【19】中華民國　　【12】專利公報　(B)

【11】證書號數：I312632

【45】公告日：中華民國98(2009) 年 7 月 21 日

【51】Int. Cl.：　*H04L9/32 (2006.01)*　　*H04L29/06 (2006.01)*

發明　　全 12 頁

【54】名稱：　認證處理方法、認證處理程式、記錄媒體及認證處理裝置

AUTHENTICATION METHOD, AUTHENTICATION APPARATUS, AND COMPUTER PRODUCT

【21】申請案號：095106973　　【22】申請日：中華民國95(2006)年3月2日

【11】公開編號：200709639　　【43】公開日：中華民國96(2007)年3月1日

【30】優先權：　2005/08/26　　日本　　2005-246506

【72】發明人：　清水明宏 AKIHIRO SHIMIZU；辻貴介 TAKASUKE TSUJI

【71】申請人：　三統安防系統股份有限公司 TRINITY SECURITY SYSTEMS, INC.
日本

【74】代理人：　洪澄文

【56】參考文獻：

TW I228903　　TW I231899

US 6230269B1　　US 6434700B1

US 6912653B2　　US 2003/0097567A1

[57]申請專利範圍：

1.一種認證處理方法，於對被認證裝置進行認證之認證裝置，

其特徵在於包含：

由前述被認證裝置取得使用任意值而產生之用於本次認證處理之本次認證資訊的取得步驟；

由前述被認證裝置接收：使用前述本次認證資訊，將用於下次認證處理之下次認證資訊予以隱藏的第一送訊資訊；以及使用前述下次認證資訊，將前述任意值予以隱藏的第二送訊資訊的收訊步驟；

使用由前述收訊步驟接收到的前述第一送訊資訊與由前述取得步驟取得的前述本次認證資訊來計算出前述下次認證資訊，使用該下次認證資訊與前述第二送訊資訊來算出前述任意值的計算步驟；以及

根據由前述計算步驟算出的前述任意值與由前述取得步驟取得的前述

本次認證資訊，來判斷是否對前述被認證裝置進行認證。

2.如申請專利範圍第1項之認證處理方法，其中，前述取得步驟係取得對於前述任意值，藉由單向轉換函數進行運算而產生的本次認證資訊；

前述判斷步驟係判斷對於前述任意值，藉由單向轉換函數進行運算而得的值是否與前述本次認證資訊相一致。

3.如申請專利範圍第1或2項之認證處理方法，其中，前述收訊步驟係接收對於前述下次認證資訊與前述本次認證資訊，藉由遮罩函數進行運算所得的值，來作為第一送訊資訊，且接收對於前述任意值與前述下次認證資訊，藉由前述遮罩函數進行運算所得的值，來作為第二送訊資訊；

前述計算步驟係對於前述第一送訊資訊與前述本次認證資訊，藉由前述遮罩函數進行運算，而計算出前述下次認證資訊，且對於前述下次認證資訊與前述第二送訊資訊，藉由前述遮罩函數進行運算，而計算出前述任意值。

