例中，該對稱加密密鑰在一對話期間每一時間間隔被變異或是當有來自第一終端的提示時被變異。

【0159】 變異該對稱加密密鑰的一個方式是建立一個新的對話。在該對話設立期間將變異該密鑰資料，因此該對稱加密密鑰也經變異。然而，此同時耗費了電腦資源還有時間來進行完整的對話設立。一種更快的方式是僅變異該對稱加密密鑰。此僅於該些終端處進行；未涉及該伺服器。

【0160】 何時進行變異動作要由安全應用程式來決定。例如在聊天應用程式中，可能針對各個要被傳送至另一終端的訊息來變異該對稱加密密鑰是適當的。在時間緊迫的應用程式中，可能在（例如）每十次封包就進行變異是較佳的，或甚至完全不進行。

【0161】 是否一個新的封包應該具有經變異的對稱加密密鑰，要由起始的終端（傳送者）來控制。此藉由對各個通訊封包加入一版本號碼（也就是對稱加密密鑰版本）來完成。若起始的終端希望利用此特性，則它必須對每個傳送的封包增加該變數。

【0162】 在伺服器設定時，該對稱加密密鑰版本初始被設為0。如果該傳送者從未改變此數值，則將不會發生變異。相反地，如果傳送者（例如）在頭四個封包使用3、7、13、14等數值，則回應的終端需要針對對應的封包變異3、4、6、1次。

【0163】 接收的第一終端永遠檢查其接收之各通訊封包的版本數。如果已經改變，則該接收終端必須在解密該訊息之前據以變異該對稱加密密鑰。如果該數值大於先前的封包，則它就變異適當的次數。如果該數值較小，則它必須利用具有對稱加密密鑰版本 = 0的對稱加密密鑰並從頭重新開始。

【0164】 對稱加密密鑰的變異可利用512位元的密碼學雜湊函數並利用現有對稱加密密鑰作為輸入來完成。

系統概要

【0165】 第15圖顯示按照本案之教示之系統通訊的示意概視圖。第15圖中的系統300可為如上描述的系統300或設備300。

【0166】 第一終端100a起始與伺服器340及第二終端100b之間的設定，該第二終端100b是一回應終端，如以

上參照第5、6、7、8、9、10A、10B、11、12、13及14圖所揭露。

【0167】 隨著已經產生對稱加密密鑰，第一終端100a及第二終端100b能在所建立的通訊通道上安全地溝通。

【0168】 本案之教示的一個益處在於可由通訊中終端兩者產生一對稱加密密鑰，而無須在終端或其他裝置之間分享該對稱加密密鑰。

【0169】 以上已主要參照一些實施例說明本發明。然而如本領域之技術人士所容易理解的，除以上所揭露以外的其他實施例同樣可能在本發明之範疇內，本發明之範疇係由隨附申請專利範圍所界定。

【符號說明】

【0170】

100 通訊設備、終端

100a 第一終端

100b 第二終端

110 顯示器

120 外殼

130 鍵盤

210 控制器

220 人機介面（使用者介面）

230 射頻（RF）介面

235 有線介面

240 電腦可讀取儲存媒體/記憶體

245 外部裝置

250 應用程式

300 系統、設備、網路

330 網路

340 伺服器

40 電腦可讀取媒體/資料碟片

41 指令

42 讀取裝置

43 電腦可讀取信號

44 電腦資料讀取裝置/電腦

510 安裝終端

511 產生NodeID

512 產生隨機加密密鑰

513 分發給終端並輸入到終端中

514 在伺服器識別終端

515 分發密鑰生成資料

516 產生密鑰資料及元資料

517 產生並傳送驗證符記

518 驗證驗證符記

519 儲存終端及密鑰資料及元資料

520 傳送第一對話請求給伺服器

530 起始對話通道

535 傳送第一對話回應給第一終端

540 傳送第二對話請求給第二終端

550 傳送第三對話請求給伺服器

560 傳送第二對話回應給第二終端

570 傳送第三對話回應給第一終端

580 產生對稱密鑰

5801 針對各終端在密碼學雜湊函數中輸入組合密鑰資料及隨機密鑰種子

5802 串連產生的位元字串成為對稱密鑰

581 產生處理檔案

5811 產生組合密鑰資料

5812 產生密鑰資料的相反數

5813 經過位元改變函數

5814 產生組合密鑰資料及經位元改變之密鑰資料的相反數的邏輯OR

582 傳送處理檔案給終端1

583 萃取組合密鑰資料

584 產生、加密並傳送隨機密鑰種子

585 產生並傳送處理檔案給終端2

586 萃取組合密鑰資料

587 產生、加密並傳送隨機密鑰種子

588 終端2產生對稱密鑰

589 終端1產生對稱密鑰

590 建立通訊通道

710 產生並傳送驗證符記

715 接收並驗證驗證符記

720 產生用於終端1及終端2的驗證符記

725 傳送驗證符記給終端1

730 接收二個驗證符記

735 驗證用於終端1的驗證符記

740 傳送用於終端2的驗證符記給終端2

745 接收並驗證驗證符記

750 產生並傳送驗證符記

755 接收並驗證驗證符記

760 產生用於終端1及終端2的驗證符記

765 傳送驗證符記給終端2

770 驗證用於終端2的驗證符記

775 傳送用於終端1的驗證符記給終端1

780 接收並驗證驗證符記

1010 產生指數

1020 擷取部分

1030 附加指數及部分

1040 接收驗證符記

1050 擷取指數

1070 擷取相應的部分

1080 比較相應的部分及部分

AT 1-S、AT S-1、AT 2-S、AT S-2 驗證符記

PF1 第一處理檔案

PF2 第二處理檔案

MTS 元資料字串

ＡＴ１、ＡＴ２、ＡＴ３ 驗證符記

【生物材料寄存】

【０１７１】 國內寄存資訊(請依寄存機構、日期、號碼順序註記)

無

【０１７２】 國外寄存資訊(請依寄存國家、機構、日期、號碼順序註記)

無

【序列表】(請換頁單獨記載)

無

【發明申請專利範圍】

【第1項】 一種用於產生一對稱加密密鑰的系統(300)，該系統包含一第一終端(100a)、一第二終端(100b)及一伺服器(340)，該第一終端及該第二終端包含密鑰生成資料，其中該伺服器(340)經配置以進行下列步驟：

根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；

傳送該第一處理檔案(PF1)給該第一終端(100a)，以及傳送該第二處理檔案(PF2)給該第二終端(100b)；

其中該第一終端(100a)經配置以進行下列步驟：

接收該第一處理檔案(PF1)；

從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

產生一第一隨機密鑰種子並將該第一隨機密鑰種子

傳送至該第二終端(100b)；

從該第二終端(100b)接收一第二隨機密鑰種子；

其中該第二終端(100b)經配置以進行下列步驟：

接收該第二處理檔案(PF2)；

從該第二處理檔案(PF2)萃取經組合的密鑰生成資料(CKD)；

產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端(100a)；

從該第一終端(100a)接收該第一隨機密鑰種子；

由此該第一終端(100a)及該第二終端(100b)各經配置以進行下列步驟：

將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

將該些函數的結果串連到該對稱加密密鑰中，各終端(100)藉以產生該對稱加密密鑰的複本。

【第2項】 如請求項1所述之系統(300)，其中該密鑰生成資料(CKD)的組合是對用於該第一終端之密鑰生成資料(KD1)及用於該第二終端之密鑰生成資料(KD2)的按位元AND運算。

【第3項】 如請求項1或2所述之系統(300)，其中該

處理檔案是基於相應終端的密鑰生成資料(KD1、KD2)的相反數經過一位元改變函數、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合。

