(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107548542 A
(43)申请公布日 2018.01.05

(21)申请号 201680002496.3

(22)申请日 2016.05.12

(30)优先权数据
10-2016-0052423 2016.04.28 KR

(85)PCT国际申请进入国家阶段日
2017.03.03

(86)PCT国际申请的申请数据
PCT/KR2016/005008 2016.05.12

(87)PCT国际申请的公布数据
WO2017/188497 KO 2017.11.02

(71)申请人 森斯通株式会社
地址 韩国首尔

(72)发明人 刘昌训 许云宁 金珉奎 徐佑蓉

(74)专利代理机构 北京青松知识产权代理事务所(特殊普通合伙) 11384
代理人 郑青松

(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/31(2006.01)
H04L 9/08(2006.01)

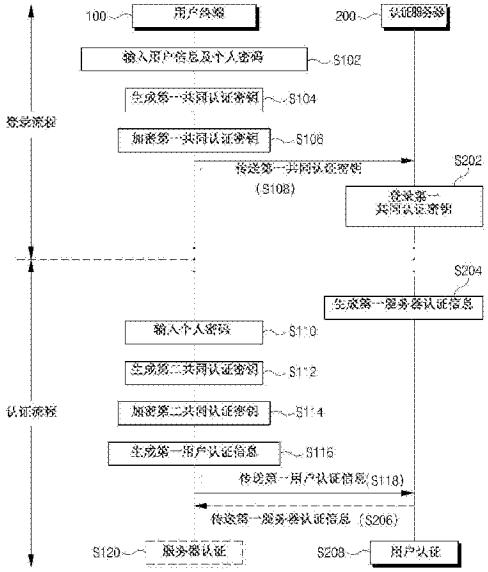
权利要求书7页 说明书30页 附图14页

(54)发明名称

经强化完整性及安全性的用户认证方法

(57)摘要

本发明涉及经强化完整性及安全性的用户认证方法，本发明的用户认证方法包括：第一步骤，如果开始用户登录所需流程，则用户终端执行第一次变换，生成第一共同认证密钥，执行第二次变换，把加密的第一共同认证密钥提供给认证服务器，所述认证服务器登录所述加密的第一共同认证密钥；第二步骤，所述认证服务器生成第一服务器认证密钥，对所述第一服务器认证密钥执行OTP演算，生成第一服务器认证信息；第三步骤，如果开始认证流程，则用户终端执行第一次变换，生成第二共同认证密钥，执行第二次变换，生成加密的第二共同认证密钥，生成第一用户认证密钥，对所述第一用户认证密钥执行OTP演算，生成第一用户认证信息；第四步骤，根据所述第一服务器认证信息与所述第一用户认证信息的一致与否，执行用户认证或执行判断所述认证服务器的真伪与否的认证服务器认证。



CN 107548542 A

1.一种用户认证方法，在利用用户终端和认证服务器的用户认证方法中，其特征在于，包括：

第一步骤，如果用户输入用户登录所需的个人密码，则所述用户终端组合所述个人密码及所述用户终端的机械性固有密钥，执行使用了单向性函数的第一次变换，生成第一共同认证密钥，执行对所述第一共同认证密钥利用加密密钥进行加密的第二次变换，将加密的第一共同认证密钥提供给所述认证服务器，所述认证服务器将所述加密的第一共同认证密钥匹配于用户信息并进行登录；

第二步骤，所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一服务器认证密钥，对所述第一服务器认证密钥或作为所述第一服务器认证密钥变换值的第二服务器认证密钥执行OTP演算，生成第一服务器认证信息；

第三步骤，如果为了认证而从用户输入所述个人密码，则所述用户终端组合所述个人密码及所述用户终端的机械性固有密钥，执行使用了单向性函数的第一次变换，实时生成第二共同认证密钥，执行对所述第二共同认证密钥利用所述加密密钥进行加密的第二次变换，生成加密的第二共同认证密钥，以从所述认证服务器预先提供的认证机构固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一用户认证密钥，对所述第一用户认证密钥或作为所述第一用户认证密钥变换值的第二用户认证密钥执行OTP演算，生成第一用户认证信息；以及

第四步骤，根据所述第一服务器认证信息与所述第一用户认证信息的一致与否，执行用户认证或执行判断所述认证服务器真伪与否的认证服务器认证。

2.根据权利要求1所述的用户认证方法，其特征在于，

在所述第一共同认证密钥或所述第二共同认证密钥中，还添加所述用户终端中安装的专用应用程序的固有密钥作为构成要素。

3.根据权利要求1所述的用户认证方法，其特征在于，

所述第四步骤包括：

认证服务器认证步骤，所述用户终端比较所述第一用户认证信息和从所述认证服务器传送的所述第一服务器认证信息，判别所述认证服务器的真伪与否；或

用户认证步骤，所述认证服务器比较所述第一服务器认证信息和从所述用户终端传送的第一用户认证信息，执行用户认证。

4.根据权利要求1所述的用户认证方法，其特征在于，

所述第二步骤包括：

所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成所述第一服务器认证密钥的步骤；

所述认证服务器生成从所述第一服务器认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第二服务器认证密钥的步骤；以及

所述认证服务器对所述第二服务器认证密钥执行OTP演算，生成所述第一服务器认证信息的步骤；

所述第三步骤包括：

如果生成所述加密的第二共同认证密钥，则所述用户终端以从所述认证服务器预先提

供的认证机构固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成所述第一用户认证密钥的步骤；

生成从所述第一用户认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第二用户认证密钥的步骤；以及

所述用户终端对所述第二用户认证密钥执行OTP演算，生成所述第一用户认证信息的步骤。

5.根据权利要求1所述的用户认证方法，其特征在于，

在所述第三步骤与第四步骤之间或在所述第四步骤之后，还包括：

所述用户终端以利用解密密钥进行解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素，执行使用了单向性函数的变换，生成第三用户认证密钥的步骤；

所述用户终端对所述第三用户认证密钥执行OTP演算，生成第二用户认证信息的步骤；

所述用户终端将所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤；

所述认证服务器将所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥，以所述第一共同认证密钥和从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息为构成要素，执行使用了单向性函数的变换，生成第三服务器认证密钥的步骤；以及

对所述第三服务器认证密钥执行OTP演算，生成第二服务器认证信息的步骤；

在所述第四步骤之后，还包括：

判断所述第二用户认证信息与所述第二服务器认证信息的一致与否，执行用户认证的步骤。

6.根据权利要求4所述的用户认证方法，其特征在于，

在所述第三步骤与第四步骤之间或在所述第四步骤之后，包括：

所述用户终端以利用解密密钥进行解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素，执行使用了单向性函数的变换，生成第三用户认证密钥的步骤；

所述用户终端生成从所述第三用户认证密钥，通过时间提取值发生器，使用时间信息，根据既定基准提取的第四用户认证密钥的步骤；

对所述第四用户认证密钥执行OTP演算，生成所述第二用户认证信息的步骤；

所述用户终端将所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤；

所述认证服务器将所述加密的第一共同认证密钥使用所述解密密钥解密为第一共同认证密钥，以从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息和所述第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第三服务器认证密钥的步骤；

所述认证服务器生成从所述第三服务器认证密钥，通过时间提取值发生器，使用时间信息，根据既定基准提取的第四服务器认证密钥的步骤；以及

对所述第四服务器认证密钥执行OTP演算，生成所述第二服务器认证信息的步骤；

在所述第四步骤之后，还包括：

判断所述第二用户认证信息与所述第二服务器认证信息的一致与否，执行用户认证的步骤。

7.根据权利要求5所述的用户认证方法，其特征在于，

所述第三步骤还包括：所述用户测定作为按1/n秒单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤，

在所述用户终端生成所述第三用户认证密钥时，还添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素，

在所述认证服务器生成所述第三服务器认证密钥时，还添加所述间隙时间值或所述间隙时间密钥作为构成要素。

8.根据权利要求6所述的用户认证方法，其特征在于，

所述第三步骤还包括：所述用户测定作为按1/n秒单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤，

在所述用户终端生成所述第三用户认证密钥时，还添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素，

在所述认证服务器生成所述第三服务器认证密钥时，还添加所述间隙时间值或所述间隙时间密钥作为构成要素。

9.根据权利要求5或6所述的用户认证方法，其特征在于，

所述单向性函数包括哈希函数作为将具有任意长度的数据映射到固定长度数据的函数，

用于所述第二次变换的加密，使用加密密钥和解密密钥相同的对称密钥加密方式。

10.根据权利要求5或6所述的用户认证方法，其特征在于，

在所述用户终端或所述认证服务器传送的包括认证信息或认证密钥的传送对象数据中，添加传送用于数据完整性验证的验证密钥，

所述验证密钥添加针对传送对象数据执行OTP演算的第一OTP演算值，

在所述用户终端或所述认证服务器接收所述数据时，比较对接收的数据执行OTP演算的第二OTP演算值和所述验证密钥，执行完整性验证。

11.根据权利要求6所述的用户认证方法，其特征在于，

所述认证服务器在在既定时间内传送了多个所述第一服务器认证信息的情况下，要求所述用户终端添加手动输入所述第二用户认证信息，如果所述第二用户认证信息通过手动输入而传送，则比较手动输入的第二用户认证信息和所述第二服务器认证信息，执行用户认证。

12.根据权利要求6或11所述的用户认证方法，其特征在于，还包括：

所述认证服务器向所述用户终端请求第三用户认证信息的步骤；

如果所述第三用户认证信息通过所述用户终端而被传送，则所述认证服务器判断所述第三用户认证信息与所述第三服务器认证信息的一致与否，执行用户认证的步骤；

所述第三用户认证信息由所述用户终端以所述认证机构的固有密钥和所述第四用户认证密钥为构成要素，执行使用了单向性函数的变换，生成第五用户认证密钥，对所述第五用户认证密钥执行OTP演算而生成，

所述第三服务器认证信息由所述认证服务器以所述认证机构的固有密钥和所述第四服务器认证密钥为构成要素，执行使用了单向性函数的变换，生成第五服务器认证密钥，对所述第五服务器认证密钥执行OTP演算而生成。

13.根据权利要求5或6所述的用户认证方法，其特征在于，

所述用户终端在执行所述第一步骤至所述第四步骤的认证流程中感知包括黑客攻击的攻击征兆，当感知攻击征兆时，生成用于强制中断认证流程的强制中断信号并传送给所述认证服务器，由此，强制中断认证流程。

14.一种用户认证方法，在使用用户终端和认证服务器的用户认证方法中，其特征在于，包括：

第一步骤，如果用户开始用户登录所需的流程，则所述用户终端以所述用户终端的机械性固有密钥为构成要素，执行使用了单向性函数的第一次变换，生成第一共同认证密钥，执行对所述第一共同认证密钥加密的第二次变换，将加密的第一共同认证密钥提供给所述认证服务器，所述认证服务器将所述加密的第一共同认证密钥匹配于用户信息进行登录；

第二步骤，所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一服务器认证密钥，对所述第一服务器认证密钥或作为所述第一服务器认证密钥变换值的第二服务器认证密钥执行OTP演算，生成第一服务器认证信息；

第三步骤，如果用户为了认证而开始认证流程，则所述用户终端以所述用户终端的机械性固有密钥为构成要素，执行使用了单向性函数的第一次变换，实时生成第二共同认证密钥，执行对所述第二共同认证密钥加密的第二次变换，生成加密的第二共同认证密钥，以从所述认证服务器预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一用户认证密钥，对所述第一用户认证密钥或作为所述第一用户认证密钥变换值的第二用户认证密钥执行OTP演算，生成第一用户认证信息；以及

第四步骤，根据所述第一服务器认证信息与所述第一用户认证信息的一致与否，执行用户认证或执行判断所述认证服务器的真伪与否的认证服务器认证。

15.根据权利要求14所述的用户认证方法，其特征在于，

用于加密所述第一共同认证密钥的第一加密密钥及用于加密所述第二共同认证密钥的第二加密密钥，借助于以用户输入的个人密码为构成要素，执行使用了单向性函数的变换而生成，或随机生成。

16.根据权利要求15所述的用户认证方法，其特征在于，

所述第一加密密钥及所述第二加密密钥借助于添加所述用户终端的机械性固有密钥作为构成要素，组合所述个人密码和所述用户终端的机械性固有密钥，执行使用了单向性函数的变换而生成。

17.根据权利要求16所述的用户认证方法，其特征在于，

在所述第一共同认证密钥、所述第二共同认证密钥、所述第一加密密钥及所述第二加密密钥各自生成时，添加所述用户终端中安装的专用应用程序的固有密钥作为构成要素。

18.根据权利要求15所述的用户认证方法，其特征在于，

所述第二步骤包括：

所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成所述第一服务器认证密钥的步骤；

所述认证服务器生成从所述第一服务器认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第二服务器认证密钥的步骤；以及

所述认证服务器对所述第二服务器认证密钥执行OTP演算，生成所述第一服务器认证信息的步骤；

所述第三步骤包括：

如果生成所述加密的第二共同认证密钥，则所述用户终端以从所述认证服务器预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一用户认证密钥的步骤；

生成从所述第一用户认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第二用户认证密钥的步骤；以及

所述用户终端对所述第二用户认证密钥执行OTP演算，生成所述第一用户认证信息的步骤。

19.根据权利要求15所述的用户认证方法，其特征在于，

在所述第三步骤与第四步骤之间或在所述第四步骤之后，还包括：

所述用户终端以利用解密密钥而解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素，执行使用了单向性函数的变换，生成第三用户认证密钥的步骤；

所述用户终端对所述第三用户认证密钥执行OTP演算，生成第二用户认证信息的步骤；

所述用户终端将所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤；

所述认证服务器将所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥，以所述第一共同认证密钥和从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息为构成要素，执行使用了单向性函数的变换，生成第三服务器认证密钥的步骤；以及

对所述第三服务器认证密钥执行OTP演算，生成第二服务器认证信息的步骤；

在所述第四步骤之后，还包括：

判断所述第二用户认证信息和所述第二服务器认证信息的一致与否，执行用户认证的步骤。

20.根据权利要求18所述的用户认证方法，其特征在于，

在所述第三步骤与第四步骤之间或在所述第四步骤之后，包括：

所述用户终端以利用解密密钥而解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素，执行使用了单向性函数的变换，生成第三用户认证密钥的步骤；

所述用户终端生成从所述第三用户认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第四用户认证密钥的步骤；

对所述第四用户认证密钥执行OTP演算，生成所述第二用户认证信息的步骤；

所述用户终端将所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步

骤；

所述认证服务器将所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥，以从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息和所述第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第三服务器认证密钥的步骤；

所述认证服务器生成从所述第三服务器认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第四服务器认证密钥的步骤；以及

对所述第四服务器认证密钥执行OTP演算，生成所述第二服务器认证信息的步骤；

在所述第四步骤之后，还包括：

判断所述第二用户认证信息和所述第二服务器认证信息的一致与否，执行用户认证的步骤。

21.根据权利要求19所述的用户认证方法，其特征在于，

所述第三步骤还包括：所述用户测定作为按1/n秒单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤，

在所述用户终端生成所述第三用户认证密钥时，还添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素，

在所述认证服务器生成所述第三服务器认证密钥时，还添加所述间隙时间值或所述间隙时间密钥作为构成要素。

22.根据权利要求20所述的用户认证方法，其特征在于，

所述第三步骤还包括：所述用户测定作为按1/n秒单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤，

在所述用户终端生成所述第三用户认证密钥时，还添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素，

在所述认证服务器生成所述第三服务器认证密钥时，还添加所述间隙时间值或所述间隙时间密钥作为构成要素。

23.根据权利要求14或15所述的用户认证方法，其特征在于，

在所述用户终端或所述认证服务器传送的包括认证信息或认证密钥的传送对象数据中，添加传送用于数据完整性验证的验证密钥，

所述验证密钥添加针对传送对象数据执行OTP演算的第一OTP演算值，

在所述用户终端或所述认证服务器接收所述数据时，比较对接收的数据执行OTP演算的第二OTP演算值和所述验证密钥，执行完整性验证。

24.根据权利要求20所述的用户认证方法，其特征在于，

所述认证服务器在在既定时间内传送了多个所述第一服务器认证信息的情况下，要求所述用户终端添加手动输入所述第二用户认证信息，如果所述第二用户认证信息通过手动输入而传送，则比较手动输入的第二用户认证信息和所述第二服务器认证信息，执行用户认证。