4.如申請專利範圍第1或2項之認證處理方法，其中，復包含取得前述被認證裝置特有之認證鍵的認證鍵取得步驟；

前述收訊步驟係接收藉由對於前述下次認證資訊，使用前述認證鍵進行預定運算所得的值，而將前述任意值予以隱藏的值，來作為第二送訊資訊；

前述計算步驟係使用前述認證鍵與前述下次認證資訊與前述第二送訊資訊，來計算出前述任意值。

5.如申請專利範圍第1或2項之認證處理方法，其中，復包含取得前述被認證裝置特有之認證鍵的認證鍵取得步驟；

前述收訊步驟係接收使用前述本次認證資訊，將對於前述下次認證資訊，使用前述認證鍵進行預定運算所得的值予以隱藏的值，來作為第一送訊資訊；

前述計算步驟係使用前述認證鍵與前述第一送訊資訊與前述本次認證資訊，來計算出前述下次認證資訊。

6.如申請專利範圍第1或2項之認證處理方法，其中，復包含：取得以前述下次認證資訊為加密鍵而將前述任意值予以加密的加密資訊的加密資訊取得步驟；

前述判斷步驟係以前述下次認證資訊為加密鍵而將前述加密資訊予以解碼，根據經解碼的加密資訊，來判斷是否對前述被認證裝置進行認證。

7.如申請專利範圍第6項之認證處理方法，其中，前述取得步驟係取得對於前述任意值進行2次單向轉換函數的運算而產生的本次認證資訊；

前述判斷步驟係判斷對於前述任意值進行2次前述單向轉換函數的運算而得的值是否與前述本次認證資訊相一致，根據其判斷結果，來判斷是否對前述被認證裝置進行認證。

8.一種認證處理方法，於對認證裝置請求認證之被認證裝置，

其特徵在於包含：

使用任意值，而產生用於本次認證處理之本次認證資訊的產生步驟；

將由前述產生步驟所產生的本次認證資訊發送至前述認證裝置的發送步驟；

進行計算：使用前述本次認證資訊，將用於下次認證處理的下次認

證資訊予以隱藏的第一送訊資訊；以及使用前述下次認證資訊，將前述任意值予以隱藏的第二送訊資訊的計算步驟；以及

將由前述計算步驟所計算出的前述第一送訊資訊與前述第二送訊資訊傳送至前述認證裝置的送訊步驟。

9.如申請專利範圍第8項之認證處理方法，其中，前述產生步驟係對於前述任意值進行單向轉換函數之運算，藉此產生前述本次認證資訊。

10.如申請專利範圍第8或9項之認證處理方法，其中，前述計算步驟係對於前述下次認證資訊與前述本次認證資訊，計算出進行遮罩函數之運算後的值，來作為第一送訊資訊，且對於前述任意值與前述下次認證資訊，計算出進行前述遮罩函數之運算後的值，來作為第二送訊資訊。

11.如申請專利範圍第8或9項之認證處理方法，其中，復包含：產生前述被認證裝置特有之認證鍵的認證鍵產生步驟；以及

將前述認證鍵發送至前述認證裝置的認證鍵發送步驟；

前述計算步驟係計算出藉由於前述下次認證資訊中使用前述認證鍵進行預定運算所得的值，將前述任意值予以隱藏的值。

12.如申請專利範圍第8或9項之認證處理方法，其中，復包含：產生前述被認證裝置特有之認證鍵的認證鍵產生步驟；以及

將前述認證鍵發送至前述認證裝置的認證鍵發送步驟；

前述計算步驟係計算出使用前述本次認證資訊，將於前述下次認證資訊中使用前述認證鍵進行預定運算所得的值予以隱藏的值，來作為第一送訊資訊。

13.如申請專利範圍第8或9項之認證處理方法，其中，復包含：產生以前述下次認證資訊為加密鍵而將前述任意值予以加密的加密資訊的加密資訊產生步驟；以及

將前述加密資訊發送至前述認證裝置的加密資訊發送步驟。

14.如申請專利範圍第13項之認證處理方法，其中，前述產生步驟係對於前述任意值進行2次單向轉換函數之運算，而產生前述本次認證資訊。

15.一種認證處理程式，其特徵在於：使電腦執行申請專利範圍第1或8項之認證處理方法。

16.一種電腦可讀取之記錄媒體，記錄有申請專利範圍第15項之認證處理程式。

17.一種認證處理裝置，其特徵在於包含：

取得手段，用以由被認證裝置取得使用任意值而產生之用於本次認證處理之本次認證資訊；

收訊手段，用以由前述被認證裝置接收：使用前述本次認證資訊，將用於下次認證處理之下次認證資訊予以隱藏的第一送訊資訊；以及使用前述下次認證資訊，將前述任意值予以隱藏的第二送訊資訊；

計算手段，用以使用由前述收訊手段接收到的前述第一送訊資訊與由前述取得手段取得的前述本次認證資訊來計算出前述下次認證資訊，使用該下次認證資訊與前述第二送訊資訊來算出前述任意值；以及