【第4項】 如請求項3所述之系統(300)，其中該位元改變函數是經配置以一機率將一輸入字串中每個1位元相反成一個0位元的函數。

【第5項】 如以上任一請求項所述之系統(300)，其中該第一終端(100a)及該第二終端(100b)各經配置，分別藉由對該第一處理檔案(PF1)及用於該第一終端的該密鑰生成資料(KD1)作按位元AND運算、以及對該第二處理檔案(PF2)及用於該第二終端的該密鑰生成資料(KD2)作按位元AND運算，以萃取該經組合密鑰生成資料(CKD)。

【第6項】 如以上任一請求項所述之系統(300)，其中該第一終端(100a)、該第二終端(100b)及該伺服器(340)個經配置來變異一密鑰生成資料，以及來更新該密鑰生成資料的一版本。

【第7項】 如以上任一請求項所述之系統(100、300)，其中該系統(100、300)是一設備(100)，且該第一終端(100a)是將被安裝在該設備(300)中的一外部裝置(245)，以及該設備經配置以執行該伺服器(340)

或與該伺服器(340)通訊。

【第8項】 一種用於產生一對稱加密密鑰的方法，該對稱加密密鑰用於使用在包含一第一終端(100a)、一第二終端(100b)及一伺服器(340)的一系統(300)中，該第一終端及該第二終端包含密鑰生成資料，其中該方法包含下列步驟：

該伺服器(340)根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

該伺服器(340)根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；

該伺服器(340)傳送該第一處理檔案(PF1)給該第一終端(100a)，以及傳送該第二處理檔案(PF2)給該第二終端(100b)；

該第一終端(100a)接收該第一處理檔案(PF1)；

該第一終端(100a)從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

該第一終端(100a)產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端(100b)；

該第一終端(100a)從該第二終端(100b)接收一第二隨機密鑰種子；

該第二終端(100b)接收該第二處理檔案(PF2)；

該第二終端(100b)從該第二處理檔案(PF2)萃取經組合的密鑰生成資料(CKD)；

該第二終端(100b)產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端(100a)；

該第二終端(100b)從該第一終端(100a)接收該第一隨機密鑰種子；

該第一終端(100a)及該第二終端(100b)各將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

該第一終端(100a)及該第二終端(100b)各將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

該第一終端(100a)及該第二終端(100b)兩者都將該些函數的結果串連到該對稱加密密鑰中。

【第9項】 一種供用於一系統(300)中產生一對稱加密密鑰的伺服器(340)，該系統包含一第一終端(100a)及一第二終端(100b)，該第一終端及該第二終端包含

密鑰生成資料，其中該伺服器經配置以進行下列步驟：

根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；及

傳送該第一處理檔案(PF1)給該第一終端(100a)以及傳送該第二處理檔案(PF2)給該第二終端(100b)。

【第10項】 一種包含密鑰生成資料的終端(100)，該密鑰生成資料用於在一系統(300)中產生一對稱加密密鑰，該系統包含一第二終端(100b)及一伺服器(300)，該第二終端包含密鑰生成資料，其中該終端(100)經配置以進行下列步驟：

接收一第一處理檔案(PF1)；

從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端(100b)；

從該第二終端(100b)接收一第二隨機密鑰種子；

將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

將該些函數的結果串連到該對稱加密密鑰中。

【第11項】 一種供用於一系統(300)中之一伺服器中產生一對稱加密密鑰的方法，該系統包含一第一終端(100a)及一第二終端(100b)，該第一終端及該第二終端包含密鑰生成資料，其中該方法包含下列步驟：

根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；及

傳送該第一處理檔案(PF1)給該第一終端(100a)以及傳送該第二處理檔案(PF2)給該第二終端(100b)。

【第12項】 一種用於產生一對稱加密密鑰的方法，該

對稱加密密鑰供用於一系統(300)中的一終端(100)中，該終端包含密鑰生成資料，該系統包含一第二終端(100b)及一伺服器(300)，該第二終端包含密鑰生成資料，其中該方法包含下列步驟：

接收一第一處理檔案(PF1)；

從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端(100b)；

從該第二終端(100b)接收一第二隨機密鑰種子；

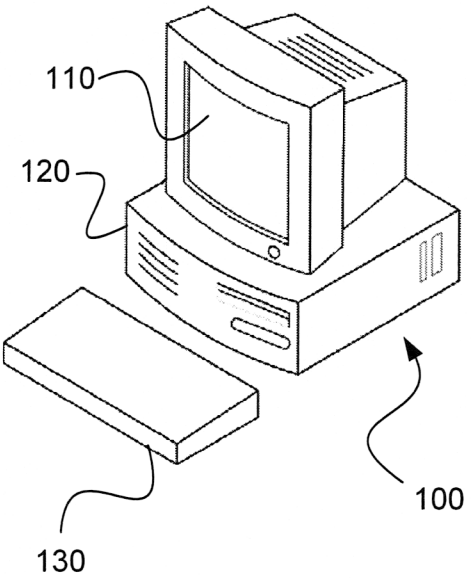
將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