25.根据权利要求20或24所述的用户认证方法，其特征在于，还包括：

所述认证服务器向所述用户终端请求第三用户认证信息的步骤；

如果所述第三用户认证信息通过所述用户终端而被传送，则所述认证服务器判断所述

第三用户认证信息与所述第三服务器认证信息的一致与否，执行用户认证的步骤；

所述第三用户认证信息由所述用户终端以所述认证机构的固有密钥和所述第四用户认证密钥为构成要素，执行使用了单向性函数的变换，生成第五用户认证密钥，对所述第五用户认证密钥执行OTP演算而生成，

所述第三服务器认证信息由所述认证服务器以所述认证机构的固有密钥和所述第四服务器认证密钥为构成要素，执行使用了单向性函数的变换，生成第五服务器认证密钥，对所述第五服务器认证密钥执行OTP演算而生成。

26.根据权利要求14或15所述的用户认证方法，其特征在于，

所述用户终端在执行所述第一步骤至所述第四步骤的认证流程中感知包括黑客攻击的攻击征兆，当感知攻击征兆时，生成用于强制中断认证流程的强制中断信号并传送给所述认证服务器，由此，强制中断认证流程。

经强化完整性及安全性的用户认证方法

技术领域

[0001] 本发明涉及过强化完整性及安全性的用户认证方法，更具体而言，涉及一种在公开网络上从根源上切断个人信息泄露，摆脱黑客攻击危险，强化了安全性、能够验证传送数据的完整性、强化了完整性及安全性的用户认证方法用户认证方法。

背景技术

[0002] 在现代社会，与面对面接触相比，通过在线环境实现金融交易或需要各种用户认证的业务正在普遍化。与面对面接触相比，在线上的用户认证需要更慎重地接入，大部分情形要求在用户终端中安装包括ActiveX及键盘安全程序等的各种安全程序或控制程序，通过电子证书或安全卡、OTP装置等安全装置来强化安全性，应对信息泄露。

[0003] 作为代表性用户认证方法之一的OTP(One Time Password，一次性密码)装置，预先向用户提供内置有固有密钥的OTP装置，当用户接入电子金融交易网，向认证服务器(金融机构的服务器)要求认证时，以所述固有密钥作为演算密钥，根据与当前时间关联的随机数，生成OTP号码，用户以生成的OTP号码为密码，手动输入并传送给认证服务器，以该方式认证为真正的用户。

[0004] 但是，在用户与多家金融机构交易的情况下，需分别具备各金融机构提供的多个OTP认证装置，因此，消费者需另行购买各金融机构的OTP认证装置，存在需要持有多个OTP认证装置的不便，还存在需在多个OTP认证装置中逐一查找特定金融机构用认证装置的不便。

[0005] 另外，由于用户无法任意更换OTP装置的固有密钥，因而当OTP装置丢失时，需直接访问金融机构并重新获得发放等，不便较多。而且，金融机构在客户的OTP装置的固有密钥泄露时，向所有顾客重新发放OTP装置等，需要花费巨大费用和时间，存在这样的问题。

[0006] 另一方面，在用户通过指定的密码进行认证或登录的情况下，相关服务器等需登录、存储及管理用户的密码，从用户立场而言，需认知密码，要求定期变更，以防泄露，因而存在管理不便的问题。

[0007] 而且，随着黑客技术的发展，因屏幕捕获、肩窥攻击(shoulder surfing attack)、屏幕监视等屏幕黑客技术或因PC中安装的软件(spyware)等而导致电子证书或密码等泄露等，信息泄露多种多样，即使是加密的密码，对于专业的黑客而言，经过某种程度的努力也可能解密，因此就用户认证所需的流程而言，在对用户追求便利性的同时，还需要强化安全性。另外，在传送过程中，也需要验证错误，强化完整性。

[0008] 【现有技术文献】

[0009] 【专利文献】

[0010] (专利文献1)大韩民国注册专利第10-1270941号(2013.05.29.)

发明内容

[0011] 本发明要解决的技术问题

[0012] 因此，本发明的目的在于，提供一种能够克服所述以往问题的经强化完整性及安全性的用户认证方法。

[0013] 本发明的另一目的在于，提供一种用户认证流程简便、能够强化安全性、能够验证完整性的经强化完整性及安全性的用户认证方法。

[0014] 本发明的另一目的在于，提供一种即使在公开的网络环境下也能够没有信息泄露危险地便利应用的经强化完整性及安全性的用户认证方法。

[0015] 本发明的又一目的在于，提供一种用户可以判断认证所需的认证机构、认证服务器等的真伪与否的经强化完整性及安全性的用户认证方法。

[0016] 本发明的又一目的在于，提供一种不用在认证机构或认证服务器上管理用户的密码，也能够进行认证，并且能够利用与时间相联系的多重要素而经强化完整性及安全性的用户认证方法。

[0017] 技术方案

[0018] 根据旨在达成所述技术课题一部分的本发明的具体化，本发明的利用用户终端和认证服务器的用户认证方法包括：第一步骤，如果用户输入用户登录所需的个人密码，则所述用户终端组合所述个人密码及所述用户终端的机械性固有密钥，执行使用了单向性函数的第一次变换，生成第一共同认证密钥，执行把所述第一共同认证密钥利用加密密钥进行加密的第二次变换，把加密的第一共同认证密钥提供给所述认证服务器，所述认证服务器把所述加密的第一共同认证密钥匹配于用户信息并进行登录；第二步骤，所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一服务器认证密钥，对所述第一服务器认证密钥或作为所述第一服务器认证密钥变换值的第二服务器认证密钥执行OTP(One Time Password)演算，生成第一服务器认证信息；第三步骤，如果为了认证而从用户输入所述个人密码，则所述用户终端组合所述个人密码及所述用户终端的机械性固有密钥，执行使用了单向性函数的第一次变换，实时生成第二共同认证密钥，执行把所述第二共同认证密钥利用所述加密密钥进行加密的第二次变换，生成加密的第二共同认证密钥，以从所述认证服务器预先提供的认证机构固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一用户认证密钥，对所述第一用户认证密钥或作为所述第一用户认证密钥变换值的第二用户认证密钥执行OTP(One Time Password)演算，生成第一用户认证信息；第四步骤，根据所述第一服务器认证信息与所述第一用户认证信息的一致与否，执行用户认证或执行判断所述认证服务器真伪与否的认证服务器认证。

[0019] 在所述第一共同认证密钥或所述第二共同认证密钥上，还可以添加在所述用户终端上安装的专用应用程序的固有密钥作为构成要素。

[0020] 所述第四步骤可以包括：服务器认证步骤或用户认证步骤，所述服务器认证步骤为，所述用户终端比较所述第一用户认证信息和从所述认证服务器传送的所述第一服务器认证信息，判别所述认证服务器的真伪与否的步骤；所述用户认证步骤为，所述认证服务器比较所述第一服务器认证信息和从所述用户终端传送的第一用户认证信息，执行用户认证的步骤。

[0021] 所述第二步骤可以包括：所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成所述第一服务器

认证密钥的步骤;所述认证服务器生成从所述第一服务器认证密钥,通过时间提取值发生器,利用时间信息,根据既定基准提取的第二服务器认证密钥的步骤;所述认证服务器对所述第二服务器认证密钥执行OTP(One Time Password)演算,生成所述第一服务器认证信息的步骤;所述第三步骤可以包括:如果生成所述加密的第二共同认证密钥,则所述用户终端以从所述认证服务器预先提供的认证机构固有密钥和所述加密的第二共同认证密钥为构成要素,执行使用了单向性函数的变换,生成所述第一用户认证密钥的步骤;生成从所述第一用户认证密钥,通过时间提取值发生器,利用时间信息,根据既定基准提取的第二用户认证密钥的步骤;所述用户终端对所述第二用户认证密钥执行OTP(One Time Password)演算,生成所述第一用户认证信息的步骤。

[0022] 在所述第三步骤与第四步骤之间或在所述第四步骤之后,还可以包括:所述用户终端以利用解密密钥进行解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素,执行使用了单向性函数的变换,生成第三用户认证密钥的步骤;所述用户终端对所述第三用户认证密钥执行OTP(One Time Password)演算,生成第二用户认证信息的步骤;所述用户终端把所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤;所述认证服务器把所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥,以所述第一共同认证密钥和从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息为构成要素,执行使用了单向性函数的变换,生成第三服务器认证密钥的步骤;对所述第三服务器认证密钥执行OTP(One Time Password)演算,生成第二服务器认证信息的步骤;在所述第四步骤之后,还可以包括:判断所述第二用户认证信息与所述第二服务器认证信息的一致与否,执行用户认证的步骤。

[0023] 在所述第三步骤与第四步骤之间或在所述第四步骤之后,可以包括:所述用户终端以利用解密密钥进行解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素,执行使用了单向性函数的变换,生成第三用户认证密钥的步骤;所述用户终端生成从所述第三用户认证密钥,通过时间提取值发生器,利用时间信息,根据既定基准提取的第四用户认证密钥的步骤;对所述第四用户认证密钥执行OTP(One Time Password)演算,生成所述第二用户认证信息的步骤;可以包括:所述用户终端把所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤;所述认证服务器把所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥,以从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息和所述第一共同认证密钥为构成要素,执行使用了单向性函数的变换,生成第三服务器认证密钥的步骤;所述认证服务器生成从所述第三服务器认证密钥,通过时间提取值发生器,利用时间信息,根据既定基准提取的第四服务器认证密钥的步骤;对所述第四服务器认证密钥执行OTP(One Time Password)演算,生成所述第二服务器认证信息的步骤;在所述第四步骤之后,还可以包括:判断所述第二用户认证信息与所述第二服务器认证信息的一致与否,执行用户认证的步骤。

[0024] 所述第三步骤还可以包括:所述用户测定作为按1/n(n为任意的正实数)秒(second)单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间差值并传送给所述认证服务器的步骤;在所述用户终端生成所述第三用户认证密钥时,还可以添

加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素;在所述认证服务器生成所述第三服务器认证密钥时,还可以添加所述间隙时间值或所述间隙时间密钥作为构成要素。

[0025] 所述第三步骤还可以包括:所述用户测定作为按1/n(n为任意的正实数)秒(second)单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤;在所述用户终端生成所述第三用户认证密钥时,还可以添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素;在所述认证服务器生成所述第三服务器认证密钥时,还可以添加所述间隙时间值或所述间隙时间密钥作为构成要素。

[0026] 所述单向性函数可以包括哈希(HASH)函数,作为把具有任意长度的数据映射到固定长度数据的函数,用于所述第二次变换的加密,可以使用加密密钥和解密密钥相同的对称密钥加密方式。

[0027] 在所述用户终端或所述认证服务器传送的包括认证信息或认证密钥的传送对象数据中,可以添加传送用于数据完整性验证的验证密钥,所述验证密钥可以添加针对传送对象数据执行OTP(One Time Password)演算的第一OTP演算值,在所述用户终端或所述认证服务器接收所述数据时,可以比较对接收的数据执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥,执行完整性验证。

[0028] 所述认证服务器在既定时间内传送了多个所述第一服务器认证信息的情况下,可以要求所述用户终端添加手动输入的所述第二用户认证信息,如果所述第二用户认证信息通过手动输入而传送,则比较手动输入的第二用户认证信息和所述第二服务器认证信息,执行用户认证。

[0029] 还可以包括:所述认证服务器向所述用户终端请求第三用户认证信息的步骤;如果所述第三用户认证信息通过所述用户终端而传送,则所述认证服务器判断所述第三用户认证信息与所述第三服务器认证信息的一致与否,执行用户认证的步骤;所述第三用户认证信息可以由所述用户终端以所述认证机构的固有密钥和所述第四用户认证密钥为构成要素,执行使用了单向性函数的变换,生成第五用户认证密钥,对所述第五用户认证密钥执行OTP(One Time Password)演算而生成;所述第三服务器认证信息可以由所述认证服务器以所述认证机构的固有密钥和所述第四服务器认证密钥为构成要素,执行使用了单向性函数的变换,生成第五服务器认证密钥,对所述第五服务器认证密钥执行OTP(One Time Password)演算而生成。

[0030] 所述用户终端可以在执行所述第一步骤至所述第四步骤的认证流程中,感知包括黑客攻击的攻击征兆,当感知攻击征兆时,生成用于强制中断认证流程的强制中断信号并传送给所述认证服务器,由此,强制中断认证流程。

[0031] 根据旨在达成所述技术课题一部分的本发明的另一具体化,本发明的利用用户终端和认证服务器的用户认证方法包括:第一步骤,如果用户开始用户登录所需的流程,则所述用户终端以所述用户终端的机械性固有密钥为构成要素,执行使用了单向性函数的第一次变换,生成第一共同认证密钥,执行对所述第一共同认证密钥加密的第二次变换,把加密的第一共同认证密钥提供给所述认证服务器,所述认证服务器把所述加密的第一共同认证密钥匹配于用户信息进行登录;第二步骤,所述认证服务器以内置的认证机构的固有密钥

和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一服务器认证密钥，对所述第一服务器认证密钥或作为所述第一服务器认证密钥变换值的第二服务器认证密钥执行OTP(One Time Password)演算，生成第一服务器认证信息；第三步骤，如果用户为了认证而开始认证流程，则所述用户终端以所述用户终端的机械性固有密钥为构成要素，执行使用了单向性函数的第一次变换，实时生成第二共同认证密钥，执行对所述第二共同认证密钥加密的第二次变换，生成加密的第二共同认证密钥，以从所述认证服务器预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一用户认证密钥，对所述第一用户认证密钥或作为所述第一用户认证密钥变换值的第二用户认证密钥执行OTP(One Time Password)演算，生成第一用户认证信息；第四步骤，根据所述第一服务器认证信息和所述第一用户认证信息的一致与否，执行用户认证或执行判断所述认证服务器的真伪与否的认证服务器认证。

[0032] 用于加密所述第一共同认证密钥的第一加密密钥及用于加密所述第二共同认证密钥的第二加密密钥，可以借助于以用户输入的个人密码为构成要素，执行使用了单向性函数的变换而生成，或随机生成。

[0033] 所述第一加密密钥及所述第二加密密钥可以借助于添加所述用户终端的机械性固有密钥作为构成要素，组合所述个人密码和所述用户终端的机械性固有密钥，执行使用了单向性函数的变换而生成。

[0034] 在所述第一共同认证密钥、所述第二共同认证密钥、所述第一加密密钥及所述第二加密密钥各自生成时，可以添加所述用户终端中安装的专用应用程序的固有密钥作为构成要素。

[0035] 所述第二加密密钥可以利用第三加密密码而加密，所述第三加密密码借助于组合所述个人密码和所述用户终端的机械性固有密钥，执行使用了单向性函数的变换而生成。

[0036] 所述第二步骤可以包括：所述认证服务器以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成所述第一服务器认证密钥的步骤；所述认证服务器生成从所述第一服务器认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第二服务器认证密钥的步骤；所述认证服务器对所述第二服务器认证密钥执行OTP(One Time Password)演算，生成所述第一服务器认证信息的步骤；所述第三步骤可以包括：如果生成所述加密的第二共同认证密钥，则所述用户终端以从所述认证服务器预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第一用户认证密钥的步骤；生成从所述第一用户认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第二用户认证密钥的步骤；所述用户终端对所述第二用户认证密钥执行OTP(One Time Password)演算，生成所述第一用户认证信息的步骤。