判斷手段，用以根據由前述計算手段算出的前述任意值與由前述取得手段取得的前述本次認證資訊，來判斷是否對前述被認證裝置進行認證。

18.一種認證處理裝置，其特徵在於包含：

產生手段，用以使用任意值，而產生用於本次認證處理之本次認證資訊；

發送手段，用以將由前述產生手段所產生的本次認證資訊發送至由本身裝置請求認證的另一裝置；

計算手段，用以計算：使用前述本次認證資訊，將用於下次認證處理的下次認證資訊隱藏的第一送訊資訊；以及使用前述下次認證資訊將前述任意值予以隱藏的第二送訊資訊；以及

送訊手段，用以將由前述計算手段所計算出的前述第一送訊資訊與前述第二送訊資訊傳送至前述另一裝置。

圖式簡單說明：

第 1 圖係顯示實施形態之認證處理系統的系統構成說明圖。

第 2 圖係顯示構成認證處理系統之使用者、伺服器的硬體構成之一例的方塊圖。

第 3 圖係顯示構成認證處理系統之使用者、伺服器之功能性構成的方塊圖。

第 4 圖係顯示使用者的初始登錄處理步驟的流程圖。

第 5 圖係顯示初次(n=1)以後，進行第 n 次認證處理之步驟的流程圖。

第 6 圖係顯示使用者的初始登錄處理步驟的流程圖。

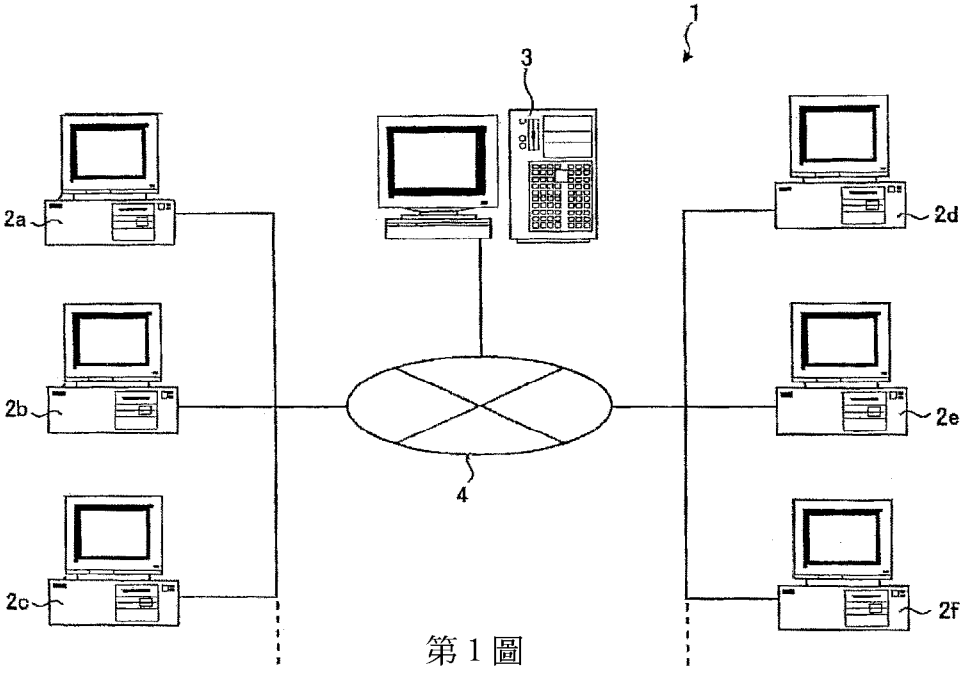
第 7 圖係顯示初次(n=1)以後，進行第 n 次認證處理之步驟的流程圖。