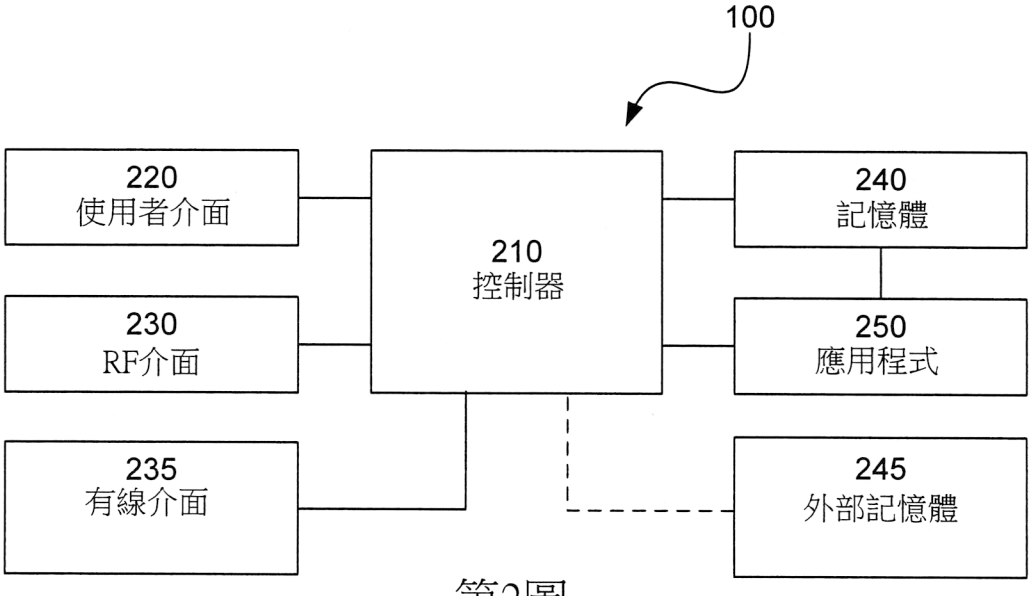
將該些函數的結果串連到該對稱加密密鑰中。

【第13項】 一種經編寫有指令(41)的電腦可讀取儲存媒體(40)，當該等指令(41)在一處理器上執行時進行如請求項8、11或12所述的方法。

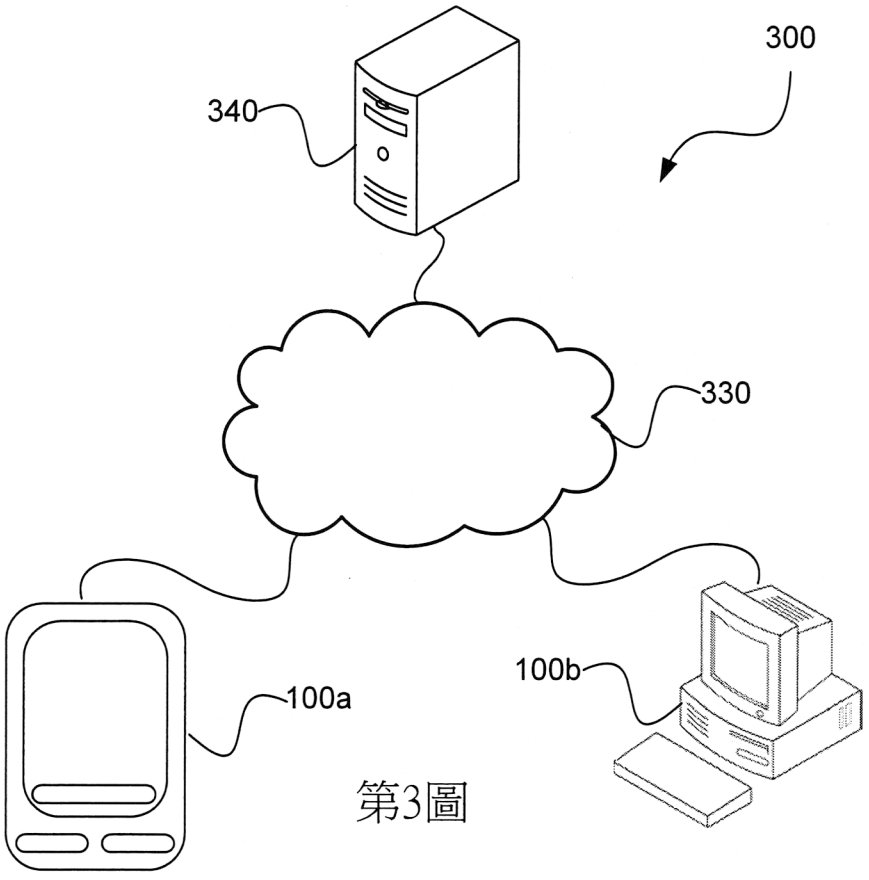
圖式


110
120
100
130

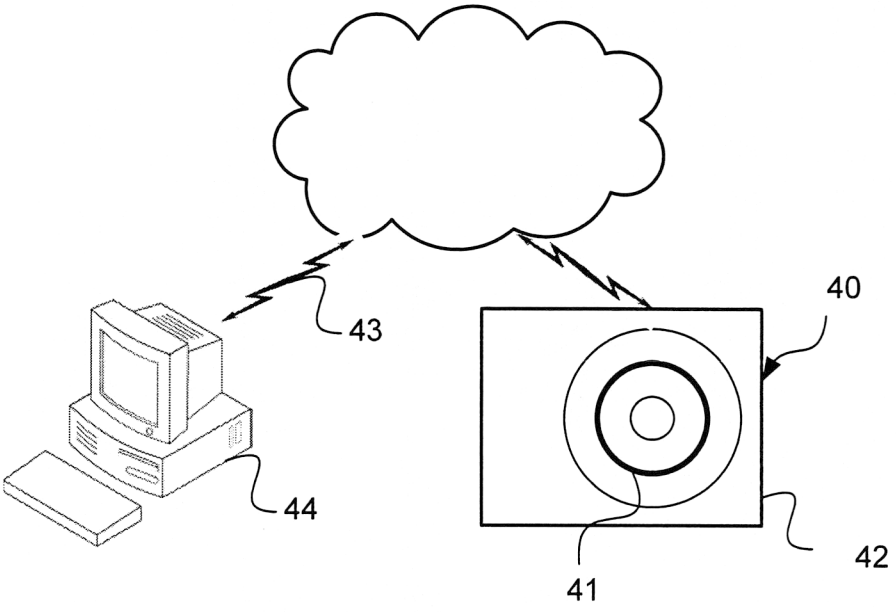
第1圖


100
220
使用者介面
210
控制器
240
記憶體
230
RF介面
250
應用程式
235
有線介面
245
外部記憶體

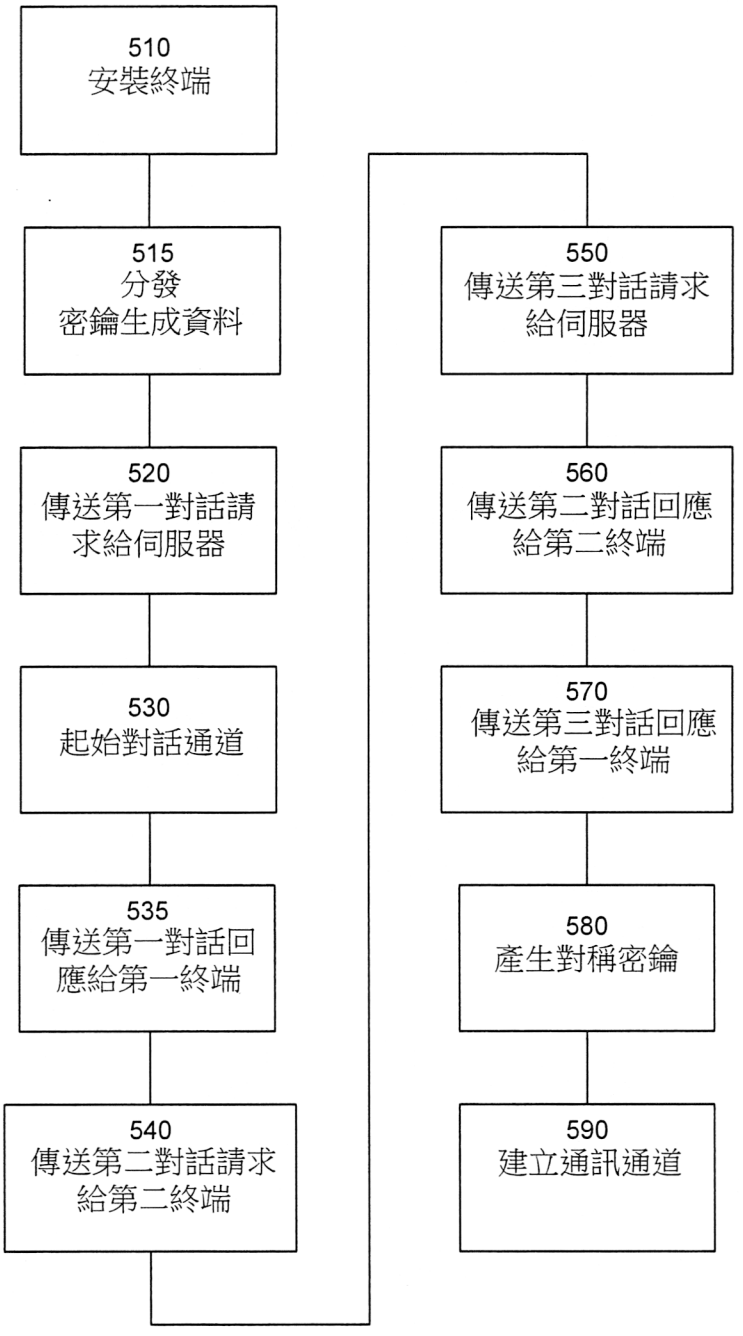
第2圖



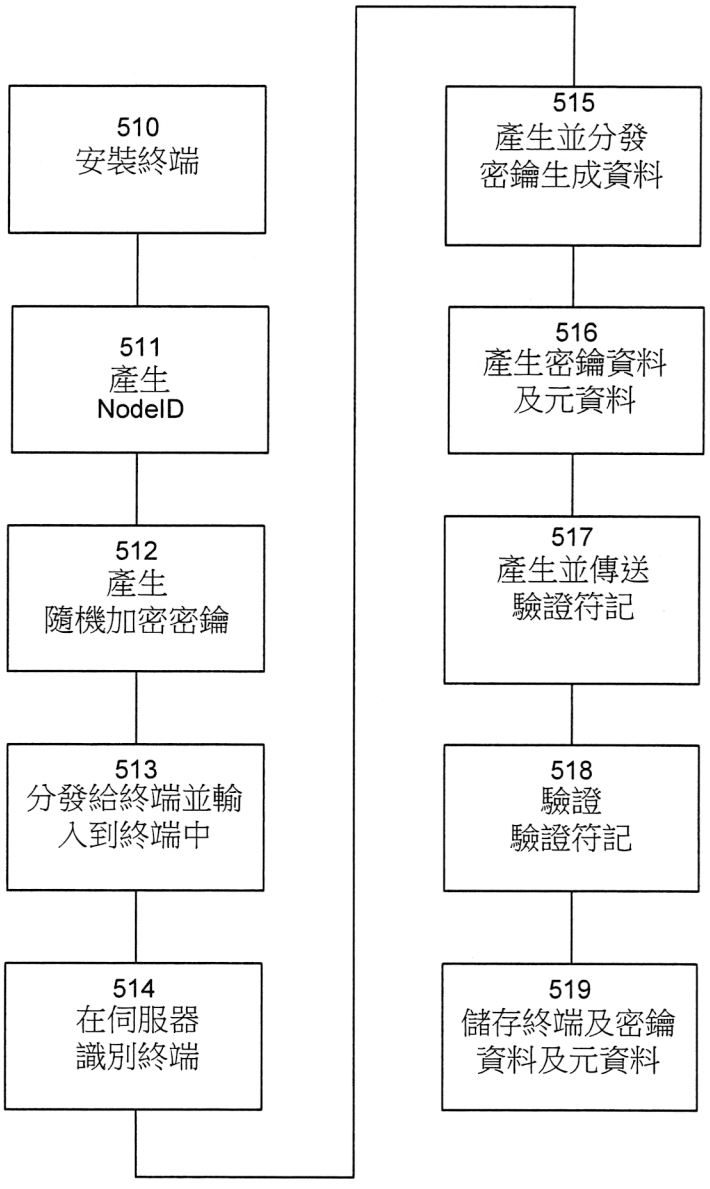
第3圖