[0037] 在所述第三步骤与第四步骤之间或在所述第四步骤之后，还可以包括：所述用户终端以利用解密密钥而解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素，执行使用了单向性函数的变换，生成第三用户认证密钥的步骤；所述用户终端对所述第三用户认证密钥执行OTP(One Time Password)演算，生成第二用户认证信息的步骤；所述用户终端把所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤；所述认证

服务器把所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥，以所述第一共同认证密钥和从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息为构成要素，执行使用了单向性函数的变换，生成第三服务器认证密钥的步骤；对所述第三服务器认证密钥执行OTP(One Time Password)演算，生成第二服务器认证信息的步骤；在所述第四步骤之后，还可以包括：判断所述第二用户认证信息和所述第二服务器认证信息的一致与否，执行用户认证的步骤。

[0038] 在所述第三步骤与第四步骤之间或在所述第四步骤之后，还可以包括：所述用户终端以利用解密密钥而解密的第二共同认证密钥或未加密状态的所述第二共同认证密钥、从所述认证服务器传送的所述第一服务器认证信息或所述第一用户认证信息为构成要素，执行使用了单向性函数的变换，生成第三用户认证密钥的步骤；所述用户终端生成从所述第三用户认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第四用户认证密钥的步骤；对所述第四用户认证密钥执行OTP(One Time Password)演算，生成所述第二用户认证信息的步骤；所述用户终端把所述第二用户认证信息和所述解密密钥传送给所述认证服务器的步骤；所述认证服务器把所述加密的第一共同认证密钥利用所述解密密钥解密为第一共同认证密钥，以从所述用户终端传送的第一用户认证信息或所述第一服务器认证信息和所述第一共同认证密钥为构成要素，执行使用了单向性函数的变换，生成第三服务器认证密钥的步骤；所述认证服务器生成从所述第三服务器认证密钥，通过时间提取值发生器，利用时间信息，根据既定基准提取的第四服务器认证密钥的步骤；对所述第四服务器认证密钥执行OTP(One Time Password)演算，生成所述第二服务器认证信息的步骤；在所述第四步骤之后，还可以包括：判断所述第二用户认证信息和所述第二服务器认证信息的一致与否，执行用户认证的步骤。

[0039] 所述第三步骤还可以包括：所述用户测定作为按1/n(n为任意的正实数)秒(second)单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤；在所述用户终端生成所述第三用户认证密钥时，还可以添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素；在所述认证服务器生成所述第三服务器认证密钥时，还可以添加所述间隙时间值或所述间隙时间密钥作为构成要素。

[0040] 所述第三步骤还可以包括：所述用户测定作为按1/n(n为任意的正实数)秒(second)单位测定的用户输入认证所需个人密码所需要时间的时间值的间隙时间值并传送给所述认证服务器的步骤；在所述用户终端生成所述第三用户认证密钥时，还可以添加所述间隙时间值或作为在所述间隙时间值中根据既定基准提取的数字值的间隙时间密钥作为构成要素；在所述认证服务器生成所述第三服务器认证密钥时，还可以添加所述间隙时间值或所述间隙时间密钥作为构成要素。

[0041] 在所述用户终端或所述认证服务器传送的包括认证信息或认证密钥的传送对象数据中，可以添加传送用于数据完整性验证的验证密钥，所述验证密钥可以添加针对传送对象数据执行OTP(One Time Password)演算的第一OTP演算值，在所述用户终端或所述认证服务器接收所述数据时，可以比较对接收的数据执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证。

[0042] 所述认证服务器在在既定时间内传送了多个所述第一服务器认证信息的情况下，

可以要求所述用户终端添加手动输入所述第二用户认证信息，如果所述第二用户认证信息通过手动输入而传送，则比较手动输入的第二用户认证信息和所述第二服务器认证信息，执行用户认证。

[0043] 还可以包括：所述认证服务器向所述用户终端请求第三用户认证信息的步骤；如果所述第三用户认证信息通过所述用户终端而传送，则所述认证服务器判断所述第三用户认证信息与所述第三服务器认证信息的一致与否，执行用户认证的步骤；所述第三用户认证信息可以由所述用户终端以所述认证机构的固有密钥和所述第四用户认证密钥为构成要素，执行使用了单向性函数的变换，生成第五用户认证密钥，对所述第五用户认证密钥执行OTP(One Time Password)演算而生成；所述第三服务器认证信息可以由所述认证服务器以所述认证机构的固有密钥和所述第四服务器认证密钥为构成要素，执行使用了单向性函数的变换，生成第五服务器认证密钥，对所述第五服务器认证密钥执行OTP(One Time Password)演算而生成。

[0044] 所述用户终端可以在执行所述第一步骤至所述第四步骤的认证流程中，感知包括黑客攻击的攻击征兆，当感知攻击征兆时，生成用于强制中断认证流程的强制中断信号并传送给所述认证服务器，由此，强制中断认证流程。

[0045] 有益效果

[0046] 根据本发明，具有在公开网络上从根源上切断个人信息泄露，摆脱黑客攻击危险，强化安全性，能够验证传送数据完整性的效果。另外，能够检查认证所需的认证服务器、认证机构、Web站点等的真伪与否，具有能够实现可确保完整性及唯一性的用户认证的优点。另外，当生成认证信息时，采取利用之前值执行单方向性变换而生成下个值的链锁(chaining)方式，从而具有能够从根本上防止通过终端的时间操作来预知未来将生成的值等操作的效果。

附图说明

[0047] 图1是本发明实施例的用户认证方法中使用的认证装置的简略概念图；

[0048] 图2是显示本发明第一实施例的用户认证方法的顺序图；

[0049] 图3是显示图2中生成第一共同认证密钥及加密的第一共同认证密钥的过程的框图；

[0050] 图4是显示图2中第一服务器认证信息的生成过程的框图；

[0051] 图5是显示图2中第一用户认证信息的生成过程的框图；

[0052] 图6是显示本发明第二实施例的用户认证方法的顺序图；

[0053] 图7是显示图6中第二用户认证信息的生成过程的框图；

[0054] 图8是显示图6中第二服务器认证信息的生成过程的框图；

[0055] 图9是显示第三服务器认证信息及第三用户认证信息的生成过程的框图；

[0056] 图10是显示本发明第三实施例的用户认证方法中生成第二用户认证信息的过程的框图；

[0057] 图11是显示本发明第三实施例的用户认证方法中第二服务器认证信息的生成过程的框图；

[0058] 图12是显示本发明第四实施例的用户认证方法的顺序图；

[0059] 图13是显示图12中生成第一共同认证密钥及加密的第一共同认证密钥的过程的框图；

[0060] 图14是显示本发明第五实施例的用户认证方法的顺序图。

[0061] 【附图标记】

[0062] 100：用户终端 200：认证服务器

具体实施方式

[0063] 下面，本发明的优选实施例提供用于帮助本发明所属技术领域的技术人员彻底理解本发明，除此之外别无它意，将参照附图进行详细说明。

[0064] 图1是本发明实施例的用户认证方法中使用的认证装置500的简略概念图。

[0065] 如图1所示，本发明实施例的用户认证方法所需的认证装置500具备用户终端100及认证服务器200。

[0066] 所述用户终端100与所述认证服务器200通过有线无线互联网相互连接，在所述用户终端100中，安装有所述认证服务器200提供的用户认证所需专用应用程序(以下称为“专用程序”)。所述用户终端100可以是包括智能手机、平板电脑、PDA等在内的普通技术人员熟知的移动终端。另外，可以包括台式计算机、笔记本电脑、瘦客户机(thin client)用终端、零配置(zero-client)用终端等。其中，瘦客户机(thin client)用终端是指设计成在只搭载CPU、存储器等必需硬件装置的状态下，在通过网络连接的中央服务器中管理所有业务的业务用终端。所述零配置(zero client)用终端是指连存储器等必需的要素也全部去除，不需要PC主机本身，使所有业务在服务器中处理，只执行连接服务器的终端的作用。

[0067] 在本发明中，所述用户终端100是指，用户可以使用的可进行有线无线通信的所有终端，但在需要特别区分的情况下，包括智能手机、平板电脑、PDA等的移动终端指称第一用户终端，台式计算机、笔记本电脑、瘦客户机(thin client)用终端、零配置(zero-client)用终端等指称第二用户终端，且附图符号使用相同的符号“100”。

[0068] 所述认证服务器200一般而言可以包括金融机构等认证机构用于用户认证等认证流程的服务器，可以包括其他普通技术人员熟知的认证服务器。

[0069] 需要指出的是，以下使用的用于认证的认证号码、密码等号码、固有密钥、认证密钥、认证信息等，是由字母、特殊字符、数字、各种符号等组合而成的，不只单纯意味着数字的组合，既可以意味着加密的，也可以意味着未加密的。另外，号码、密钥、信息、值等词尾术语，是为了相互区分而从便利的角度赋予的术语，并非赋予特别的意义。

[0070] 另外，下面所述用户终端100执行的各种结构可以是借助于用户终端100中安装的专用程序而执行的结构。因此，如果说借助于所述用户终端100而执行，那么，也可以意味着借助于所述用户终端100中安装的专用程序而执行。

[0071] 另外，在本发明中，使用了“既定基准”字样的术语，既定基准这一术语，是存在某种基准或预先确定的基准的意义，即使同一术语使用多次，也并非意味着具有相互相同的基准。因此，在本发明中使用的术语“既定基准”，即使在多次使用的情况下，除特别明示为相同基准的情形之外，不意味着相互相同的基准。

[0072] 下面将以用户终端100及认证服务器200为基本构成，说明本发明的用户认证方法的各实施例。

[0073] 图2是显示本发明第一实施例的用户认证方法的顺序图，图3是显示图2中生成第一共同认证密钥及加密的第一共同认证密钥的过程的框图，图4是显示第一服务器认证信息的生成过程的框图，图5是显示第一用户认证信息的生成过程的框图。

[0074] 如图2至图5所示，本发明第一实施例的用户认证方法可以从用户为了通过用户终端100进行用户登录而下载并安装所述专用程序开始。用户登录流程既可以在所述专用程序的安装过程中执行，也可以在所述专用程序的安装之后，通过另外的用户登录过程执行。

[0075] 首先，如果用户开始用户登录所需的流程，用户通过所述用户终端100输入用户信息和个人密码S102，则所述用户终端100利用所述用户终端100的机械性固有密钥，执行使用了单向性函数110的第一次变换，生成第一共同认证密钥S104。

[0076] 其中，所述第一共同认证密钥既可以以所述用户终端100的机械性固有密钥为单独构成要素，通过根据既定基准而生成的演算密钥，通过利用了所述单向性函数110的第一次变换而生成，也可以在所述用户终端100的机械性固有密钥中添加其他构成要素。

[0077] 在本发明的第一实施例的情况下，用户输入的所述个人密码可以添加为生成所述第一共同认证密钥所需的构成要素。

[0078] 其中，所述用户终端100的机械性固有密钥例如可以包括序列号或USIM(全球用户身份模块)号码等，此外，还可以包括用于区分所述用户终端而赋予的各种固有号码、电话号码等。

[0079] 所述单向性函数110可以意味着把任意长度的数据映射、变换成固定长度的数据的函数和被认为不可逆变换，即，无法恢复为原来数据的函数。作为所述单向性函数110，可以包括MD5、SHA、SHA2、scrypt等密码学哈希(HASH)函数、CRC32及CHECKSUM等非密码学哈希函数，可以包括普通技术人员所知的所有单向性函数，所述第一共同认证密钥可以使用在这些单向性函数中选择的某一种单向性函数而生成。

[0080] 所述第一共同认证密钥如图3所示，可以以所述个人密码及所述用户终端100的机械性固有密钥为构成要素，通过根据既定基准而生成的演算密钥进行演算并经第一次变换而生成。在所述第一共同认证密钥中，还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。

[0081] 然后，所述第一共同认证密钥通过加密单元111，通过利用加密密钥进行加密的第二次变换，生成为加密的第一共同认证密钥S106。

[0082] 其中，加密可以使用用于加密的加密密钥和用于解密的解密密钥相同的对称密钥方式，可以使用在Twofish、Serpent、AES、Blowfish、CAST5、RC4、3DES、IDEA、RC6、DES等中选择的加密方式。此外，也可以应用通常技术人员熟知的加密方式。

[0083] 所述用户终端100把所述加密的第一共同认证密钥与所述用户信息一同传送给所述认证服务器200(S108)。

[0084] 所述认证服务器200把所述用户终端100传送的所述加密的第一共同认证密钥匹配于所述用户信息，与所述用户信息一同登录及存储S202。据此执行用户登录流程。所述用户登录流程执行后，所述用户终端100可以删除所述加密的第一共同认证密钥。

[0085] 以往的情形，执行用户登录后，通常在认证服务器中存储个人密码，但本发明第一实施例的情形，不在所述认证服务器200或用户终端100中存储密码，在所述认证服务器200中，只存储所述加密的第一共同认证密钥。

[0086] 因此，在用户忘记或泄露个人密码的情况下，可以通过新登录流程，把包括新密码的加密的第一共同认证密钥传送给所述认证服务器200进行登录，因而强化了安全性。

[0087] 另外具有的优点是，通过使用了单向性函数的第一变换，可以防止个人信息泄露，通过加密的第二变换，在公开的网络环境中，可以无忧虑地不受黑客攻击而安全进行用户认证或认证服务器认证。

[0088] 然后，所述认证服务器200可以组合内置的认证机构的固有密钥和所述加密的第一共同认证密钥而生成第一服务器认证信息S204。

[0089] 所述第一服务器认证信息如图4所示，可以根据两种方式而生成。

[0090] 一种方法如图4的(a)所示，所述认证服务器200可以以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第一服务器认证密钥，对所述第一服务器认证密钥进行OTP(One Time Password)演算，生成以时间值同步的第一服务器认证信息。其中，所述第一服务器认证密钥可以以所述认证机构的固有密钥为演算密钥，针对所述加密的第一共同认证密钥，执行使用了所述单向性函数210的变换而生成。另外，所述第一服务器认证信息可以通过使用了OTP发生器230的OTP演算而生成。

[0091] 另一种方法如图4的(b)所示，所述认证服务器200以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，通过使用了单向性函数210的变换而生成第一服务器认证密钥，生成从所述第一服务器认证密钥，利用时间信息，根据既定基准提取的第二服务器认证密钥。

[0092] 所述第二服务器认证密钥通过另外的时间提取值发生器220而被提取，从而生成，所述第二服务器认证密钥可以意味着从第一服务器认证密钥生成的任意的时间同步值。所述时间提取值发生器220工作原理与普通的OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器220以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器220应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0093] 然后，所述认证服务器200可以通过OTP(One Time Password)发生器230，对所述第二服务器认证密钥执行OTP演算，生成所述第一服务器认证信息。

[0094] 所述第一服务器认证信息可以在用户登录之后，与其他流程无关地独立生成。即，所述第一服务器认证信息只要在所述用户登录之后直至后述第一用户认证信息生成时的时间内生成即可。

[0095] 而且，即使在把所述第一服务器认证信息传送给所述用户终端100的情况下，既可以生成后即时传送，也可以在判断为需要的时间点传送。另外，还可以根据用户终端100的请求而传送。

[0096] 然后，如果用户开始认证流程，用户为了认证在所述用户终端100中而输入所述个人密码S110，则所述用户终端100利用所述用户终端100的机械性固有密钥，执行使用了单向性函数110的第一次变换而生成第二共同认证密钥S112。

[0097] 其中，所述第二共同认证密钥可以以所述用户终端100的机械性固有密钥为单独构成要素，通过根据既定基准生成的演算密钥，通过使用了所述单向性函数110的第一次变换而生成，但是，也可以在所述用户终端100的机械性固有密钥中添加其他构成要素。

[0098] 在本发明的第一实施例情况下，与第一共同认证密钥的生成方式相同，用户输入的所述个人密码可以添加为生成所述第二共同认证密钥所需的构成要素。

[0099] 即，组合所述个人密码及所述用户终端100的机械性固有密钥，执行使用了单向性函数110的第一次变换，生成第二共同认证密钥S112。

[0100] 所述单向性函数110可以使用与生成所述第一共同认证密钥的单向性函数相同的函数，能够以相同方式应用。

[0101] 所述第二共同认证密钥可以与所述第一共同认证密钥的生成方式相同，并且借助于以所述个人密码及所述用户终端100的机械性固有密钥为构成要素，通过根据既定基准而生成的演算密钥进行演算，借助第一次变换而生成。