第 8 圖係顯示使用者的初始登錄處理步驟的流程圖。

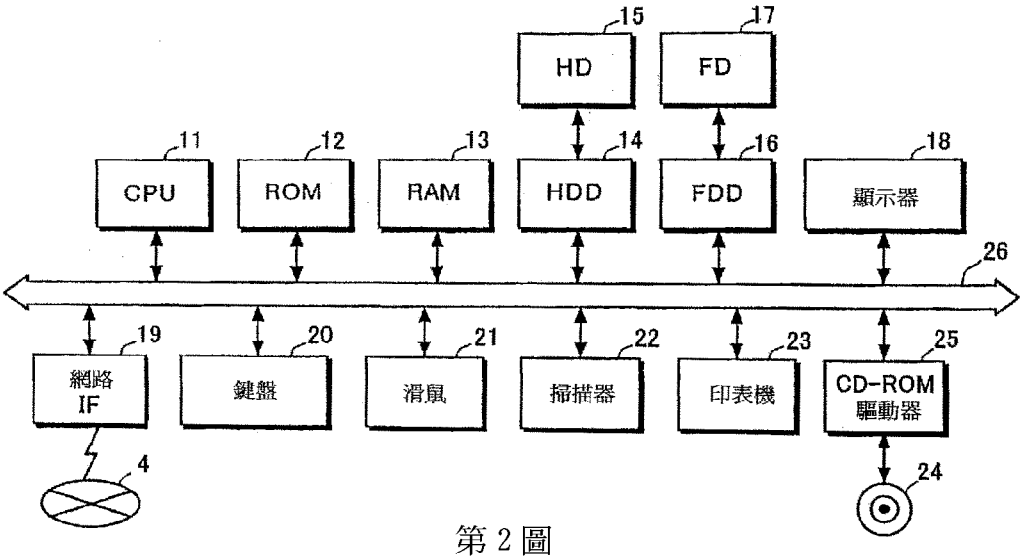
第 9 圖係顯示初次(n=1)以後，進行第 n 次認證處理之步驟的流程圖。

第 10 圖係顯示 SAS-2 認證方式中使用者認證之處理步驟的流程圖。

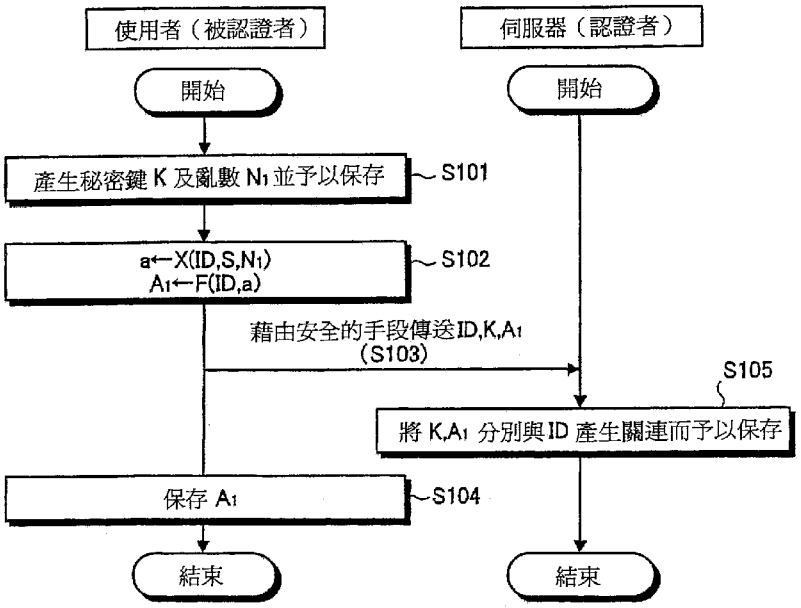
第 11 圖係顯示 SAS-2 認證方式中使用者認證之處理步驟的流程圖。



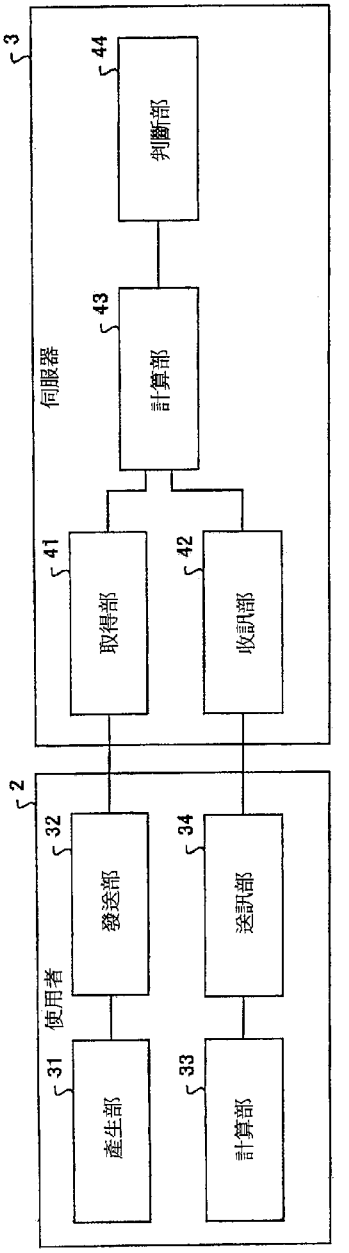
第 1 圖


15
HD
17
FD
11
CPU
12
ROM
13
RAM
14
HDD
16
FDD
18
顯示器
26
19
網路
IF
20
鍵盤
21
滑鼠
22
掃描器
23
印表機
25
CD-ROM
驅動器
4
24

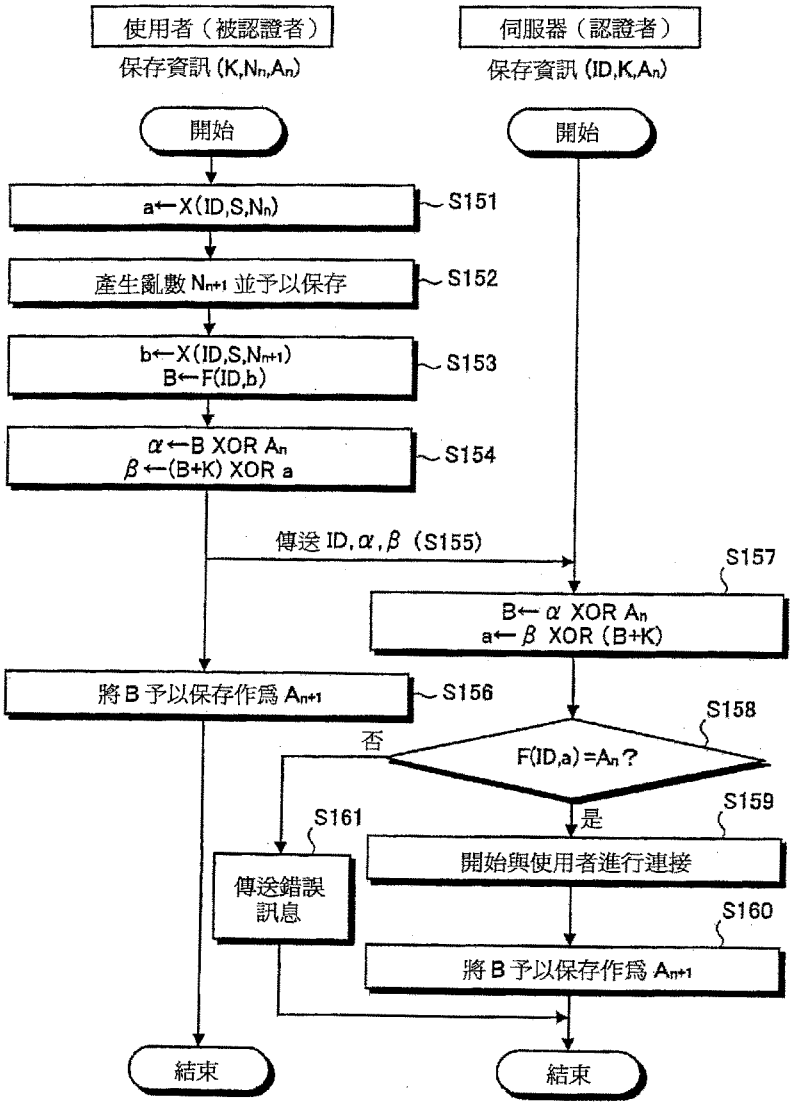
第 2 圖


使用者（被認證者）
伺服器（認證者）
開始
開始
產生秘密鍵 K 及亂數 N1 並予以保存
S101
a←X(ID,S,N1)
A1←F(ID,a)
S102
藉由安全的手段傳送ID,K,A1
(S103)
S105
將 K,A1 分別與 ID 產生關連而予以保存
保存 A1
S104
結束
結束