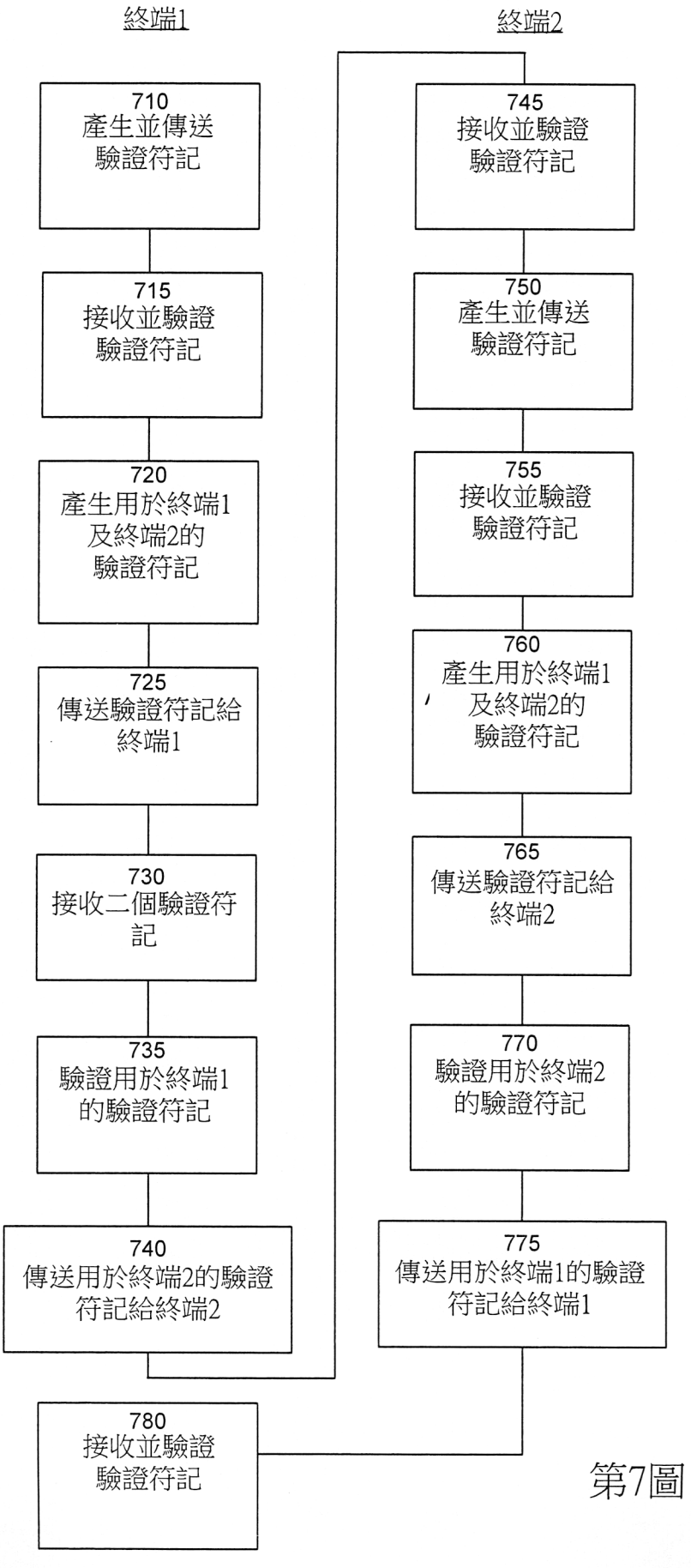
第4圖


510
安裝終端
515
分發
密鑰生成資料
520
傳送第一對話請求給伺服器
530
起始對話通道
535
傳送第一對話回應給第一終端
540
傳送第二對話請求給第二終端
550
傳送第三對話請求給伺服器
560
傳送第二對話回應給第二終端
570
傳送第三對話回應給第一終端
580
產生對稱密鑰
590
建立通訊通道

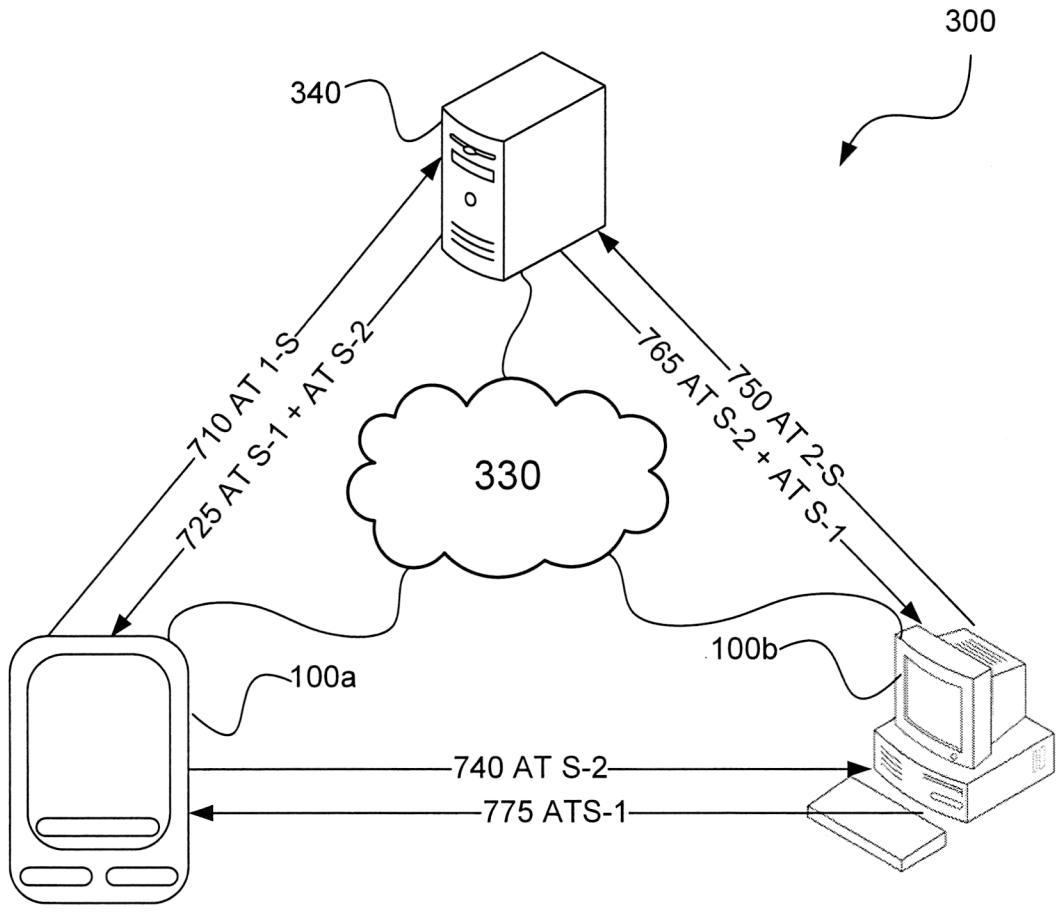
第5圖


510
安裝終端
511
產生
NodeID
512
產生
隨機加密密鑰
513
分發給終端並輸
入到終端中
514
在伺服器
識別終端
515
產生並分發
密鑰生成資料
516
產生密鑰資料
及元資料
517
產生並傳送
驗證符記
518
驗證
驗證符記
519
儲存終端及密鑰
資料及元資料