[0102] 在所述第二共同认证密钥中，还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。这可以与在所述第一共同认证密钥中包含所述专用程序固有密钥作为构成要素的情形对应。

[0103] 然后，所述第二共同认证密钥与第一共同认证密钥的情形相同，通过加密单元111，通过利用所述加密密钥进行加密的第二次变换，生成为加密的第二共同认证密钥S114。加密方式与第一共同认证密钥的情形相同地应用。

[0104] 然后，所述用户终端100利用所述加密的第二共同认证密钥，生成第一用户认证信息S116。对于生成与所述第一用户认证信息对应的所述第一服务器认证信息，已经作过说明。

[0105] 所述第一用户认证信息如图5所示，可以根据两种方式生成。

[0106] 一种方法如图5的(a)所示，所述认证服务器200可以以预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，通过使用了单向性函数110的变换，生成第一用户认证密钥，对所述第一用户认证密钥执行OTP(One Time Password)演算，生成以时间值同步的第一用户认证信息。所述认证机构的固有密钥可以在所述专用程序安装时内置并提供，或在认证流程开始前通过更新等提供。

[0107] 其中，所述第一用户认证密钥可以以所述认证机构的固有密钥为演算密钥，针对所述加密的第二共同认证密钥，执行通过所述单向性函数110的变换而生成。另外，所述第一用户认证信息可以通过利用了OTP发生器130的OTP演算而生成。

[0108] 另一种方法如图5的(b)所示，所述认证服务器200以预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，通过使用了单向性函数110的变换而生成第一用户认证密钥，生成从所述第一用户认证密钥，使用时间信息，根据既定基准提取的第二用户认证密钥。所述认证机构的固有密钥可以在所述专用程序安装时内置并提供，或在认证流程开始前通过更新等而提供。

[0109] 所述第二用户认证密钥通过另外的时间提取值发生器120被提取而生成，所述第二用户认证密钥可以意味着从第一用户认证密钥生成的任意的时间同步值。所述时间提取值发生器120工作原理与普通的OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器120以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器120应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0110] 然后，所述认证服务器200可以通过OTP发生器130，对所述第二服务器认证密钥执

行OTP(One Time Password)演算,生成所述第一服务器认证信息。

[0111] 其中,所述第一用户认证信息的生成方式应与所述第一服务器认证信息的生成方式保持同一性。如果所述第一服务器认证信息以通过图4的(a)说明的方式生成,那么,所述第一用户认证信息也应通过图5的(a)说明的方式生成。另外,单向性函数或OTP演算等也应相互对应地应用。而且,如果所述第一服务器认证信息以通过图4的(b)说明的方式生成,则所述第一用户认证信息也应以通过图5的(b)说明的方式生成。另外,单向性函数或OTP演算、时间值提取等也应对应地应用相同的方式。

[0112] 然后,如果所述第一用户认证信息通过所述用户终端100被传送给所述认证服务器200(S118),则所述认证服务器200根据认证信息的一致与否,即,根据所述第一用户认证信息和所述第一服务器认证信息的一致与否,执行用户认证S208。所述第一用户认证信息既可以由用户手动输入而被传送,也可以使其自动传送,还可以根据用户的传送指示而使其自动传送。

[0113] 其中,所述用户终端100可以使用与所述认证服务器200连接的一个或多个用户终端。例如,可以利用第一用户终端100,进行加密的第一共同认证密钥等的登录流程,利用第二用户终端100进行认证流程,也可以是相反的情形。另外,在认证流程的情况下,第一用户认证信息可以通过所述第一用户终端100生成,所述第一用户认证信息的输入或传送可以通过所述第二用户终端100执行。此外,在多样的流程中,可以使用多个用户终端100。

[0114] 而且,通过用户在用户终端100中比较所述第一用户认证信息和所述第一服务器认证信息,可以确认所述认证服务器200的真伪与否、连接于认证服务器200的接入网页的真伪与否或提供认证服务的服务提供商或认证机构的真伪与否。以往,尽管谎称认证机构并与认证机构的接入网页类似地构成而使用户混同的案例很多,但事实上对此却没有恰当的对策。在本发明中,为了解决这种问题,用户可以确认认证机构(或服务提供商)的真伪与否。

[0115] 为此,当生成所述第一服务器认证信息时,所述认证服务器200将所述第一服务器认证信息通过所述接入网页来显示或传送给所述用户终端100(S206)。所述第一服务器认证信息被显示或传送后,所述用户终端100将其与所述第一用户认证信息进行比较,由此可以进行判别真伪与否的认证服务器认证,即,判别所述认证服务器200是否为真正的认证服务器、所述接入网页是否为真的S120。即,可以确认所述认证服务器200的真伪与否、连接于认证服务器200的接入网页的真伪与否或提供认证服务的服务提供商或认证机构的真伪与否。

[0116] 其中,在所述第一服务器认证信息为在所述加密的第二共同认证密钥生成前预先传送到所述用户终端100的状态的情况下,无需再传送或另行传送,利用预先传送的所述第一服务器认证信息执行认证服务器认证。

[0117] 在本发明的第一实施例中,如果在所述用户终端100中比较所述第一服务器认证信息及所述第一用户认证信息,则通过一致与否,能够进行判别认证机构或认证服务器200真伪与否的认证机构认证或认证服务器认证,如果在所述认证服务器200中比较所述第一服务器认证信息及所述第一用户认证信息,则通过一致与否,能够进行用户认证。

[0118] 其中,所述认证服务器的认证流程S206、S120和所述用户认证流程S118、S208既可以同时执行,也可以在先执行所述认证服务器的认证流程后,如果确认认证,则既可以执行

所述用户认证流程，也可以选择认证服务器认证流程或用户认证流程中某一者并执行。

[0119] 在所述本发明第一实施例的情况下，将所述用户终端100与所述认证服务器200间传送的所有数据可以执行公开密钥方式的加密并传送。

[0120] 在所述本发明第一实施例的情况下，对于执行用户认证而非认证服务器认证的情形，当使用多个用户终端100或同时使用移动终端、台式电脑、平板电脑等而执行用户认证时，由于黑客攻击、异常现象或错误等其他原因，会有在既定时间内向所述认证服务器200传送多个所述第一用户认证信息的情形。

[0121] 在这种情况下，为了确实的认证，所述认证服务器200即使是传送了所述第一用户认证信息的情形，也可以向所述用户终端100请求再传送所述第一用户认证信息，而且可以请求通过手动输入进行再传送，而不是自动传送。此时，第一用户认证信息应显示于所述用户终端100的画面中，以便用户可以手动输入。其中，手动输入可以请求连续执行两次。如果通过手动输入而传送第一用户认证信息，则所述认证服务器200可以比较通过手动输入而传送的第一用户认证信息和所述第一服务器认证信息，执行用户认证。

[0122] 另一方面，当在认证过程中有黑客攻击等攻击征兆时，例如，当载入时间比平常时显著缓慢时，对于在台式电脑中登录的情形，在包括台式电脑的画面和移动终端画面中显示的事先预定值不同的情形在内，感知到普通技术人员熟知的黑客攻击等攻击征兆的情况下，所述用户终端100可以自动或手动向所述认证服务器200传送能够强制中断认证流程的强制中断信号。所述强制中断信号被传送到所述认证服务器200后，所述用户终端100及所述认证服务器200中断所述认证流程，待机直至开始新认证流程时为止。

[0123] 作为另一示例，在感知所述攻击征兆的情况下，所述认证服务器200也可以自我判断，将询问是否强制中断的信号传送给所述用户终端100，对应于用户终端100的响应信号，决定是否强制中断。

[0124] 而且，在包括所述用户终端100与所述认证服务器200间传送的认证信息及认证密钥等的所有传送对象数据中，可以添加用于数据完整性验证的验证密钥。即，可以在传送对象数据中添加所述验证密钥并传送。所述验证密钥可以包括针对各个传送对象数据而执行OTP(One Time Password)演算的第一OTP演算值。

[0125] 而且，在所述用户终端100或所述认证服务器200接收所述数据时，可以比较对接收的数据执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证。

[0126] 例如，在所述用户终端100将所述第一用户认证信息传送给所述认证服务器200的情况下，可以在所述第一用户认证信息中，添加对所述第一用户认证信息进行OTP演算的第一OTP演算值作为验证密钥并传送。此时，所述认证服务器200接收了所述第一用户认证信息时，比较对分离了所述验证密钥的第一用户认证信息执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证，由此能够进行所述第一用户认证信息的完整性验证。

[0127] 在所述本发明第一实施例的情况下，在执行所述用户终端100比较所述第一用户认证信息和所述第一服务器认证信息并进行认证的认证服务器认证的情况下，需要添加的用户认证流程。而且，在执行所述认证服务器200比较所述第一用户认证信息和所述第一服务器认证信息并进行认证的用户认证的情况下，为了进一步确保可靠性，有时需要添加的

用户认证。为此，需要后述的本发明的第二实施例。

[0128] 下面说明本发明的第二实施例。

[0129] 图6是显示本发明第二实施例的用户认证方法的顺序图，

[0130] 图7是显示图6中生成第二用户认证信息的过程的框图，图8是显示第二服务器认证信息的生成过程的框图。

[0131] 如图6至图8所示，本发明第二实施例的用户认证方法全部包括通过本发明第一实施例说明的认证流程，包括在通过所述第一用户认证信息和所述第一服务器认证信息而实现用户认证S208或认证服务器认证S120的状态下添加的过程。因此，通过所述第一用户认证信息和所述第一服务器认证信息而实现用户认证S208或认证服务器认证S120的过程，已通过本发明的第一实施例进行了说明，因而省略详细说明。

[0132] 在生成所述第一服务器认证信息及所述第一用户认证信息并执行所述用户认证S208或认证服务器认证S120之前步骤，或通过所述第一服务器认证信息及所述第一用户认证信息执行所述用户认证S208或认证服务器认证S120之后，所述用户终端100利用所述第一用户认证信息或所述第一服务器认证信息和所述第二共同认证密钥，生成第二用户认证信息S122。

[0133] 作为生成所述第二用户认证信息所需的构成要素，一般使用第一用户认证信息及所述第二共同认证密钥，但在所述认证服务器200传送了所述第一服务器认证信息的情况下，也可以利用所述第一服务器认证信息。这在所述第一服务器认证信息和所述第一用户认证信息为相互相同值的前提下才可能。下面说明利用第一用户认证信息生成所述第二用户认证信息的情形。

[0134] 另外，所述第二共同认证密钥意味着利用解密密钥对所述加密的第二共同认证密钥进行解密的第二共同认证密钥，或指未加密状态的第二共同认证密钥。下面，在第二共同认证密钥没有特别的修饰词的情况下，所述第二共同认证密钥意味着被解密的第二共同认证密钥，或意味着未加密状态的第二共同认证密钥。

[0135] 所述第二用户认证信息如图7所示，可以根据两种方式生成。

[0136] 一种方法如图7的(a)所示，可以以所述第二共同认证密钥和所述第一用户认证信息为构成要素，通过使用了单向性函数110的变换而生成第三用户认证密钥，对所述第三用户认证密钥进行OTP(One Time Password)演算，生成以时间值同步的所述第二用户认证信息。

[0137] 其中，所述第三用户认证密钥可以以所述第二共同认证密钥为演算密钥，对所述第一用户认证信息执行利用了所述单向性函数110的变换而生成。另外，所述第二用户认证信息可以通过利用了OTP发生器130的OTP演算而生成。

[0138] 另一种方法如图7的(b)所示，以所述第二共同认证密钥和所述第一用户认证信息为构成要素，通过利用了单向性函数110的变换而生成第三用户认证密钥，生成从所述第三用户认证密钥，利用时间信息，根据既定基准提取的第四用户认证密钥。

[0139] 所述第四用户认证密钥通过另外的时间提取值发生器120而被提取、生成，所述第四用户认证密钥可以意味着从第三用户认证密钥生成的任意的时间同步值。所述时间提取值发生器120工作原理与普通OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器120以数字或字母及其他多

样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器120应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0140] 然后，所述用户终端100可以针对所述第四用户认证密钥，执行使用了OTP发生器130的OTP(One Time Password)演算，生成以时间值同步的所述第二用户认证信息。

[0141] 所述第二用户认证信息生成后，所述用户终端100将所述第二用户认证信息和用于对所述加密的第一共同认证密钥进行解密的解密密钥提供给所述认证服务器200(S124)。

[0142] 所述认证服务器200利用所述用户终端100提供的所述解密密钥，将所述加密的第一共同认证密钥解密为第一共同认证密钥。下面，没有特别修饰词的第一共同认证密钥术语可以意味着解密的第一共同认证密钥。

[0143] 而且，利用所述第一共同认证密钥和所述第一服务器认证信息，生成第二服务器认证信息S210。其中，在所述用户终端100传送所述第一用户认证信息的情况下，可以使用所述第一用户认证信息而替代所述第一服务器认证信息，这与生成所述第二用户认证信息时相同。

[0144] 所述第二服务器认证信息如图8所示，可以根据两种方式生成。

[0145] 一种方法如图8的(a)所示，所述认证服务器200可以以所述第一服务器认证信息和所述第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第三服务器认证密钥，对所述第三服务器认证密钥进行OTP(One Time Password)演算，生成以时间值同步的第二服务器认证信息。其中，所述第三服务器认证密钥可以以所述第一共同认证密钥为演算密钥，针对所述第一服务器认证信息执行使用了所述单向性函数210的变换而生成。另外，所述第二服务器认证信息可以针对所述第三服务器认证密钥，通过使用了OTP发生器230的OTP演算而生成。

[0146] 另一种方法如图8的(b)所示，所述认证服务器200以所述第一服务器认证信息和所述第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第三服务器认证密钥，生成从所述第三服务器认证密钥，利用时间信息，根据既定基准提取的第四服务器认证密钥。

[0147] 所述第四服务器认证密钥通过另外的时间提取值发生器220而被提取、生成，所述第四服务器认证密钥可以意味着从第三服务器认证密钥生成的任意的时间同步值。所述时间提取值发生器220工作原理与普通OTP(One Time Password)发生器相同，普通OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器220以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器220应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0148] 然后，所述认证服务器200可以通过OTP(One Time Password)发生器230，对所述第四服务器认证密钥执行OTP演算，生成所述第二服务器认证信息。

[0149] 其中，所述第二用户认证信息的生成方式应与所述第二服务器认证信息的生成方式保持同一性。如果所述第二服务器认证信息以通过图8的(a)说明的方式生成，那么，所述第二用户认证信息也应以通过图7的(a)说明的方式生成。另外，单向性函数或OTP演算等也应相互对应地应用。而且，如果所述第二服务器认证信息以通过图8的(b)说明的方式生成，则所述第二用户认证信息也应以通过图7的(b)说明的方式生成。另外，单向性函数或OTP演

算、时间值提取等也应对应地应用相同的方式。

[0150] 然后，所述认证服务器200根据认证信息的一致与否，即，根据所述第二用户认证信息和所述第二服务器认证信息的一致与否，执行用户认证S212。所述第二用户认证信息既可以由用户手动输入并传送，也可以使其自动传送，还可以根据用户的传送指示而使其自动传送。

[0151] 其中，所述用户终端100可以使用与所述认证服务器200连接的一个或多个用户终端。例如，可以利用第一用户终端100，进行加密的第一共同认证密钥等的登录流程，利用第二用户终端100进行认证流程，也可以是相反的情形。另外，在认证流程的情况下，第一用户认证信息或第二用户认证信息可以通过所述第一用户终端100生成，所述第一用户认证信息或第二用户认证信息的输入或传送可以通过所述第二用户终端100执行。此外，在多样的流程中，可以使用多个用户终端100。