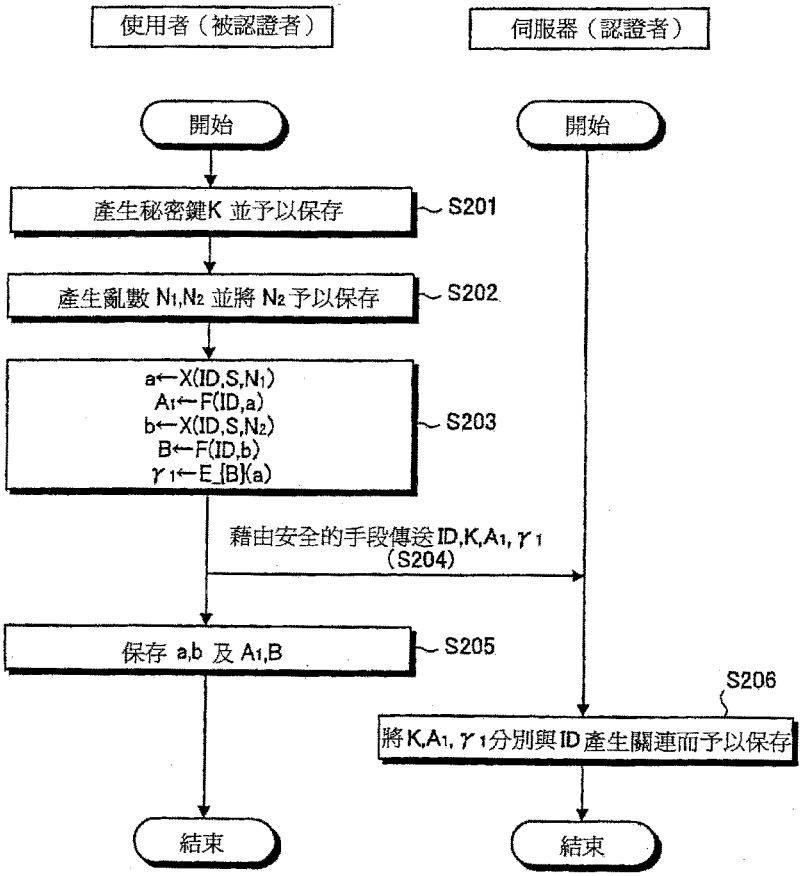
第 4 圖



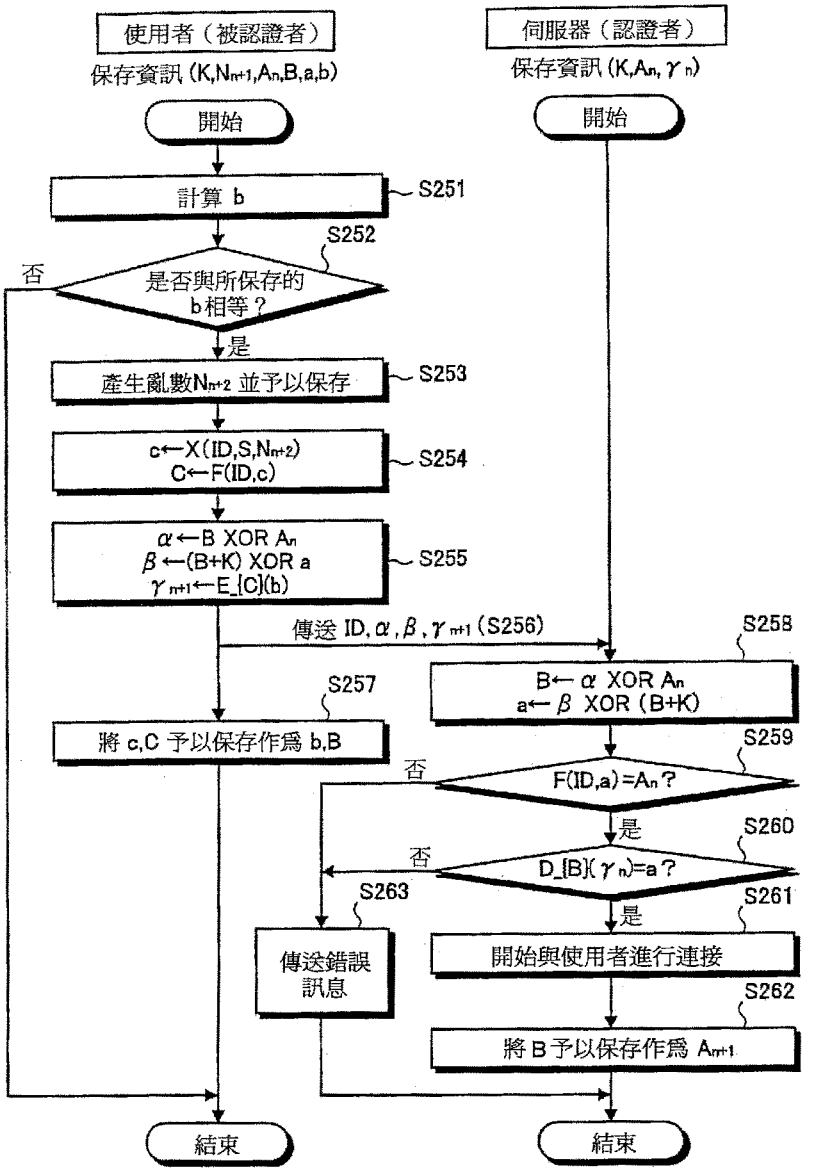
第 3 圖


使用者（被認證者）
保存資訊 (K,Nn,An)
伺服器（認證者）
保存資訊 (ID,K,An)
開始
開始
a←X(ID,S,Nn)
S151
產生亂數 Nn+1 並予以保存
S152
b←X(ID,S,Nn+1)
B←F(ID,b)
S153
α←B XOR An
β←(B+K) XOR a
S154
傳送 ID,α,β (S155)
S157
B← α XOR An
a← β XOR (B+K)
將 B 予以保存作爲 An+1
S156
S158
否