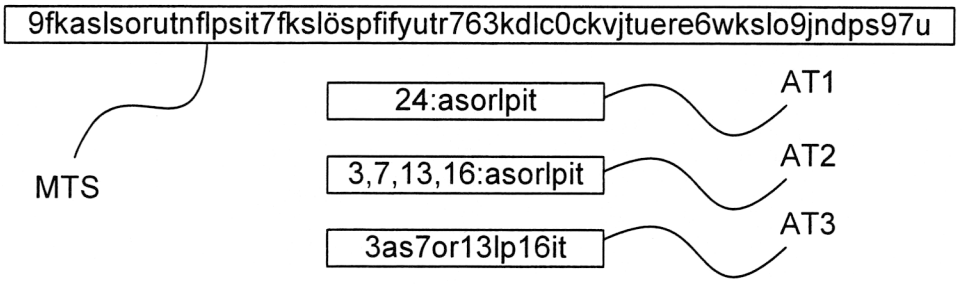
第6圖


終端1
終端2
710
產生並傳送
驗證符記
745
接收並驗證
驗證符記
715
接收並驗證
驗證符記
750
產生並傳送
驗證符記
720
產生用於終端1
及終端2的
驗證符記
755
接收並驗證
驗證符記
725
傳送驗證符記給
終端1
760
產生用於終端1
及終端2的
驗證符記
730
接收二個驗證符
記
765
傳送驗證符記給
終端2
735
驗證用於終端1
的驗證符記
770
驗證用於終端2
的驗證符記
740
傳送用於終端2的驗證
符記給終端2
775
傳送用於終端1的驗證
符記給終端1
780
接收並驗證
驗證符記