[0152] 在所述本发明第二实施例的情况下，在所述用户终端100与所述认证服务器200间传送的所有数据可以执行公开密钥方式的加密并传送。

[0153] 在所述本发明第二实施例中，对于执行用户认证的情形，当使用多个用户终端100或同时使用移动终端、台式电脑、平板电脑等而执行用户认证时，由于黑客攻击、异常现象或错误等其他原因，会有在既定时间内传送多个所述第一用户认证信息或多个第一服务器认证信息的情形。

[0154] 特别是在使第一服务器认证信息传送给所述用户终端100，执行认证服务器认证，使第二用户认证信息传送给所述认证服务器200，执行用户认证的情况下，为了认证服务器认证，会存在所述认证服务器200在既定时间(例如，30秒、60秒等)内向互不相同的用户终端100或相同的用户终端100传送多个所述第一服务器认证信息的情形。

[0155] 此时，为了确实的认证，所述认证服务器200即使在所述用户终端100传送了所述第二用户认证信息之后，也可以向所述用户终端100请求再传送所述第二用户认证信息，而且可以请求通过手动输入进行再传送，而不是自动传送。此时，第二用户认证信息应显示于所述用户终端100的画面中。如果在所述用户终端100中通过手动输入而传送，则所述认证服务器200可以比较手动输入的第二用户认证信息和所述第二服务器认证信息，添加执行用户认证。

[0156] 为了提高认证的安全性，也可以在通过所述第二用户认证信息再传送的添加认证后或替代通过所述第二用户认证信息再传送的添加认证，通过第三用户认证信息及第三服务器认证信息的比较而进行添加认证。通过图9对此进行说明。

[0157] 图9是显示第三服务器认证信息及第三用户认证信息的生成过程的框图。

[0158] 在通过所述第二用户认证信息的再传送而添加认证后，或替代通过所述第二用户认证信息再传送的添加认证，所述认证服务器200向所述用户终端100请求所述第三用户认证信息。

[0159] 此时，所述用户终端100可以如图9的(a)所示，以作为生成所述第二用户认证信息所需构成要素的第四用户认证密钥和所述认证机构的固有密钥为构成要素，执行使用了单向性函数110的变换，生成第五用户认证密钥，对所述第五用户认证密钥执行OTP(One Time Password)演算，生成所述第三用户认证信息。

[0160] 此时，所述认证服务器200生成与所述第三用户认证信息对应的第三服务器认证

信息。

[0161] 所述认证服务器200可以如图9的(b)所示，以作为生成所述第二服务器认证信息所需构成要素的第四服务器认证密钥和所述认证机构的固有密钥为构成要素，执行使用了单向性函数210的变换，生成第五服务器认证密钥，对所述第五服务器认证密钥执行OTP(One Time Password)演算，生成所述第三服务器认证信息。

[0162] 然后，如果所述第三用户认证信息被传送到所述认证服务器200，则在所述认证服务器200中，判断所述第三用户认证信息与所述第三服务器认证信息的一致与否，执行添加的用户认证。

[0163] 而且，当在认证过程中有黑客攻击等攻击征兆时，例如，当载入时间比平常时显著缓慢时，对于在台式电脑中登录的情形，在包括台式电脑的画面和移动终端画面中显示的事先预定值不同的情形在内，感知到普通技术人员熟知的黑客攻击等攻击征兆的情况下，所述用户终端100可以自动或手动向所述认证服务器200传送能够强制中断认证流程的强制中断信号。所述强制中断信号被传送到所述认证服务器200后，所述用户终端100及所述认证服务器200中断所述认证流程，待机直至开始新认证流程时为止。

[0164] 作为另一示例，在感知所述攻击征兆的情况下，所述认证服务器200也可以自我判断，将询问是否强制中断的信号传送给所述用户终端100，对应于用户终端100的响应信号，决定是否强制中断。

[0165] 另一方面，在包括所述用户终端100与所述认证服务器200间传送的认证信息及认证密钥等的所有传送对象数据中，可以添加用于数据完整性验证的验证密钥。即，可以在传送对象数据中添加所述验证密钥并传送。所述验证密钥可以包括针对各个传送对象数据而执行OTP(One Time Password)演算的第一OTP演算值。

[0166] 而且，在所述用户终端100或所述认证服务器200接收所述数据时，可以比较对接收的数据执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证。

[0167] 例如，在所述用户终端100将所述第一用户认证信息或所述第二用户认证信息传送给所述认证服务器200的情况下，可以在所述第一用户认证信息或所述第二用户认证信息中，添加对所述第一用户认证信息或所述第二用户认证信息进行OTP演算的第一OTP演算值作为验证密钥并传送。此时，所述认证服务器200接收了所述第一用户认证信息或所述第二用户认证信息时，比较对分离了所述验证密钥的第一用户认证信息或所述第二用户认证信息执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证，由此能够进行所述第一用户认证信息或所述第二用户认证信息的完整性验证。

[0168] 本发明第二实施例的情形具有强化安全性、确保完整性的优点。其中，还可以添加构成要素，强化认证流程上的安全性。这通过本发明的第三实施例进行说明。

[0169] 图10是显示本发明第三实施例的用户认证方法中生成第二用户认证信息的过程的框图，图11是显示本发明第三实施例的用户认证方法中第二服务器认证信息的生成过程的框图。

[0170] 如图10及图11所示，除本发明第二实施例在生成第二用户认证信息及所述第二服务器认证信息时添加间隙时间(gap time)值或间隙时间密钥作为构成要素之外，本发明第三实施例具有与本发明第二实施例相同的构成。

[0171] 所述间隙时间值可以在通过本发明第一实施例及第二实施例而说明的流程中，在用户输入用于认证的个人密码的流程S110中求出。具体而言，所述用户输入用于认证的个人密码后，所述用户终端100可以按1/n(n为任意的正实数)秒(second)单位测定所述用户输入个人密码所需要的时间，可以把此时测定的时间值定义为间隙时间值。

[0172] 其中，1/n秒可以意味着在所述用户终端100的硬件或软件上可拆分范围的时间单位。例如，将个人密码从首位值输入至末位值，用秒单位，可以表现为需要10秒，但在按1/1000秒单位测定的情况下，可以获得10436等测定值。或者，当以1/1000000秒单位或1/1000000000秒单位进行测定时，将获得包含大量数字的测定值。

[0173] 其中，当把从用于输入所述个人密码的输入窗口在画面中显示的时间点至所述个人密码的首位值输入的时间点的时间区间定义为第一时间区间，把从所述个人密码的末位值输入的时间点至告知所述个人密码输入完成的输入键(或回车键)的信号输入的时间点的时间区间定义为第二时间区间时，所述间隙时间值可以为从所述第一时间区间中某一时间点至所述第二时间区间中某一时间点的时间测定值。

[0174] 所述间隙时间密钥可以意味着从所述间隙时间值根据既定基准提取的数字值。

[0175] 在测定所述间隙时间值的情况下，所述用户终端100还把所述间隙时间值及/或所述间隙时间密钥传送给所述认证服务器200。如果从所述用户终端100传送了所述间隙时间值或/及所述间隙时间密钥，则所述认证服务器200将其与所述用户信息等匹配，进行存储及登录。

[0176] 在本发明的第三实施例中，所述第二用户认证信息如图10所示，可以根据两种方式生成。

[0177] 一种方法如图10的(a)所示，可以以所述第二共同认证密钥和所述第一用户认证信息、间隙时间值或间隙时间密钥为构成要素，通过使用了单向性函数110的变换，生成第三用户认证密钥，对所述第三用户认证密钥执行OTP(One Time Password)演算，生成以时间值同步的所述第二用户认证信息。

[0178] 其中，所述第三用户认证密钥可以以所述第二共同认证密钥为演算密钥，针对在所述间隙时间值或间隙时间密钥中组合了所述第一用户认证信息的值，执行使用了所述单向性函数110的变换而生成。另外，所述第二用户认证信息可以针对所述第三用户认证密钥，通过利用了OTP发生器130的OTP演算而生成。

[0179] 另一种方法如图10的(b)所示，可以以所述第二共同认证密钥和所述第一用户认证信息及所述间隙时间值或间隙时间密钥为构成要素，通过使用了单向性函数110的变换而生成第三用户认证密钥，可以生成从所述第三用户认证密钥，利用时间信息，根据既定基准而提取的第四用户认证密钥。

[0180] 所述第四用户认证密钥通过另外的时间提取值发生器120而被提取、生成，所述第四用户认证密钥可以意味着从第三用户认证密钥生成的任意的时间同步值。所述时间提取值发生器120工作原理与普通OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器120以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器120应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0181] 然后，所述用户终端100可以针对所述第四用户认证密钥，执行使用了OTP发生器

130的OTP(One Time Password)演算，生成以时间值同步的所述第二用户认证信息。

[0182] 所述第二服务器认证信息如图11所示，可以根据两种方式生成。

[0183] 一种方法如图11的(a)所示，所述认证服务器200可以以所述间隙时间值或间隙时间密钥和所述第一服务器认证信息、所述第一共同认证密钥为构成要素，通过使用了单向性函数210的变换而生成第三服务器认证密钥，对所述第三服务器认证密钥进行OTP(One Time Password)演算，生成以时间值同步的第二服务器认证信息。其中，所述第三服务器认证密钥可以以所述第一共同认证密钥为演算密钥，针对在所述间隙时间值或间隙时间密钥中组合了所述第一服务器认证信息的值，执行使用了所述单向性函数210的变换而生成。另外，所述第二服务器认证信息可以针对所述第三服务器认证密钥，通过使用了OTP发生器230的OTP演算而生成。

[0184] 另一种方法如图11的(b)所示，所述认证服务器200可以以所述间隙时间值或间隙时间密钥和所述第一服务器认证信息、所述第一共同认证密钥为构成要素，通过使用了单向性函数210的变换而生成第三服务器认证密钥，生成从所述第三服务器认证密钥，利用时间信息，根据既定基准而提取的第四服务器认证密钥。

[0185] 所述第四服务器认证密钥通过另外的时间提取值发生器220而被提取、生成，所述第四服务器认证密钥可以意味着从第三服务器认证密钥生成的任意的时间同步值。所述时间提取值发生器220工作原理与普通OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器220以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器220应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0186] 然后，所述认证服务器200可以通过OTP(One Time Password)发生器230，对所述第四服务器认证密钥执行OTP演算，生成所述第二服务器认证信息。

[0187] 其中，所述第二用户认证信息的生成方式应与所述第二服务器认证信息的生成方式保持同一性。如果所述第二服务器认证信息以通过图11的(a)说明的方式生成，那么，所述第二用户认证信息也应以通过图10的(a)说明的方式生成。另外，单向性函数或OTP演算等也应相互对应地应用。而且，如果所述第二服务器认证信息以通过图11的(b)说明的方式生成，那么，所述第二用户认证信息也应以通过图10的(b)说明的方式生成。另外，单向性函数或OTP演算、时间值提取等也应对应地应用相同的方式。

[0188] 就本发明第一实施例至第三实施例的情形而言，通过用户终端100而输入的个人密码执行使用了单向性函数的第一次变换及利用了加密的第二次变换并传送给所述认证服务器200，因而具有提高安全性的优点。

[0189] 图12是显示本发明第四实施例的用户认证方法的顺序图，图13是显示图12中生成第一共同认证密钥及加密的第一共同认证密钥的过程的框图。

[0190] 如图12及图13所示，本发明第四实施例的用户认证方法可以从用户为了通过用户终端100进行用户登录而下载并安装所述专用程序开始。用户登录流程既可以在所述专用程序的安装过程中执行，也可以在所述专用程序的安装之后，通过另外的用户登录过程执行。

[0191] 首先，用户开始用户登录所需流程，如果用户通过所述用户终端100输入用户信息和个人密码S102，则所述用户终端100生成第一共同认证密钥和用于加密所述第一共同认

证密钥的第一加密密钥S103。用于加密所述第一共同认证密钥的第一加密密钥既可以根据既定基准随机生成，也可以通过另外选择的构成要素而生成。

[0192] 本发明第四实施例的情形说明的是，所述第一加密密钥以所述用户输入的个人密码为构成要素而生成的情形。

[0193] 所述第一加密密钥借助于以所述用户输入的个人密码为构成要素，执行使用了单向性函数的变换而生成。所述单向性函数的演算密钥可以利用根据既定基准而生成的值。

[0194] 所述单向性函数作为把任意长度的数据映射、变换成固定长度的数据的函数，可以意味着被认为不可逆变换，即，无法恢复为原来数据的所有函数。作为所述单向性函数，可以包括MD5、SHA、SHA2、scrypt等密码学哈希(HASH)函数、CRC32及CHECKSUM等非密码学哈希函数，可以包括普通技术人员所知的所有单向性函数，所述第一共同认证密钥可以使用在这些单向性函数中选择的某一种单向性函数而生成。

[0195] 作为用于生成所述第一加密密钥的构成要素，除所述个人密码之外，还可以添加所述用户终端100的机械性固有密钥，其中，还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。也可以添加另外的其他构成要素。

[0196] 其中，所述用户终端100的机械性固有密钥例如可以包括序列号或USIM(全球用户身份模块)号码等，此外，可以包括为了区分所述用户终端而赋予的各种固有号码、电话号码等。

[0197] 在所述第一加密密钥的生成前后或与生成同时，所述用户终端100可以如图13所示，利用所述用户终端100的机械性固有密钥，执行使用了单向性函数110的第一次变换，生成第一共同认证密钥S103。所述单向性函数110的演算密钥可以利用根据既定基准而生成的值。

[0198] 所述第一共同认证密钥可以以所述用户终端100的机械性固有密钥为单独构成要素，通过使用了所述单向性函数110的第一次变换而生成。所述第一共同认证密钥可以添加其他构成要素而生成。例如，也还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。另外，也可以添加固有性得到认定的其他构成要素。

[0199] 在本发明第一至第三实施例的情况下，用户输入的所述个人密码是用于生成所述第一共同认证密钥的构成要素，在本发明第四实施例的情况下，所述个人密码是用于生成所述第一加密密钥的构成要素，不用作所述第一共同认证密钥的构成要素。

[0200] 这是为了从根源上切断个人密码的盗用或泄露并在公开的网络上强化安全性。

[0201] 然后，所述第一共同认证密钥通过加密单元120，通过利用所述第一加密密钥进行加密的第二次变换，生成为加密的第一共同认证密钥S106。

[0202] 其中，加密可以使用用于加密的加密密钥和用于解密的解密密钥相同的对称密钥方式，可以使用在Twofish、Serpent、AES、Blowfish、CAST5、RC4、3DES、IDEA、RC6、DES等中选择的加密方式。此外，也可以应用通常技术人员熟知的加密方式。

[0203] 所述用户终端100将所述加密的第一共同认证密钥与所述用户信息一同传送给所述认证服务器200(S108)。

[0204] 所述认证服务器200将所述用户终端100传送的所述加密的第一共同认证密钥匹

配于所述用户信息，与所述用户信息一同登录及存储S202。据此执行用户登录流程。所述用户登录流程执行后，所述用户终端100可以删除所述加密的第一共同认证密钥及所述第一加密密钥。根据情况，可将所述加密的第一共同认证密钥及所述第一加密密钥存储于由所述用户终端100设置的专用存储空间或由所述专用程序在所述用户终端100内设置的专用存储空间。

[0205] 就以往技术而言，执行用户登录后，认证服务器通常存储个人密码，但本发明第四实施例的情形，所述认证服务器200或用户终端100不存储密码，所述认证服务器200只存储所述加密的第一共同认证密钥。

[0206] 因此，在用户忘记或泄露了个人密码的情况下，使得可以通过新登录流程，通过包含新密码的第一加密密钥重新进行加密，将加密的第一共同认证密钥传送到所述认证服务器200进行登录，就认证机构而言，即使在所述加密的第一共同认证密钥因黑客攻击等而被泄露的情况下，使安全性也得到强化。