F(ID,a)=An?
是
S159
S161
傳送錯誤訊息
開始與使用者進行連接
S160
將 B 予以保存作爲 An+1
結束
結束

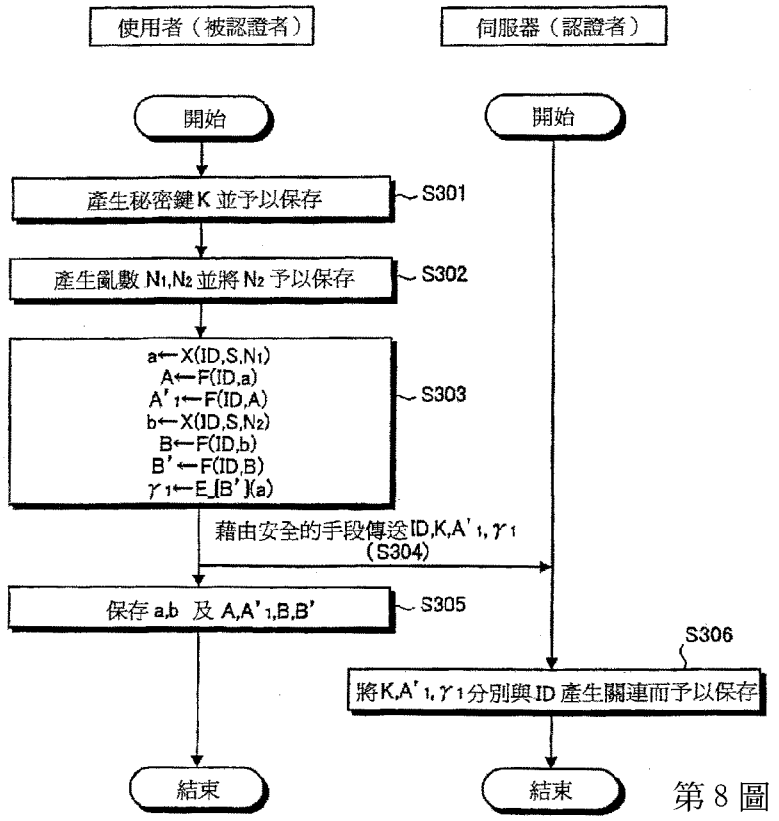
第 5 圖


使用者（被認證者）
伺服器（認證者）
開始
開始
產生秘密鍵K 並予以保存
S201
產生亂數 N1,N2 並將 N2 予以保存
S202
a←X(ID,S,N1)
A1←F(ID,a)
b←X(ID,S,N2)
B←F(ID,b)
γ1←E_{B}(a)
S203
藉由安全的手段傳送 ID,K,A1, γ1
(S204)
保存 a,b 及 A1,B
S205
S206
將K,A1, γ1分別與ID產生關連而予以保存
結束
結束