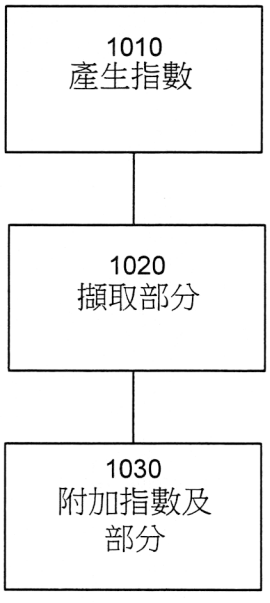
第7圖


300
340
710 AT 1-S
725 AT S-1 + AT S-2
765 AT S-2 + AT S-1
750 AT 2-S
330
100a
100b
740 AT S-2
775 ATS-1

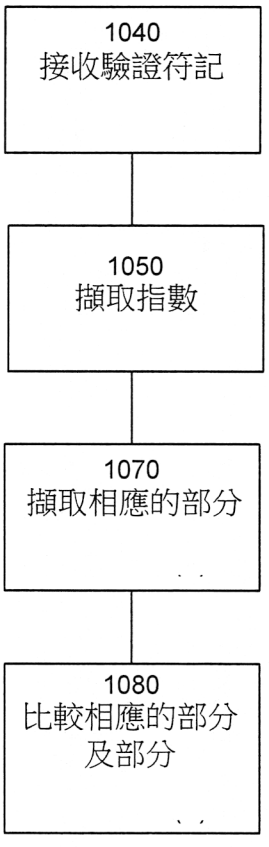
第8圖



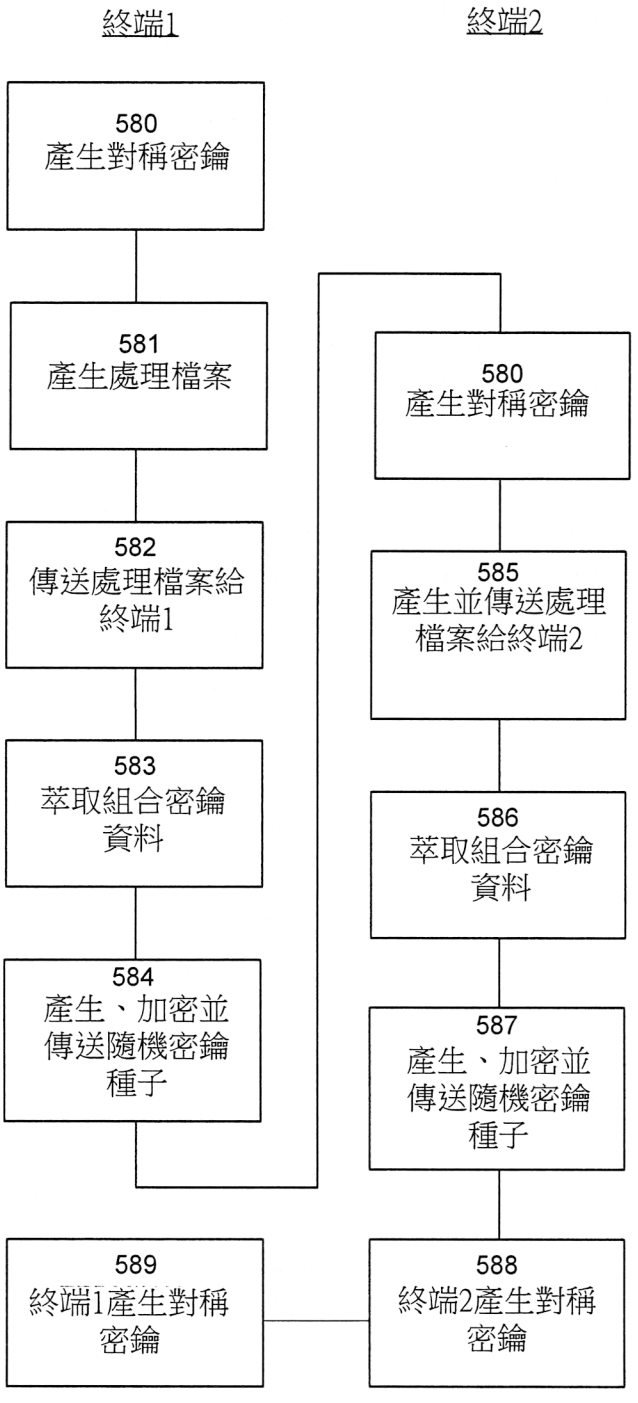
第9圖



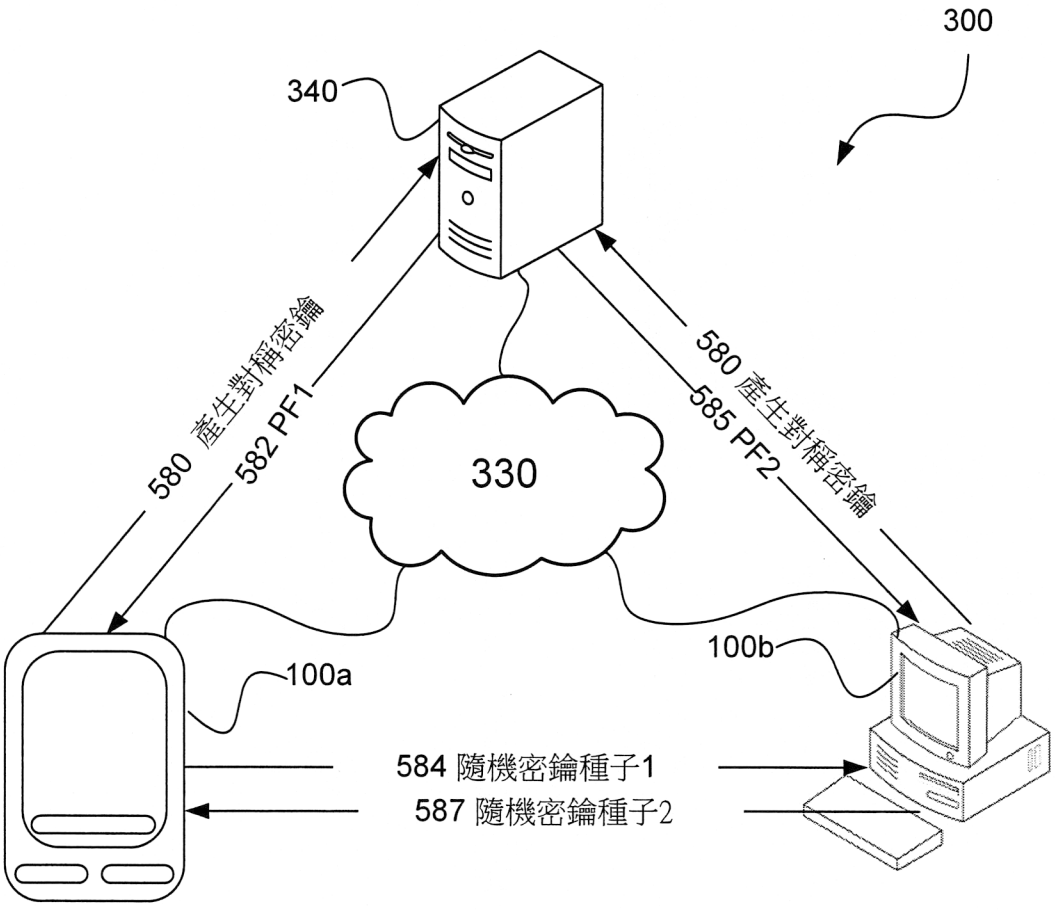
第10A圖



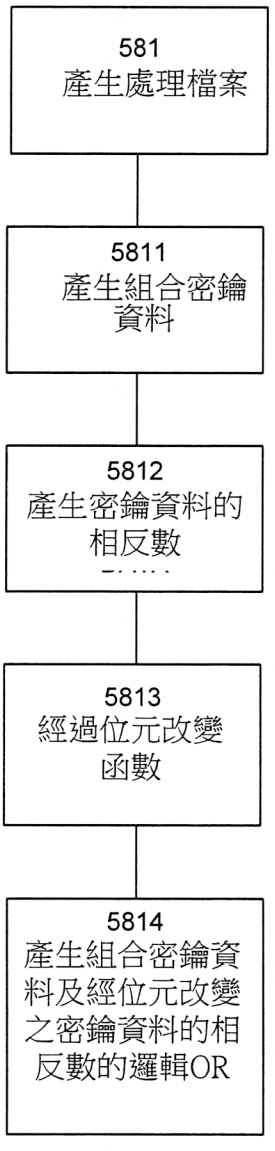
第10B圖


終端1
終端2
580
產生對稱密鑰
581
產生處理檔案
582
傳送處理檔案給終端1
583
萃取組合密鑰資料
584
產生、加密並傳送隨機密鑰種子
589
終端1產生對稱密鑰
580
產生對稱密鑰
585
產生並傳送處理檔案給終端2
586
萃取組合密鑰資料
587
產生、加密並傳送隨機密鑰種子
588
終端2產生對稱密鑰

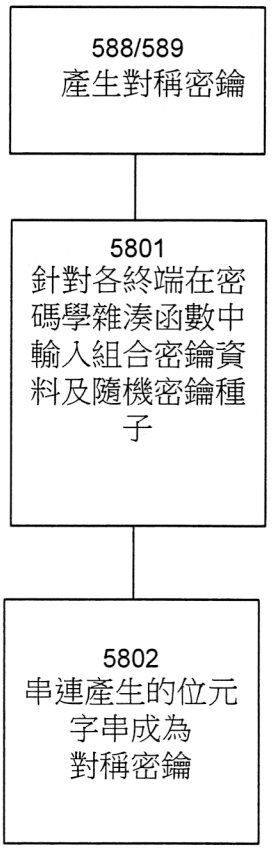
第11圖


300
340
580 產生對稱密鑰
582 PF1
580 產生對稱密鑰
585 PF2
330
100a
100b
584 隨機密鑰種子1
587 隨機密鑰種子2

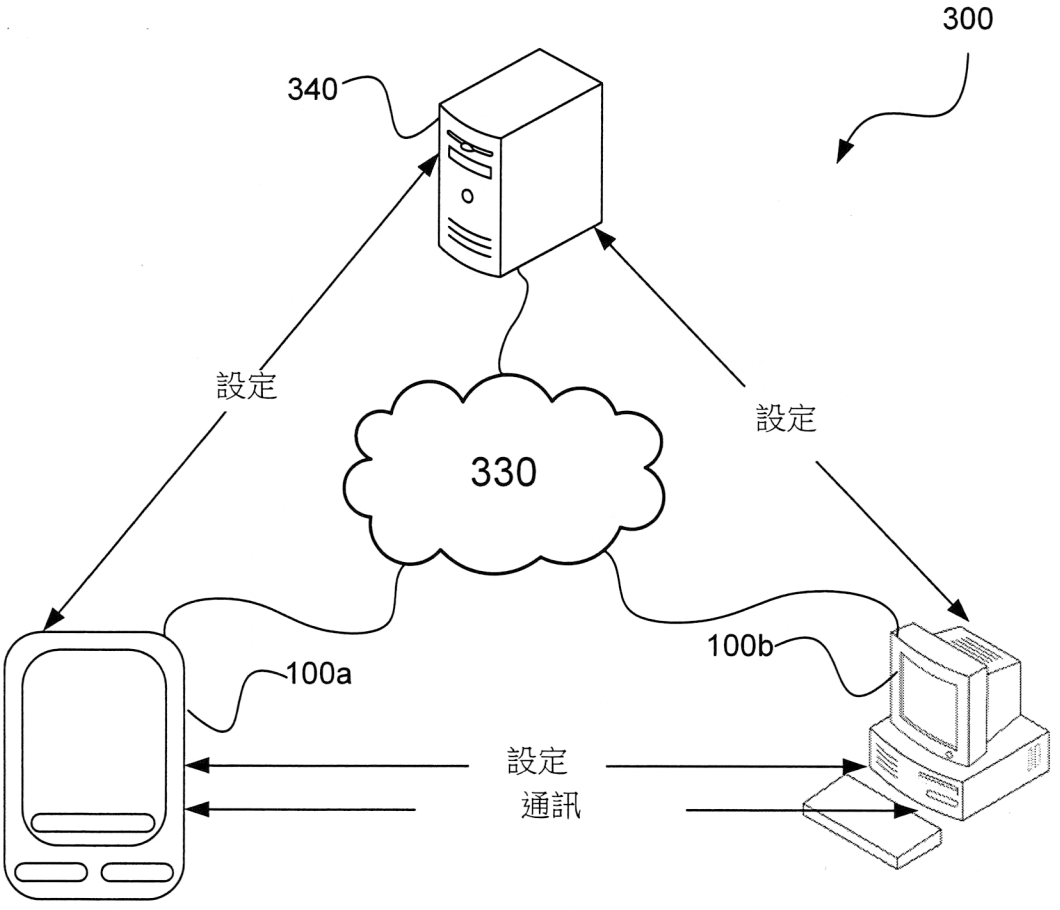
第12圖


581
產生處理檔案
5811
產生組合密鑰資料
5812
產生密鑰資料的相反數
5813
經過位元改變函數
5814
產生組合密鑰資料及經位元改變之密鑰資料的相反數的邏輯OR