[0207] 另外，在第一共同认证密钥中，个人密码不成为构成要素，可以通过使用了单向性函数的第一变换及加密的第二变换而防止个人信息泄露，具有在公开的网络环境下，可以没有黑客攻击顾虑地安全地进行用户认证或认证服务器认证的优点。

[0208] 然后，所述认证服务器200可以组合内置的认证机构的固有密钥与所述加密的第一共同认证密钥而生成第一服务器认证信息S204。

[0209] 所述第一服务器认证信息可以与本发明第一实施例情形一样，根据通过图4所说明的两种方式而生成。

[0210] 一种方法如图4的(a)所示，所述认证服务器200可以以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第一服务器认证密钥，对所述第一服务器认证密钥进行OTP(One Time Password)演算，生成以时间值同步的第一服务器认证信息。其中，所述第一服务器认证密钥可以以所述认证机构的固有密钥为演算密钥，针对所述加密的第一共同认证密钥，执行使用了所述单向性函数210的变换而生成。另外，所述第一服务器认证信息可以通过使用了OTP发生器230的OTP演算而生成。

[0211] 另一种方法如图4的(b)所示，所述认证服务器200以内置的认证机构的固有密钥和所述加密的第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第一服务器认证密钥，生成从所述第一服务器认证密钥，利用时间信息，根据既定基准而提取的第二服务器认证密钥。

[0212] 所述第二服务器认证密钥通过另外的时间提取值发生器220而被提取、生成，所述第二服务器认证密钥可以意味着从第一服务器认证密钥生成的任意的时间同步值。所述时间提取值发生器220工作原理与普通的OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器220以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器220应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0213] 然后，所述认证服务器200可以通过OTP(One Time Password)发生器230，对所述第二服务器认证密钥执行OTP演算，生成所述第一服务器认证信息。

[0214] 所述第一服务器认证信息可以在用户登录之后，与其他流程无关地独立生成。即，

所述第一服务器认证信息只要在所述用户登录之后直至后述第一用户认证信息生成时的时间内生成即可。

[0215] 而且，即使在将所述第一服务器认证信息传送给所述用户终端100的情况下，既可以生成后即时传送，也可以在判断为需要的时间点传送。另外，还可以根据用户终端100的请求而传送。

[0216] 然后，如果用户开始认证流程，用户在所述用户终端100开始认证所需流程，用户输入个人密码S110，那么，所述用户终端100生成第二共同认证密钥和第二加密密钥S113。所述第二共同认证密钥是对应于所述第一共同认证密钥的要素，所述第二加密密钥是对应于所述第一加密密钥的要素。因此，生成方式应相互对应。用于加密所述第二共同认证密钥的所述第二加密密钥既可以根据既定基准随机生成，也可以通过另外选择的构成要素生成。

[0217] 其中，所述第二加密密钥以所述个人密码为构成要素而生成。所述第二加密密钥可以借助于以用户输入的所述个人密码为构成要素，执行使用了单向性函数的变换而生成。所述单向性函数的演算密钥可以利用根据既定基准而生成的值。

[0218] 作为用于生成所述第二加密密钥的构成要素，除所述个人密码之外，可以添加所述用户终端100的机械性固有密钥，其中，也还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。也可以添加另外的其他构成要素。其中，所述用户终端100的机械性固有密钥例如可以包括序列号或USIM(全球用户身份模块)号码等，此外，可以包括为了区分所述用户终端而赋予的各种固有号码、电话号码等。

[0219] 在所述第一加密密钥的生成前后或与生成同时，所述用户终端100可以利用所述用户终端100的机械性固有密钥，执行使用了单向性函数110的第一次变换，生成第一共同认证密钥S103。所述单向性函数的演算密钥可以利用根据既定基准而生成的值。

[0220] 所述第二共同认证密钥可以与所述第一共同认证密钥的生成方式相同地，以所述用户终端100的机械性固有密钥为单独构成要素，通过使用了所述单向性函数110的第一次变换而生成，但可以在其中添加其他构成要素。例如，也还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。另外，也可以添加固有性得到认定的其他构成要素。这可以对应于在所述第一共同认证密钥中包含所述专用程序的固有密钥或其他构成要素的情形。

[0221] 在本发明第一至第三实施例的情况下，用户输入的所述个人密码是用于生成所述第二共同认证密钥的构成要素，在本发明第四实施例的情况下，所述个人密码是用于生成所述第二加密密钥的构成要素，不用作所述第二共同认证密钥的构成要素。

[0222] 即，组合所述个人密码及所述用户终端100的机械性固有密钥，执行使用了单向性函数110的第一次变换，生成第二共同认证密钥S113。

[0223] 所述单向性函数110可以使用与生成所述第一共同认证密钥的单向性函数相同的函数，可以以相同方式应用。

[0224] 所述第二共同认证密钥可以与所述第一共同认证密钥的生成方式相同地，借助于以所述个人密码及所述用户终端100的机械性固有密钥为构成要素，通过根据既定基准而生成的演算密钥进行演算，借助第一次变换而生成。

[0225] 然后，所述第二共同认证密钥与第一共同认证密钥的情形相同，通过加密单元120，通过利用所述加密密钥进行加密的第二次变换，生成为加密的第二共同认证密钥S113。加密方式及第二加密密钥的生成方式，与第一共同认证密钥的加密方式及所述第一加密密钥的生成方式对应并相同地应用。

[0226] 其中，所述第二加密密钥以所述个人密码为构成要素而生成。所述第二加密密钥可以借助于以用户输入的所述个人密码为构成要素，执行使用了单向性函数的变换而生成。所述单向性函数的演算密钥可以利用根据既定基准而生成的值。

[0227] 作为用于生成所述第二加密密钥的构成要素，除所述个人密码之外，可以添加所述用户终端100的机械性固有密钥，其中，也还可以包括所述专用程序的固有密钥(例如，Device Token、Bundle ID、Package Name、App ID等)作为构成要素。另外，也可以添加另外的其他构成要素。其中，所述用户终端100的机械性固有密钥例如可以包括序列号或USIM(全球用户身份模块)号码等，此外，可以包括为了区分所述用户终端而赋予的各种固有号码、电话号码等。

[0228] 所述第二加密密钥可以存储于由所述用户终端100设置的专用存储空间或由所述专用程序在所述用户终端100内设置的专用存储空间。

[0229] 其中，所述第二加密密钥可以根据另外的加密方式进行加密并存储。例如，可以组合所述个人密码和所述用户终端的机械性固有密钥，执行使用了单向性函数的变换，利用由此生成的第三加密密钥进行加密之后存储。

[0230] 然后，所述用户终端100利用所述加密的第二共同认证密钥，生成第一用户认证信息S116。对于生成与所述第一用户认证信息对应的所述第一服务器认证信息，已经作过说明。

[0231] 所述第一用户认证信息可以根据与通过本发明第一实施例说明的方式相同的方式，以两种方式生成。

[0232] 一种方法如图5的(a)所示，所述认证服务器200可以以预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，通过使用了单向性函数110的变换，生成第一用户认证密钥，对所述第一用户认证密钥执行OTP(One Time Password)演算，生成以时间值同步的第一用户认证信息。所述认证机构的固有密钥可以在所述专用程序安装时内置并提供，或在认证流程开始前通过更新等提供。

[0233] 其中，所述第一用户认证密钥可以以所述认证机构的固有密钥为演算密钥，针对所述加密的第二共同认证密钥，执行通过所述单向性函数110的变换而生成。另外，所述第一用户认证信息可以通过使用了OTP发生器130的OTP演算而生成。

[0234] 另一种方法如图5的(b)所示，所述认证服务器200以预先提供的认证机构的固有密钥和所述加密的第二共同认证密钥为构成要素，通过使用了单向性函数110的变换而生成第一用户认证密钥，生成从所述第一用户认证密钥，利用时间信息，根据既定基准提取的第二用户认证密钥。所述认证机构的固有密钥可以在所述专用程序安装时内置并提供，或在认证流程开始前通过更新等而提供。

[0235] 所述第二用户认证密钥通过另外的时间提取值发生器120而被提取、生成，所述第二用户认证密钥可以意味着从第一用户认证密钥生成的任意的时间同步值。所述时间提取值发生器120工作原理与普通的OTP(One Time Password)发生器相同，普通的OTP(One

Time Password)发生器以数字标识输出值，但所述时间提取值发生器120以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器120应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0236] 然后，所述用户终端100可以通过OTP发生器130，对所述第二用户认证密钥执行OTP(One Time Password)演算，生成所述第一用户认证信息。

[0237] 其中，所述第一用户认证信息的生成方式应与所述第一服务器认证信息的生成方式保持同一性。如果所述第一服务器认证信息以通过图4的(a)说明的方式生成，那么，所述第一用户认证信息也应通过图5的(a)说明的方式生成。另外，单向性函数或OTP演算等也应相互对应地应用。而且，如果所述第一服务器认证信息以通过图4的(b)说明的方式生成，则所述第一用户认证信息也应以通过图5的(b)说明的方式生成。另外，单向性函数或OTP演算、时间值提取等也应对应地应用相同的方式。

[0238] 然后，如果将所述第一用户认证信息通过所述用户终端100传送给所述认证服务器200(S118)，则所述认证服务器200根据认证信息的一致与否，即，根据所述第一用户认证信息和所述第一服务器认证信息的一致与否，执行用户认证S208。所述第一用户认证信息既可以由用户手动输入并传送，也可以使其自动传送，还可以根据用户的传送指示而使其自动传送。

[0239] 其中，所述用户终端100可以使用与所述认证服务器200连接的一个或多个用户终端。例如，可以利用第一用户终端100，进行加密的第一共同认证密钥等的登录流程，利用第二用户终端100进行认证流程，也可以是相反的情形。另外，在认证流程的情况下，第一用户认证信息可以通过所述第一用户终端100生成，所述第一用户认证信息的输入或传送可以通过所述第二用户终端100执行。此外，在多样的流程中，可以使用多个用户终端100。

[0240] 而且，通过用户在用户终端100中比较所述第一用户认证信息和所述第一服务器认证信息，可以确认所述认证服务器200的真伪与否、连接于认证服务器200的接入网页的真伪与否或提供认证服务的服务提供商或认证机构的真伪与否。以往，尽管谎称认证机构并与认证机构的接入网页类似地构成而使用户混同的案例很多，但事实上对此却没有恰当的对策。在本发明中，为了解决这种问题，用户可以确认认证机构(或服务提供商)的真伪与否。

[0241] 为此，当生成所述第一服务器认证信息时，所述认证服务器200将所述第一服务器认证信息通过所述接入网页显示或传送给所述用户终端100(S206)。所述第一服务器认证信息显示或传送后，所述用户终端100将其与所述第一用户认证信息进行比较，由此可以进行判别真伪与否的认证服务器认证，即，判别所述认证服务器200是否为真正的认证服务器、所述接入网页是否为真的S120。即，可以确认所述认证服务器200的真伪与否、连接于认证服务器200的接入网页的真伪与否或提供认证服务的服务提供商或认证机构的真伪与否。

[0242] 其中，在所述第一服务器认证信息为在所述加密的第二共同认证密钥生成前预先传送到所述用户终端100的状态的情况下，无需再传送或另行传送，利用预先传送的所述第一服务器认证信息执行认证服务器认证。

[0243] 在本发明的第四实施例中，如果在所述用户终端100中比较所述第一服务器认证信息及所述第一用户认证信息，则通过一致与否，能够进行判别认证机构或认证服务器200

真伪与否的认证机构认证或认证服务器认证，如果在所述认证服务器200中比较所述第一服务器认证信息及所述第一用户认证信息，则通过一致与否，能够进行用户认证。

[0244] 其中，所述认证服务器的认证流程S206、S120和所述用户认证流程S118、S208既可以同时执行，也可以在先执行所述认证服务器的认证流程后，如果确认认证，则既可以执行所述用户认证流程，也可以选择认证服务器认证流程或用户认证流程中某一者并执行。

[0245] 在所述本发明第四实施例的情况下，在所述用户终端100与所述认证服务器200间传送的所有数据可以执行公开密钥方式的加密并传送。

[0246] 在所述本发明第四实施例的情况下，对于执行用户认证而非认证服务器认证的情形，当使用多个用户终端100或同时使用移动终端、台式电脑、平板电脑等而执行用户认证时，由于异常现象或错误等其他原因，会有在既定时间内向所述认证服务器200传送多个所述第一用户认证信息的情形。

[0247] 在这种情况下，为了确实的认证，所述认证服务器200即使是传送了所述第一用户认证信息的情形，也可以向所述用户终端100请求再传送所述第一用户认证信息，而且可以请求通过手动输入进行再传送，而不是自动传送。此时，第一用户认证信息应显示于所述用户终端100的画面中，以便用户可以手动输入。其中，手动输入可以请求连续执行两次。如果通过手动输入而传送第一用户认证信息，则所述认证服务器200可以比较通过手动输入而传送的第一用户认证信息和所述第一服务器认证信息，执行用户认证。

[0248] 而且，当在认证过程中有黑客攻击等攻击征兆时，例如，当载入时间比平常时显著缓慢时，对于在台式电脑中登录的情形，在包括台式电脑的画面和移动终端画面中显示的事先预定值不同的情形在内，感知到普通技术人员熟知的黑客攻击等攻击征兆的情况下，所述用户终端100可以自动或手动向所述认证服务器200传送能够强制中断认证流程的强制中断信号。所述强制中断信号传送到所述认证服务器200后，所述用户终端100及所述认证服务器200中断所述认证流程，待机直至开始新认证流程时为止。

[0249] 作为另一示例，在感知所述攻击征兆的情况下，所述认证服务器200也可以自我判断，把询问是否强制中断的信号传送给所述用户终端100，对应于用户终端100的响应信号，决定是否强制中断。

[0250] 另一方面，在包括所述用户终端100与所述认证服务器200间传送的认证信息及认证密钥等的所有传送对象数据中，可以添加用于数据完整性验证的验证密钥。即，可以在传送对象数据中添加所述验证密钥并传送。所述验证密钥可以包括针对各个传送对象数据而执行OTP(One Time Password)演算的第一OTP演算值。

[0251] 而且，在所述用户终端100或所述认证服务器200接收所述数据时，可以比较对接收的数据执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证。

[0252] 例如，在所述用户终端100将所述第一用户认证信息传送给所述认证服务器200的情况下，可以在所述第一用户认证信息中，添加对所述第一用户认证信息进行OTP演算的第一OTP演算值作为验证密钥并传送。此时，所述认证服务器200接收了所述第一用户认证信息时，比较对分离了所述验证密钥的第一用户认证信息执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证，由此能够进行所述第一用户认证信息的完整性验证。

[0253] 在所述本发明第四实施例的情况下，在执行所述用户终端100比较所述第一用户认证信息和所述第一服务器认证信息并进行认证的认证服务器认证的情况下，需要添加的用户认证流程。而且，在执行所述认证服务器200比较所述第一用户认证信息和所述第一服务器认证信息并进行认证的用户认证的情况下，为了进一步确保可靠性，有时需要添加的用户认证。为此，需要后述的本发明的第五实施例。

[0254] 下面说明本发明的第五实施例。

[0255] 图14是显示本发明第五实施例的用户认证方法的顺序图。

[0256] 如图14所示，本发明第五实施例的用户认证方法全部包括通过本发明第四实施例说明的认证流程，包括在通过所述第一用户认证信息和所述第一服务器认证信息而实现用户认证S208或认证服务器认证S120的状态下添加的过程。因此，通过所述第一用户认证信息和所述第一服务器认证信息而实现用户认证S208或认证服务器认证S120的过程已通过本发明第四实施例进行了说明，因而省略详细说明。

[0257] 在生成所述第一服务器认证信息及所述第一用户认证信息并执行所述用户认证S208或认证服务器认证S120之前步骤，或通过所述第一服务器认证信息及所述第一用户认证信息而执行所述用户认证S208或认证服务器认证S120之后，所述用户终端100利用所述第一用户认证信息或所述第一服务器认证信息和所述第二共同认证密钥，生成第二用户认证信息S122。