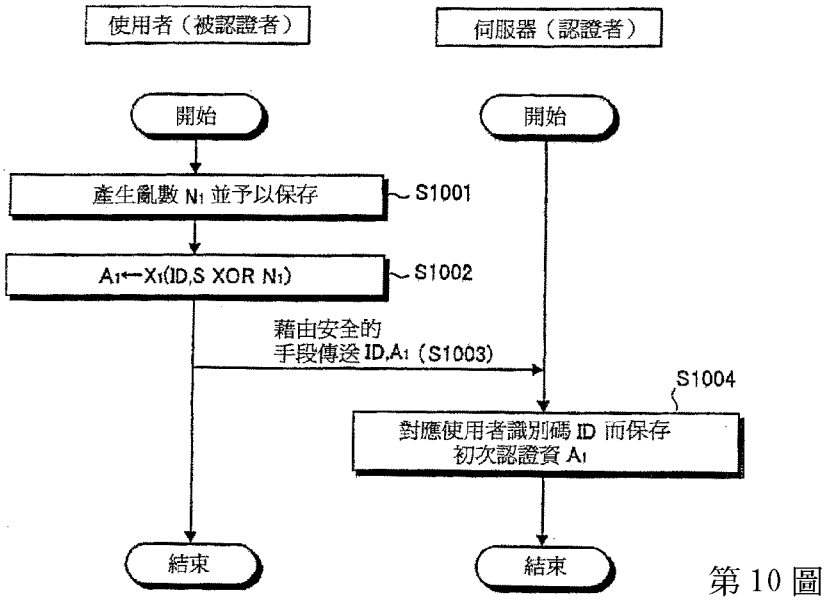
第 6 圖


使用者（被認證者）
保存資訊 (K,Nn+1,An,B,a,b)
伺服器（認證者）
保存資訊 (K,An, γ n)
開始
開始
計算 b
S251
S252
否
是否與所保存的
b相等？
是
產生亂數Nn+2 並予以保存
S253
c←X(ID,S,Nn+2)
C←F(ID,c)
S254
α←B XOR An
β←(B+K) XOR a
γ n+1←E_[C](b)
S255
傳送 ID, α , β , γ n+1 (S256)
S258
B← α XOR An
a← β XOR (B+K)
S257
將 c,C 予以保存作爲 b,B
S259
否
F(ID,a)=An？
是
S260
否
D_[B](γ n)=a？
S263
傳送錯誤
訊息
S261
是
開始與使用者進行連接
S262
將 B 予以保存作爲 An+1
結束
結束

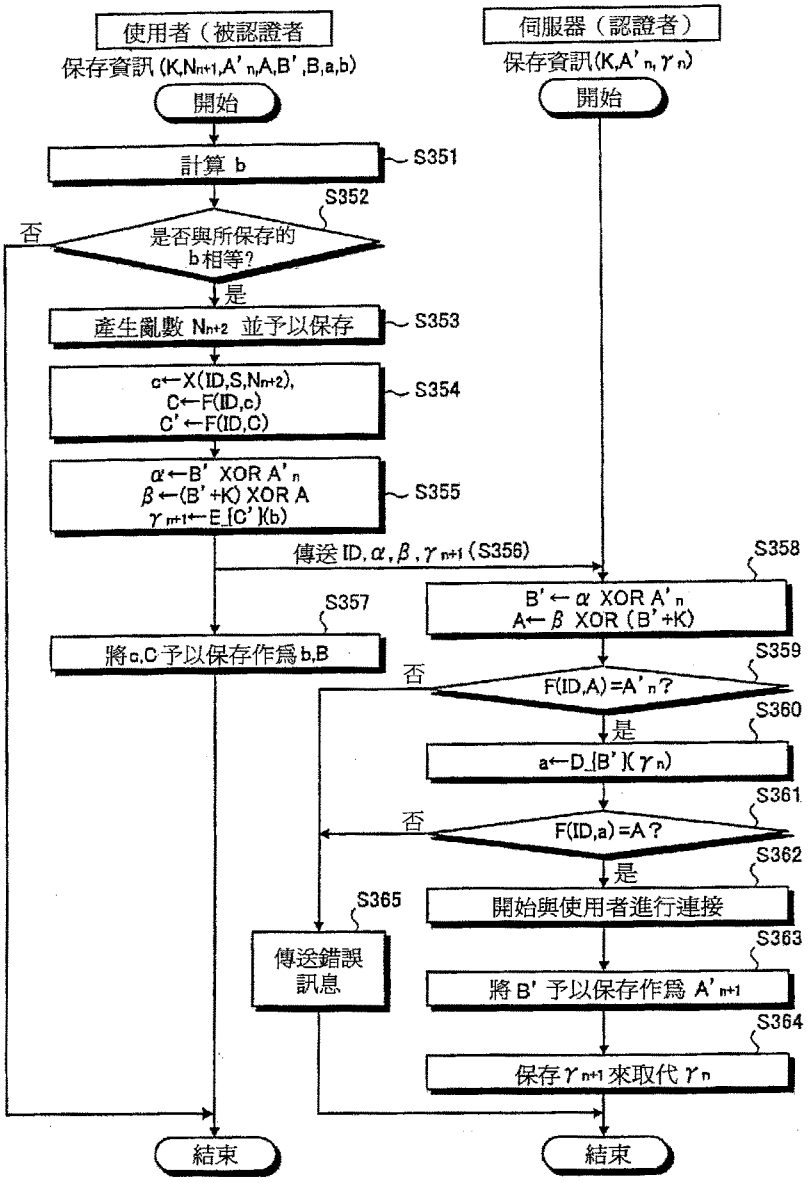
第 7 圖


使用者（被認證者）
伺服器（認證者）
開始
開始
產生秘密鍵K 並予以保存
S301
產生亂數 N1,N2 並將 N2 予以保存
S302
a←X(ID,S,N1)
A←F(ID,a)
A'1←F(ID,A)
b←X(ID,S,N2)
B←F(ID,b)
B'←F(ID,B)
γ1←E_[B']K(a)
S303
藉由安全的手段傳送ID,K,A'1,γ1
(S304)
保存 a,b 及 A,A'1,B,B'
S305
S306
將K,A'1,γ1分別與ID 產生關連而予以保存
結束
結束