第13圖


588/589
產生對稱密鑰
5801
針對各終端在密碼學雜湊函數中輸入組合密鑰資料及隨機密鑰種子
5802
串連產生的位元字串成為對稱密鑰

第14圖



第15圖

用於在二裝置（像是被連接到一個人電腦的一外部記憶體）之間建立安全連線的設備300之內。參看第3圖，第一裝置100a接著被連接到第二裝置100b。如一技術人員已知者，通訊將建立在一資料匯流排或其他內部通訊網路上。在該些裝置100a及100b中一者（或兩者）中，或是替代地在未圖示的另一裝置（像是設備300的一控制器）中執行的伺服器應用程式，對應至第3圖的伺服器340。參看第2圖，這樣的設備300可被設想成將連接一外部裝置245所至的一終端100。按照本說明書之教示而建立的安全通訊通道可接著由該控制器所實現，該控制器可能通過正由控制器210（或由另一驅動控制器）執行中的伺服器應用程式來當作一伺服器之用。可能該伺服器是一外部安全性伺服器，其經通過一有線或無線通訊通道被接觸，以管理用於該區域匯流排或其他裝置內通訊硬體的通訊交換位址的建立。

【0055】 應注意，在此情境中的外部裝置，可在一實施例中被理解為將被連接至一終端的裝置。其在此後內容可被理解為終端100的一個或多或少永久性（也可能是內建的）組件。

【0056】 第4圖顯示如上內容中所述之電腦可讀取媒體的示意圖。此實施例中的電腦可讀取媒體40是一資料碟片40。在一實施例中，資料碟片40是一磁性資料儲存碟片。資料碟片40經配置以承載指令41，當指令41被載入到控制器（像是處理器）中時執行按照以上描述之實施

代表銀行。伺服器340可由一互助銀行公司、該銀行本身或一安全連線提供者所管理。

【0067】 為了設立這樣的安全連線，第一終端100a藉由傳送一第一對話請求（520）到伺服器340來起始該設立步驟。該第一對話請求包括用於第二終端100b（該第一終端想要與其設立通訊）的一識別符。用於通道資料的識別符在一實施例中可能是對一網際網路協定通訊通道的一位址（像是一致資源定位位址(URL)或網際網路協定(IP)位址）。

【0068】 伺服器340起始或建立一對話通道（530）並以一第一對話回應來回應（535），由第一終端100a所接收的該第一對話回應指示了用於該對話通道的一識別符以及用於第二終端100b的密鑰資料。第一終端100a接著傳送（540）一第二對話請求到第二終端100b。該第二對話請求包括第一終端100a的識別及用於第一終端100a的一密鑰加密種子。

【0069】 隨著第二終端100b接收來自第一終端100a的該第二對話請求，第二終端100b傳送一第三對話請求（550）給伺服器340。該第三對話請求包括用於第一終端100a的一識別符及/或用於目前對話的一識別符。伺服器340決定是否第一終端100a被允許與第二終端100b連接，如果是則傳送一第二對話回應（560）給第二終端100b，其中該第二對話回應包括用於該對話通道的識別符以及有關第一終端100a之密鑰產生的資料。

【0095】 如果驗證了該驗證符記，則用於終端100的一身分（像是一識別）被儲存（519）在伺服器340中。在一實施例中，用於終端100的識別是NodeID。在一實施例中，用於終端100的識別是IMSI（國際行動訂戶識別）、IMEI（國際行動裝備識別符）及/或終端100的序號。在一實施例中，用於終端100的識別是一應用程式識別符，其係與運用如本說明書所教示之安全通訊通道的應用程式一起提供。

【0096】 對於其中終端是一外部裝置的實施例來說，用於該外部裝置的NodeID可連同該外部裝置一起供應，或者該外部裝置的NodeID可在登錄該外部裝置245之後即被傳送給使用者或給該外部裝置。

交互驗證

【0097】 隨著終端100a已被安裝而嘗試與第二終端100b（像是金融交易應用程式伺服器）設立一通訊通道，其中該通訊通道是由安全性伺服器340所主控，可能是相同銀行伺服器之部分或是被實施在相同銀行伺服器中，終端100a將由安全性伺服器340（此後將如上稱為伺服器340）所驗證。在伺服器340驗證終端100a之後，伺服器340被提供以用來建立與第二終端100b之安全通訊的必要的密鑰資料。

【0098】 然而，現今的社會中網際網路上流通許多詐騙，正因此我們需要安全通訊通道。然而，發明人已察覺全部此類安全通訊系統本質上有一根本的問題，在於：利

【0128】 在一實施例中，伺服器340將針對第二終端100b的驗證符記AT S-2加密。加密該驗證符記可利用用於第二終端100b之元資料的一部分，而在這樣的實施例中，該驗證符記可經配置以包含多一欄位，該欄位指示一加密指數，該加密指數只是了在元資料的何處可以找到用於加密該驗證符記的加密密鑰。因此該加密指數是在未加密之下被傳輸。如此避免任何惡意的攻擊者偽裝成第二終端100b去解密驗證符記AT S-2。

【0129】 隨著第一終端100a接收（730）該等二個驗證符記AT S-1及AT S-2，第一終端100a驗證（735）從伺服器340所接收的第一驗證符記AT S-1。

【0130】 由於第一終端100a無法取得第二終端100b的元資料，第一終端100a無法驗證從伺服器340接收的第二驗證符記AT S-2。然而，藉由伺服器340傳送目標是第二終端100b的驗證符記給第一終端100a，則通過第二終端100b達成了對伺服器340的額外驗證。

【0131】 如果對於從伺服器340接收的第一驗證符記AT S-1驗證成功，則第一終端100a繼續進行由第二終端100b實施的額外驗證。在這方面，該第一終端傳送（740）從伺服器340接收的第二驗證符記AT S-2給第二終端100b。第二終端100b接收並驗證（745）驗證符記AT S-2。如果驗證成功，則已經通過第一終端100a及第二終端100b兩者驗證了伺服器340。如此已經達成高度安全性的交互驗證。

【0132】 然而，由於理解到若惡意的詐騙操縱者已經能挾制第一終端100a及伺服器340之間的通訊通道，則針對第二終端2的驗證符記也可能被洩露。為了更進一步增加驗證的安全性，第二終端100b較佳地經配置也去驗證伺服器340。

【0133】 隨著第二終端100b已經驗證了從伺服器340通過第一終端100a所接收、且針對第二終端100b的驗證符記AT S-2，該第二終端繼續利用其對伺服器340的自有通訊通道來驗證伺服器340。

【0134】 該第二終端因此產生用於伺服器340的一驗證符記AT 2-S，並傳送（750）該驗證符記給伺服器340。伺服器340接收驗證符記AT 2-S並予以驗證（755）。如果驗證成功，則第二終端100b被伺服器340所驗證，且伺服器340產生（760）一個針對第一終端100a的驗證符記AT S-1以及一個針對第二終端100b的驗證符記AT S-2，並傳送（765）驗證符記AT S-1、AT S-2兩者至第二終端100b。

【0135】 隨著第二終端100b接收（770）二個驗證符記AT S-1及AT S-2，第二終端100b驗證從伺服器340接收的第二驗證符記AT S-2，如果成功則傳送（775）第一驗證符記AT S-1至第一終端100a，第一終端100a驗證（780）其從伺服器340通過第二終端100b所接收、並針對第一終端100a自身的驗證符記AT S-1。