[0258] 作为用于生成所述第二用户认证信息的构成要素，一般使用第一用户认证信息及所述第二共同认证密钥，但在所述认证服务器200传送了所述第一服务器认证信息的情况下，也可以利用所述第一服务器认证信息。这在所述第一服务器认证信息和所述第一用户认证信息为相互相同值的前提下才可能。下面说明利用第一用户认证信息生成所述第二用户认证信息的情形。

[0259] 另外，所述第二共同认证密钥意味着利用解密密钥对所述加密的第二共同认证密钥进行解密的第二共同认证密钥，或指未加密状态的第二共同认证密钥。下面，在第二共同认证密钥没有特别的修饰词的情况下，所述第二共同认证密钥意味着被解密的第二共同认证密钥，或意味着未加密状态的第二共同认证密钥。

[0260] 所述第二用户认证信息可以以通过本发明第二实施例说明的内容相同的方式，根据两种方式而生成。

[0261] 一种方法如图7的(a)所示，可以以所述第二共同认证密钥和所述第一用户认证信息为构成要素，通过使用了单向性函数110的变换而生成第三用户认证密钥，对所述第三用户认证密钥进行OTP(One Time Password)演算，生成以时间值同步的所述第二用户认证信息。

[0262] 其中，所述第三用户认证密钥可以以所述第二共同认证密钥为演算密钥，对所述第一用户认证信息执行使用了所述单向性函数110的变换而生成。另外，所述第二用户认证信息可以通过使用了OTP发生器130的OTP演算而生成。

[0263] 另一种方法如图7的(b)所示，以所述第二共同认证密钥和所述第一用户认证信息为构成要素，通过使用了单向性函数110的变换而生成第三用户认证密钥，生成从所述第三用户认证密钥，利用时间信息，根据既定基准提取的第四用户认证密钥。

[0264] 所述第四用户认证密钥通过另外的时间提取值发生器120而被提取、生成，所述第

四用户认证密钥可以意味着从第三用户认证密钥生成的任意的时间同步值。所述时间提取值发生器120工作原理与普通OTP(One Time Password)发生器相同，普通的OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器120以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器120应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0265] 然后，所述用户终端100可以针对所述第四用户认证密钥，执行使用了OTP发生器130的OTP(One Time Password)演算，生成以时间值同步的所述第二用户认证信息。

[0266] 所述第二用户认证信息生成后，所述用户终端100将所述第二用户认证信息和用于对所述加密的第一共同认证密钥进行解密的解密密钥提供给所述认证服务器200(S124)。

[0267] 在使用加密密钥和解密密钥相同方式的对称密钥加密方式的情况下，所述解密密钥将成为所述第一加密密钥或第二加密密钥。

[0268] 所述认证服务器200利用所述用户终端100提供的所述解密密钥，把所述加密的第一共同认证密钥解密为第一共同认证密钥S209。下面，没有特别修饰词的第一共同认证密钥术语可以意味着解密的第一共同认证密钥。

[0269] 而且，利用所述第一共同认证密钥和所述第一服务器认证信息，生成第二服务器认证信息S210。其中，在所述用户终端100传送所述第一用户认证信息的情况下，可以使用所述第一用户认证信息而替代所述第一服务器认证信息，这与生成所述第二用户认证信息时相同。

[0270] 所述第二服务器认证信息可以与通过本发明第二实施例说明的内容相同地根据两种方式生成。

[0271] 一种方法如图8的(a)所示，所述认证服务器200可以以所述第一服务器认证信息和所述第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第三服务器认证密钥，对所述第三服务器认证密钥进行OTP(One Time Password)演算，生成以时间值同步的第二服务器认证信息。其中，所述第三服务器认证密钥可以以所述第一共同认证密钥为演算密钥，针对所述第一服务器认证信息执行使用了所述单向性函数210的变换而生成。另外，所述第二服务器认证信息可以针对所述第三服务器认证密钥，通过使用了OTP发生器230的OTP演算而生成。

[0272] 另一种方法如图8的(b)所示，所述认证服务器200以所述第一服务器认证信息和所述第一共同认证密钥为构成要素，通过使用了单向性函数210的变换，生成第三服务器认证密钥，生成从所述第三服务器认证密钥，利用时间信息，根据既定基准提取的第四服务器认证密钥。

[0273] 所述第四服务器认证密钥通过另外的时间提取值发生器220而被提取、生成，所述第四服务器认证密钥可以意味着从第三服务器认证密钥生成的任意的时间同步值。所述时间提取值发生器220工作原理与普通OTP(One Time Password)发生器相同，普通OTP(One Time Password)发生器以数字标识输出值，但所述时间提取值发生器220以数字或字母及其他多样的符号等标识输出值，在这一点上，两者不同。因此，所述时间提取值发生器220应理解为包括执行普通OTP(One Time Password)演算的OTP发生器的概念。

[0274] 然后，所述认证服务器200可以通过OTP(One Time Password)发生器230，对所述

第四服务器认证密钥执行OTP演算，生成所述第二服务器认证信息。

[0275] 其中，所述第二用户认证信息的生成方式应与所述第二服务器认证信息的生成方式保持同一性。如果所述第二服务器认证信息以通过图8的(a)说明的方式生成，那么，所述第二用户认证信息也应通过图7的(a)说明的方式生成。另外，单向性函数或OTP演算等也应相互对应地应用。而且，如果所述第二服务器认证信息以通过图8的(b)说明的方式生成，则所述第二用户认证信息也应以通过图7的(b)说明的方式生成。另外，单向性函数或OTP演算、时间值提取等也应对应地应用相同的方式。

[0276] 然后，所述认证服务器200根据认证信息的一致与否，即，根据所述第二用户认证信息和所述第二服务器认证信息的一致与否，执行用户认证S212。所述第二用户认证信息既可以由用户手动输入并传送，也可以使得自动传送，还可以根据用户的传送指示而使得自动传送。

[0277] 其中，所述用户终端100可以使用与所述认证服务器200连接的一个或多个用户终端。例如，可以利用第一用户终端100，进行加密的第一共同认证密钥等的登录流程，利用第二用户终端100进行认证流程，也可以是相反的情形。另外，在认证流程的情况下，第一用户认证信息或第二用户认证信息可以通过所述第一用户终端100生成，所述第一用户认证信息或第二用户认证信息的输入或传送可以通过所述第二用户终端100执行。此外，在多样的流程中，可以使用多个用户终端100。

[0278] 在所述本发明第五实施例的情况下，在所述用户终端100与所述认证服务器200间传送的所有数据可以执行公开密钥方式的加密并传送。

[0279] 另外，在所述本发明第五实施例中，对于执行用户认证的情形，当使用多个用户终端100或同时使用移动终端、台式电脑、平板电脑等而执行用户认证时，由于异常现象或错误等其他原因，会有在既定时间内传送多个所述第一用户认证信息或多个第一服务器认证信息的情形。

[0280] 特别是在使第一服务器认证信息传送给所述用户终端100，执行认证服务器认证，使第二用户认证信息传送给所述认证服务器200，执行用户认证的情况下，为了认证服务器认证，会有所述认证服务器200在既定时间(例如，30秒、60秒等)内向互不相同的用户终端100或相同的用户终端100传送多个所述第一服务器认证信息的情形。

[0281] 此时，为了确实的认证，所述认证服务器200即使在所述用户终端100传送了所述第二用户认证信息之后，也可以向所述用户终端100请求再传送所述第二用户认证信息，而且可以请求通过手动输入进行再传送，而不是自动传送。此时，第二用户认证信息应显示于所述用户终端100的画面中。如果所述第二用户认证信息在所述用户终端100中通过手动输入而传送，则所述认证服务器200可以比较手动输入的第二用户认证信息和所述第二服务器认证信息，添加执行用户认证。

[0282] 为了提高认证的安全性，也可以在通过所述第二用户认证信息再传送的添加认证后或替代通过所述第二用户认证信息再传送的添加认证，通过第三用户认证信息及第三服务器认证信息的比较而进行添加认证。

[0283] 这是在通过所述第二用户认证信息再传送而添加认证后，或替代通过所述第二用户认证信息再传送的添加认证，所述认证服务器200向所述用户终端100请求所述第三用户认证信息。

[0284] 所述第三用户认证信息及所述第三服务器认证信息可以应用与本发明第二实施例的情形相同的方式而生成。

[0285] 即，所述用户终端100可以如图9的(a)所示，以作为生成所述第二用户认证信息所需构成要素的第四用户认证密钥和所述认证机构的固有密钥为构成要素，执行使用了单向性函数110的变换，生成第五用户认证密钥，对所述第五用户认证密钥执行OTP(One Time Password)演算，生成所述第三用户认证信息。

[0286] 此时，所述认证服务器200生成与所述第三用户认证信息对应的第三服务器认证信息。

[0287] 所述认证服务器200可以如图9的(b)所示，以作为生成所述第二服务器认证信息所需构成要素的第四服务器认证密钥和所述认证机构的固有密钥为构成要素，执行使用了单向性函数210的变换，生成第五服务器认证密钥，对所述第五服务器认证密钥执行OTP(One Time Password)演算，生成所述第三服务器认证信息。

[0288] 然后，如果将所述第三用户认证信息传送到所述认证服务器200，则在所述认证服务器200中，判断所述第三用户认证信息与所述第三服务器认证信息的一致与否，执行添加的用户认证。

[0289] 另一方面，当在认证过程中有黑客攻击等攻击征兆时，例如，当载入时间比平常时显著缓慢时，对于在台式电脑中登录的情形，在包括台式电脑的画面和移动终端画面中显示的事先预定值不同的情形在内，感知到普通技术人员熟知的黑客攻击等攻击征兆的情况下，所述用户终端100可以自动或手动向所述认证服务器200传送能够强制中断认证流程的强制中断信号。将所述强制中断信号传送到所述认证服务器200后，所述用户终端100及所述认证服务器200中断所述认证流程，待机直至开始新认证流程时为止。

[0290] 作为另一示例，在感知所述攻击征兆的情况下，所述认证服务器200也可以自我判断，将询问是否强制中断的信号传送给所述用户终端100，对应于用户终端100的响应信号，决定是否强制中断。

[0291] 另一方面，在包括所述用户终端100与所述认证服务器200间传送的认证信息及认证密钥等的所有传送对象数据中，可以添加用于数据完整性验证的验证密钥。即，可以在传送对象数据中添加所述验证密钥并传送。所述验证密钥可以包括各个传送对象数据而执行OTP(One Time Password)演算的第一OTP演算值。

[0292] 而且，在所述用户终端100或所述认证服务器200接收所述数据时，可以比较对接收的数据执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证。

[0293] 例如，在所述用户终端100将所述第一用户认证信息或所述第二用户认证信息传送给所述认证服务器200的情况下，可以在所述第一用户认证信息或所述第二用户认证信息中，添加对所述第一用户认证信息或所述第二用户认证信息进行OTP演算的第一OTP演算值作为验证密钥并传送。此时，所述认证服务器200接收了所述第一用户认证信息或所述第二用户认证信息时，比较对分离了所述验证密钥的第一用户认证信息或所述第二用户认证信息执行OTP(One Time Password)演算的第二OTP演算值和所述验证密钥，执行完整性验证，由此能够进行所述第一用户认证信息或所述第二用户认证信息的完整性验证。

[0294] 本发明第五实施例的情形具有强化安全性、确保完整性的优点。其中，还可以添加

间隙时间(gap time)值或间隙时间密钥的构成要素，强化认证流程上的安全性。这通过本发明的第六实施例进行说明。

[0295] 除本发明第五实施例在生成第二用户认证信息及所述第二服务器认证信息时，添加通过本发明第三实施例说明的间隙时间(gap time)值或间隙时间密钥作为构成要素之外，本发明第六实施例具有与本发明第五实施例相同的构成。因此，本发明第六实施例可以通过本发明第五实施例及本发明第三实施例实施，因而省略其说明。

[0296] 如上所述，根据本发明的实施例，具有在公开网络上从根源上切断个人信息泄露，摆脱黑客攻击危险，强化安全性，能够验证传送数据的完整性的效果。另外，能够检查认证所需的认证服务器、认证机构、Web站点等的真伪与否，具有能够实现可确保完整性及唯一性的用户认证的优点。另外，当生成认证信息时，采取利用之前值执行单方向性变换而生成下个值的链锁(chaining)方式，从而具有能够从根本上防止通过终端的时间操作来预知未来将生成的值等操作的效果。

[0297] 所述实施例的说明只不过是为了更彻底理解本发明而以附图为参照列举的示例，因而不得解释为限定本发明之意。另外，对于本发明所属技术领域的技术人员而言，在不超出本发明的基本原理的范围内，可以进行多样的变形和变更，这是明白无误的。