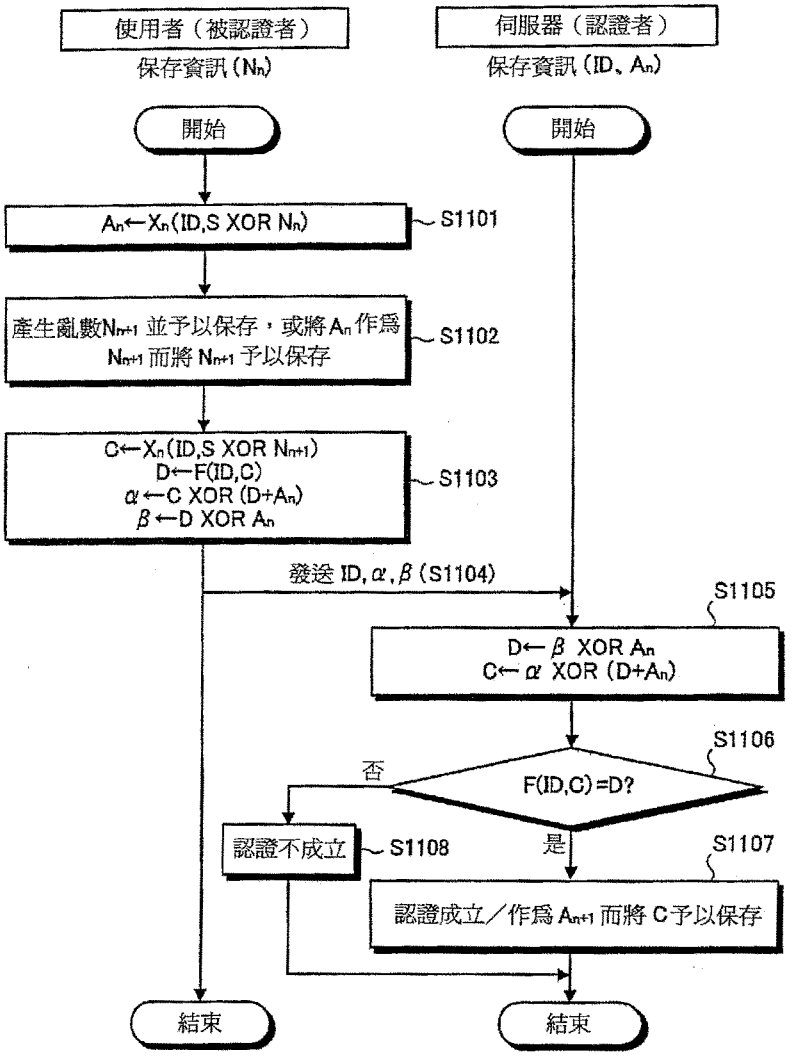
第 8 圖


使用者（被認證者）
伺服器（認證者）
開始
開始
產生亂數 N1 並予以保存
S1001
A1←X1(ID,S XOR N1)
S1002
藉由安全的
手段傳送 ID,A1 (S1003)
S1004
對應使用者識別碼 ID 而保存
初次認證資 A1
結束
結束

第 10 圖


使用者（被認證者）
保存資訊 (K,Nn+1,A'n,A,B',B,a,b)
開始
計算 b
S351
S352
是否與所保存的 b相等?
否
是
產生亂數 Nn+2 並予以保存
S353
c←X(ID,S,Nn+2),
C←F(ID,c)
C'←F(ID,C)
S354
α←B' XOR A'n
β←(B'+K) XOR A
γn+1←E_[C'](b)
S355
傳送 ID,α,β,γn+1 (S356)
S357
將c,C予以保存作爲b,B
伺服器（認證者）
保存資訊(K,A'n,γn)
開始
S358
B'←α XOR A'n
A←β XOR (B'+K)
S359
F(ID,A)=A'n?
否
是
S360
a←D_[B'](γn)
S361
F(ID,a)=A?
否
是
S362
開始與使用者進行連接
S363
將 B' 予以保存作爲 A'n+1
S364
保存γn+1來取代 γn
S365
傳送錯誤訊息
結束
結束

第 9 圖


使用者（被認證者）
保存資訊（N_n）
伺服器（認證者）
保存資訊（ID、A_n）
開始
開始
$A_n \leftarrow X_n(ID, S \text{ XOR } N_n)$
S1101
產生亂數N_{n+1}並予以保存，或將A_n作爲N_{n+1}而將N_{n+1}予以保存
S1102
$C \leftarrow X_n(ID, S \text{ XOR } N_{n+1})$
$D \leftarrow F(ID, C)$
$\alpha \leftarrow C \text{ XOR } (D+A_n)$
$\beta \leftarrow D \text{ XOR } A_n$
S1103
發送 ID, α, β (S1104)
S1105
$D \leftarrow \beta \text{ XOR } A_n$
$C \leftarrow \alpha \text{ XOR } (D+A_n)$
S1106
否
$F(ID, C) = D?$
是
認證不成立
S1108
S1107
認證成立／作爲A_{n+1}而將C予以保存
結束
結束

第 11 圖