【0136】 伺服器340不只是因此被第一終端100a所驗證，伺服器340也被第二終端100b代表第一終端100a所驗證。該二個終端因此彼此協助以驗證伺服器340。此外，由第一終端100a通過從伺服器340經由第二終端100b所接收的該些驗證符記，第一終端100a隱含地驗證了第二終端100b。另外，伺服器340被利用二個不同的通訊通道所驗證，藉以使得詐騙操縱者難以惡意地將自身識別為安全性伺服器340。

對稱加密密鑰的生成

【0137】 隨著二個終端100及伺服器340已被驗證，一個對稱加密密鑰被產生。參看第5圖，一終端100當被安裝時接收（515）密鑰生成資料，且該終端根據該密鑰生成資料產生（516）密鑰資料。該密鑰資料將被用來產生以下將揭露的對稱加密密鑰。該對稱加密密鑰將被用於第一終端100a及第二終端100b之間通訊的加密。第一終端100a可能是（如上所述）安全服務的客戶端，而第二終端100b可能是該服務的提供者。

【0138】 替代地，第一終端100a可為要被連接至一設備300的一外部裝置245，其中第二終端100b代表設備300。

【0139】 被產生的密鑰資料僅為第一終端100a及伺服器340所知，而第二終端100b不知道此密鑰資料。如此致使了增加的安全性，因為所要建立的通訊連線在沒有交

【發明申請專利範圍】

【第 1 項】 一種用於產生一對稱加密密鑰的系統(300)，該系統包含一第一終端(100a)、一第二終端(100b)及一伺服器(340)，該第一終端及該第二終端包含密鑰生成資料，其中該伺服器(340)經配置以進行下列步驟：

根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；

傳送該第一處理檔案(PF1)給該第一終端(100a)，以及傳送該第二處理檔案(PF2)給該第二終端(100b)；

其中該第一終端(100a)經配置以進行下列步驟：

接收該第一處理檔案(PF1)；

從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

產生一第一隨機密鑰種子並將該第一隨機密鑰種子

傳送至該第二終端(100b)；

從該第二終端(100b)接收一第二隨機密鑰種子；

其中該第二終端(100b)經配置以進行下列步驟：

接收該第二處理檔案(PF2)；

從該第二處理檔案(PF2)萃取經組合的密鑰生成資料(CKD)；

產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端(100a)；

從該第一終端(100a)接收該第一隨機密鑰種子；

由此該第一終端(100a)及該第二終端(100b)各經配置以進行下列步驟：

將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

將該些函數的結果串連到該對稱加密密鑰中，各終端(100)藉以產生該對稱加密密鑰的複本。

【第2項】 如請求項1所述之系統(300)，其中該密鑰生成資料(CKD)的組合是對用於該第一終端之密鑰生成資料(KD1)及用於該第二終端之密鑰生成資料(KD2)的按位元AND運算。

【第3項】 如請求項1或2所述之系統(300)，其中該

處理檔案是基於相應終端的密鑰生成資料(KD1、KD2)的相反數經過一位元改變函數、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合。

【第4項】 如請求項3所述之系統(300)，其中該位元改變函數是經配置以一機率將一輸入字串中每個1位元相反成一個0位元的函數。

【第5項】 如請求項1或2所述之系統(300)，其中該第一終端(100a)及該第二終端(100b)各經配置，分別藉由對該第一處理檔案(PF1)及用於該第一終端的該密鑰生成資料(KD1)作按位元AND運算、以及對該第二處理檔案(PF2)及用於該第二終端的該密鑰生成資料(KD2)作按位元AND運算，以萃取該經組合密鑰生成資料(CKD)。

【第6項】 如請求項1或2所述之系統(300)，其中該第一終端(100a)、該第二終端(100b)及該伺服器(340)個經配置來變異一密鑰生成資料，以及來更新該密鑰生成資料的一版本。

【第7項】 如請求項1或2所述之系統(300)，其中該系統(300)是一設備(100)，且該第一終端(100a)是將被安裝在該設備(100)中的一外部裝置(245)，以及該設備經配置以執行該伺服器(340)或與該伺服器

(340)通訊。

【第8項】 一種用於產生一對稱加密密鑰的方法，該對稱加密密鑰用於使用在包含一第一終端(100a)、一第二終端(100b)及一伺服器(340)的一系統(300)中，該第一終端及該第二終端包含密鑰生成資料，其中該方法包含下列步驟：

該伺服器(340)根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

該伺服器(340)根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；

該伺服器(340)傳送該第一處理檔案(PF1)給該第一終端(100a)，以及傳送該第二處理檔案(PF2)給該第二終端(100b)；

該第一終端(100a)接收該第一處理檔案(PF1)；

該第一終端(100a)從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

該第一終端(100a)產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端(100b)；

該第一終端(100a)從該第二終端(100b)接收一第二隨機密鑰種子；

該第二終端(100b)接收該第二處理檔案(PF2)；

該第二終端(100b)從該第二處理檔案(PF2)萃取經組合的密鑰生成資料(CKD)；

該第二終端(100b)產生該第二隨機密鑰種子並將該第二隨機密鑰種子傳送至該第一終端(100a)；

該第二終端(100b)從該第一終端(100a)接收該第一隨機密鑰種子；

該第一終端(100a)及該第二終端(100b)各將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

該第一終端(100a)及該第二終端(100b)各將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

該第一終端(100a)及該第二終端(100b)兩者都將該些函數的結果串連到該對稱加密密鑰中。

【第9項】 一種供用於一系統(300)中產生一對稱加密密鑰的伺服器(340)，該系統包含一第一終端(100a)及一第二終端(100b)，該第一終端及該第二終端包含

密鑰生成資料，其中該伺服器經配置以進行下列步驟：

根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；及

傳送該第一處理檔案(PF1)給該第一終端(100a)以及傳送該第二處理檔案(PF2)給該第二終端(100b)。

【第10項】 一種包含密鑰生成資料的終端(100)，該密鑰生成資料用於在一系統(300)中產生一對稱加密密鑰，該系統包含一第二終端(100b)及一伺服器(300)，該第二終端包含密鑰生成資料，其中該終端(100)經配置以進行下列步驟：

接收一第一處理檔案(PF1)；

從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端(100b)；

從該第二終端(100b)接收一第二隨機密鑰種子；

將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

將該些函數的結果串連到該對稱加密密鑰中。

【第11項】 一種供用於一系統(300)中之一伺服器中產生一對稱加密密鑰的方法，該系統包含一第一終端(100a)及一第二終端(100b)，該第一終端及該第二終端包含密鑰生成資料，其中該方法包含下列步驟：

根據用於該第一終端的密鑰生成資料(KD1)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第一終端(100a)產生一第一處理檔案(PF1)；

根據用於該第二終端的密鑰生成資料(KD2)、以及用於該第一終端的密鑰生成資料(KD1)和用於該第二終端的密鑰生成資料(KD2)的組合(CKD)，針對該第二終端(100b)產生一第二處理檔案(PF2)；及

傳送該第一處理檔案(PF1)給該第一終端(100a)以及傳送該第二處理檔案(PF2)給該第二終端(100b)。

【第12項】 一種用於產生一對稱加密密鑰的方法，該

對稱加密密鑰供用於一系統(300)中的一終端(100)中，該終端包含密鑰生成資料，該系統包含一第二終端(100b)及一伺服器(300)，該第二終端包含密鑰生成資料，其中該方法包含下列步驟：

接收一第一處理檔案(PF1)；

從該第一處理檔案(PF1)萃取經組合的密鑰生成資料(CKD)；

產生一第一隨機密鑰種子並將該第一隨機密鑰種子傳送至該第二終端(100b)；

從該第二終端(100b)接收一第二隨機密鑰種子；

將該經組合的密鑰生成資料(CKD)及該第一隨機種子輸入到一函數中；

將該經組合的密鑰生成資料(CKD)及該第二隨機種子輸入到該相同函數中；以及

將該些函數的結果串連到該對稱加密密鑰中。

【第13項】 一種經編寫有指令(41)的電腦可讀取儲存媒體(40)，當該等指令(41)在一處理器上執行時進行如請求項8、11或12所述的方法。