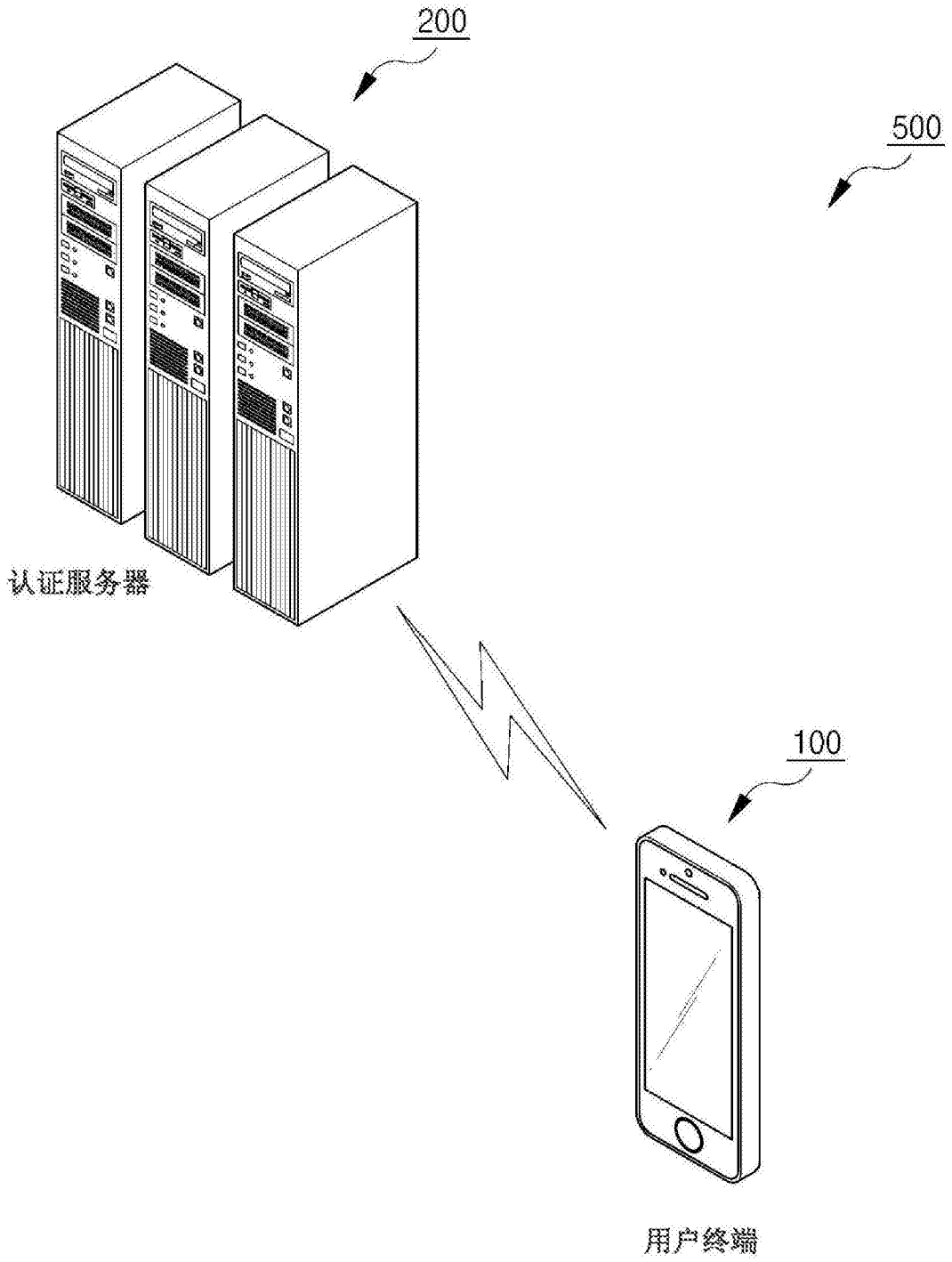


图1

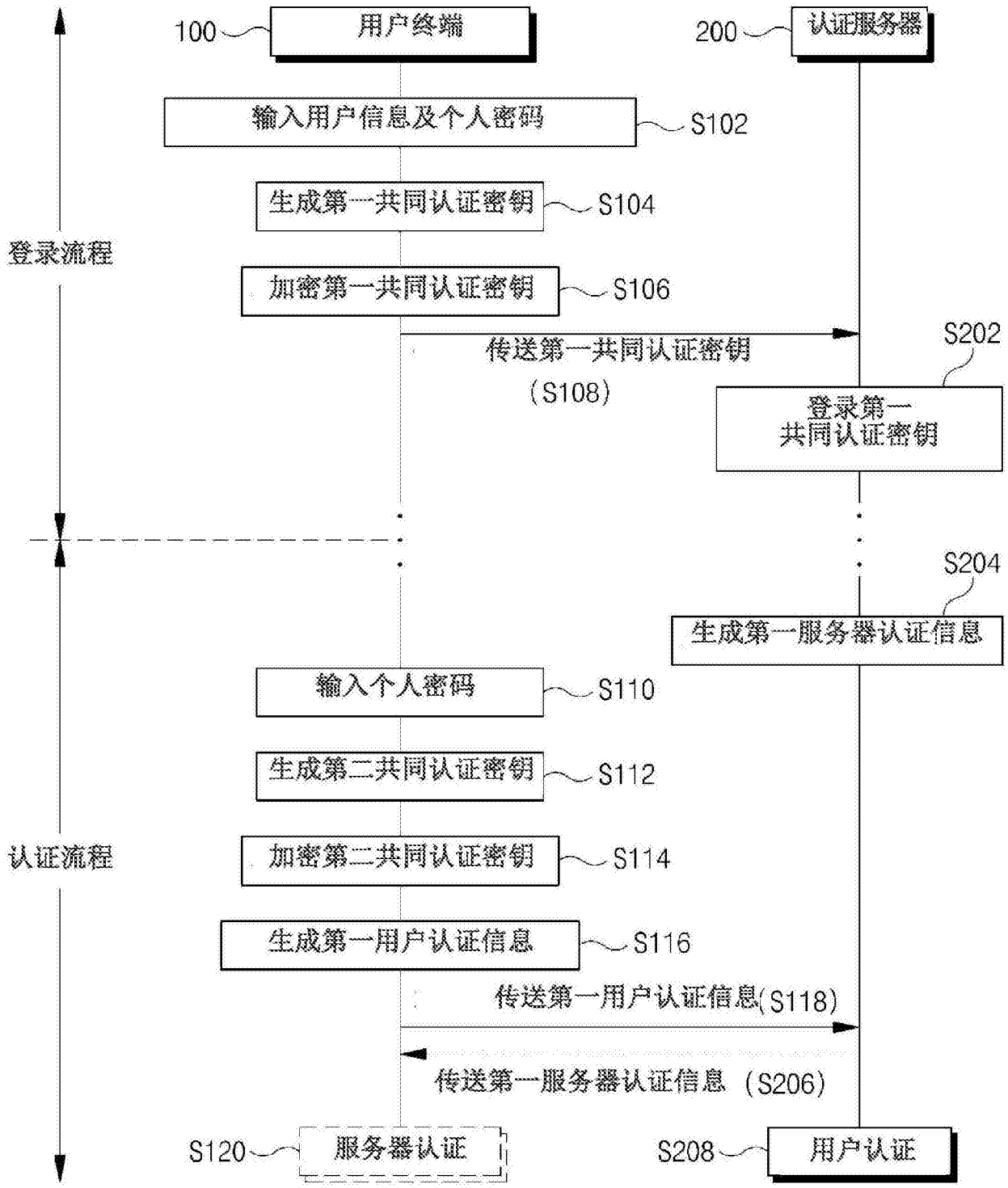

100
用户终端
200
认证服务器
输入用户信息及个人密码
S102
生成第一共同认证密钥
S104
登录流程
加密第一共同认证密钥
S106
传送第一共同认证密钥
(S108)
S202
登录第一
共同认证密钥
S204
生成第一服务器认证信息
输入个人密码
S110
生成第二共同认证密钥
S112
认证流程
加密第二共同认证密钥
S114
生成第一用户认证信息
S116
传送第一用户认证信息(S118)
传送第一服务器认证信息 (S206)
S120
服务器认证
S208
用户认证

图2

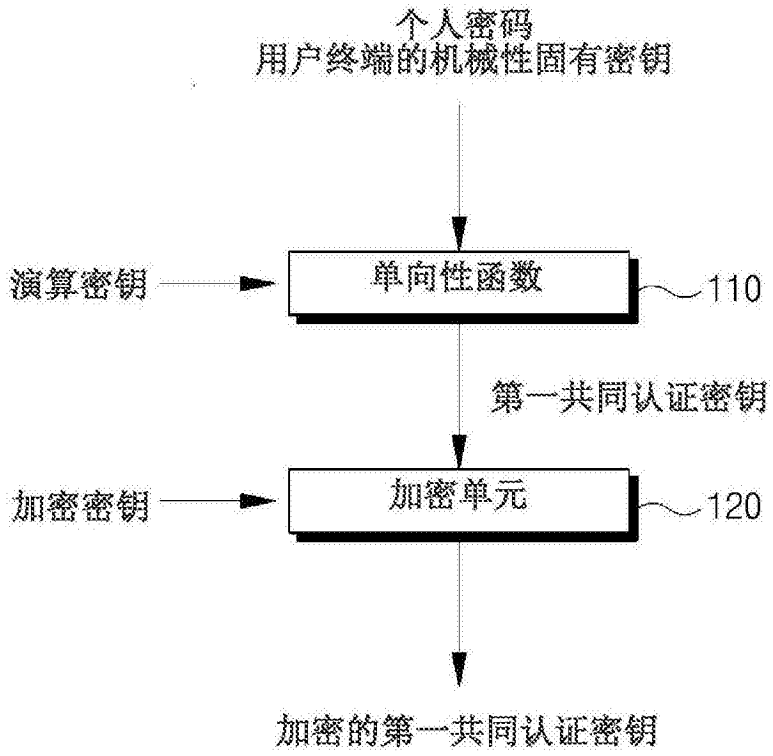
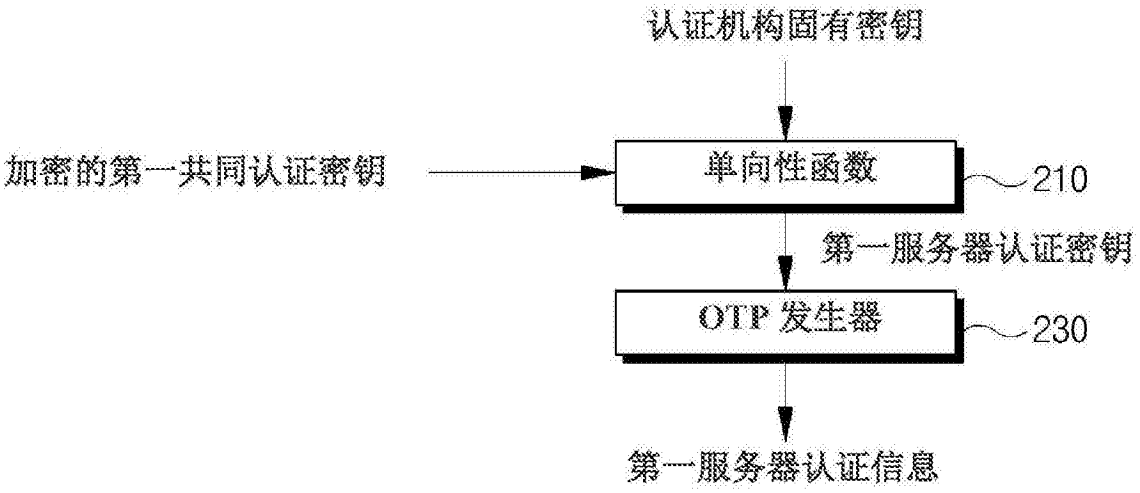
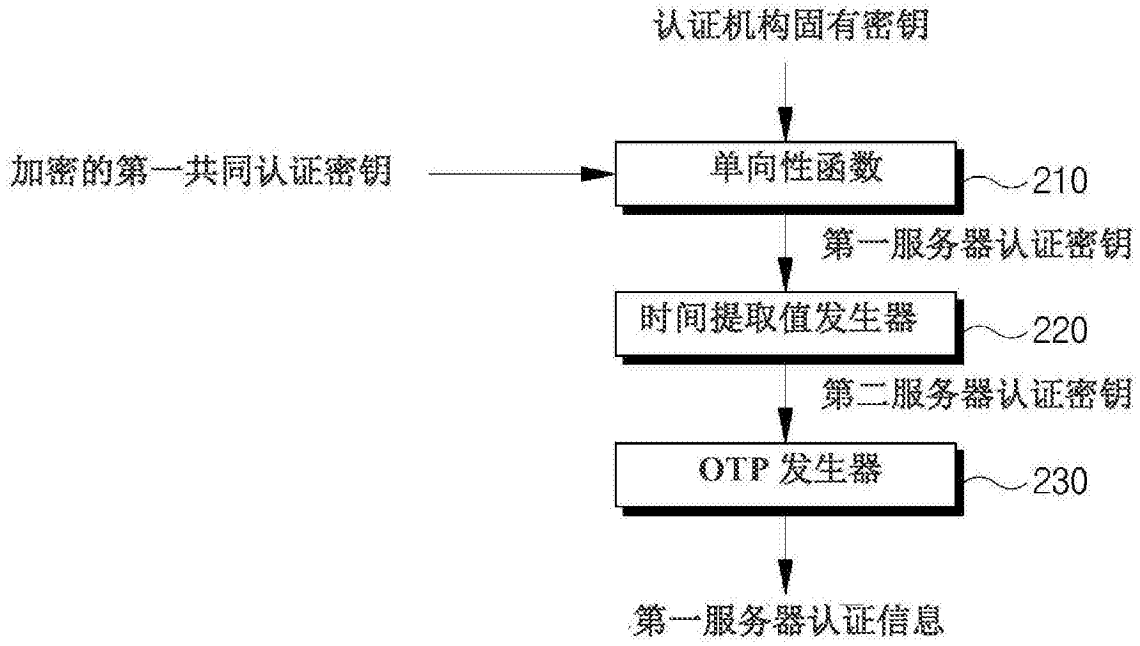

个人密码
用户终端的机械性固有密钥
演算密钥
单向性函数
110
第一共同认证密钥
加密密钥
加密单元
120
加密的第一共同认证密钥

图3

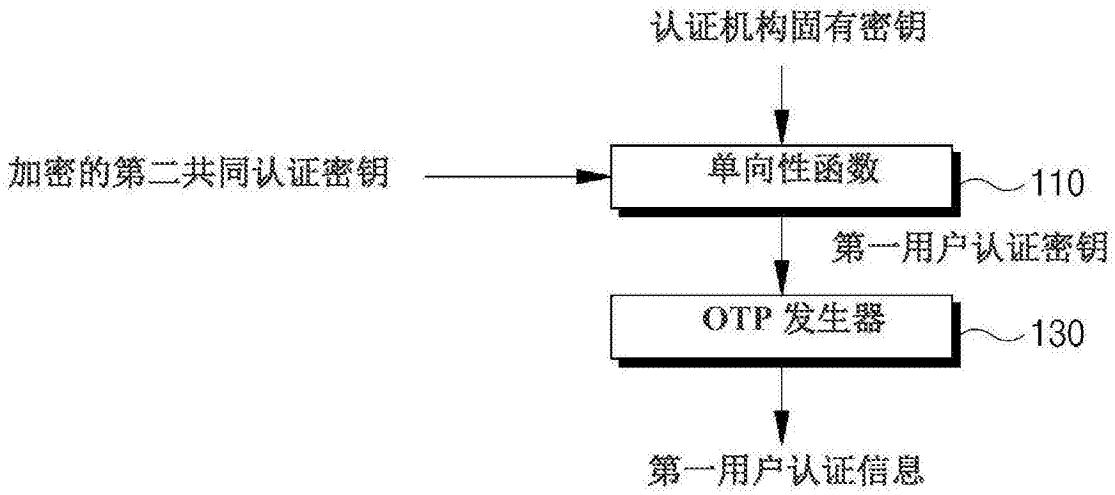

认证机构固有密钥
加密的第一共同认证密钥
单向性函数
210
第一服务器认证密钥
OTP 发生器
230
第一服务器认证信息

(a)

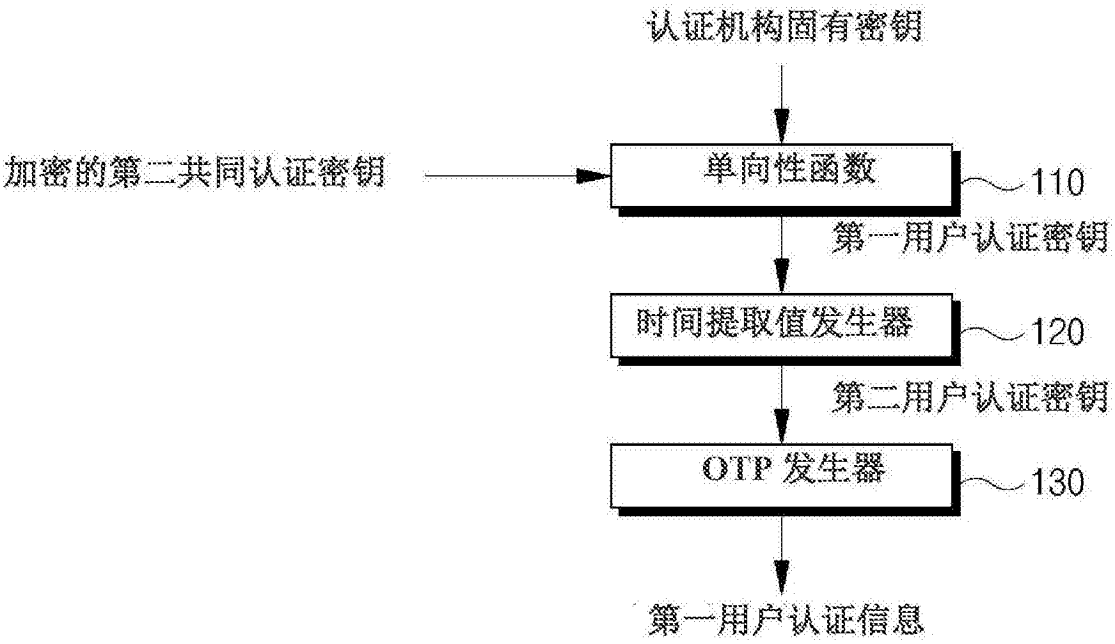

认证机构固有密钥
加密的第一共同认证密钥
单向性函数
210
第一服务器认证密钥
时间提取值发生器
220
第二服务器认证密钥
OTP 发生器
230
第一服务器认证信息

(b)

图4


认证机构固有密钥
加密的第二共同认证密钥
单向性函数
110
第一用户认证密钥
OTP 发生器
130
第一用户认证信息

(a)


认证机构固有密钥
加密的第二共同认证密钥
单向性函数
110
第一用户认证密钥
时间提取值发生器
120
第二用户认证密钥
OTP 发生器
130
第一用户认证信息

(b)

图5

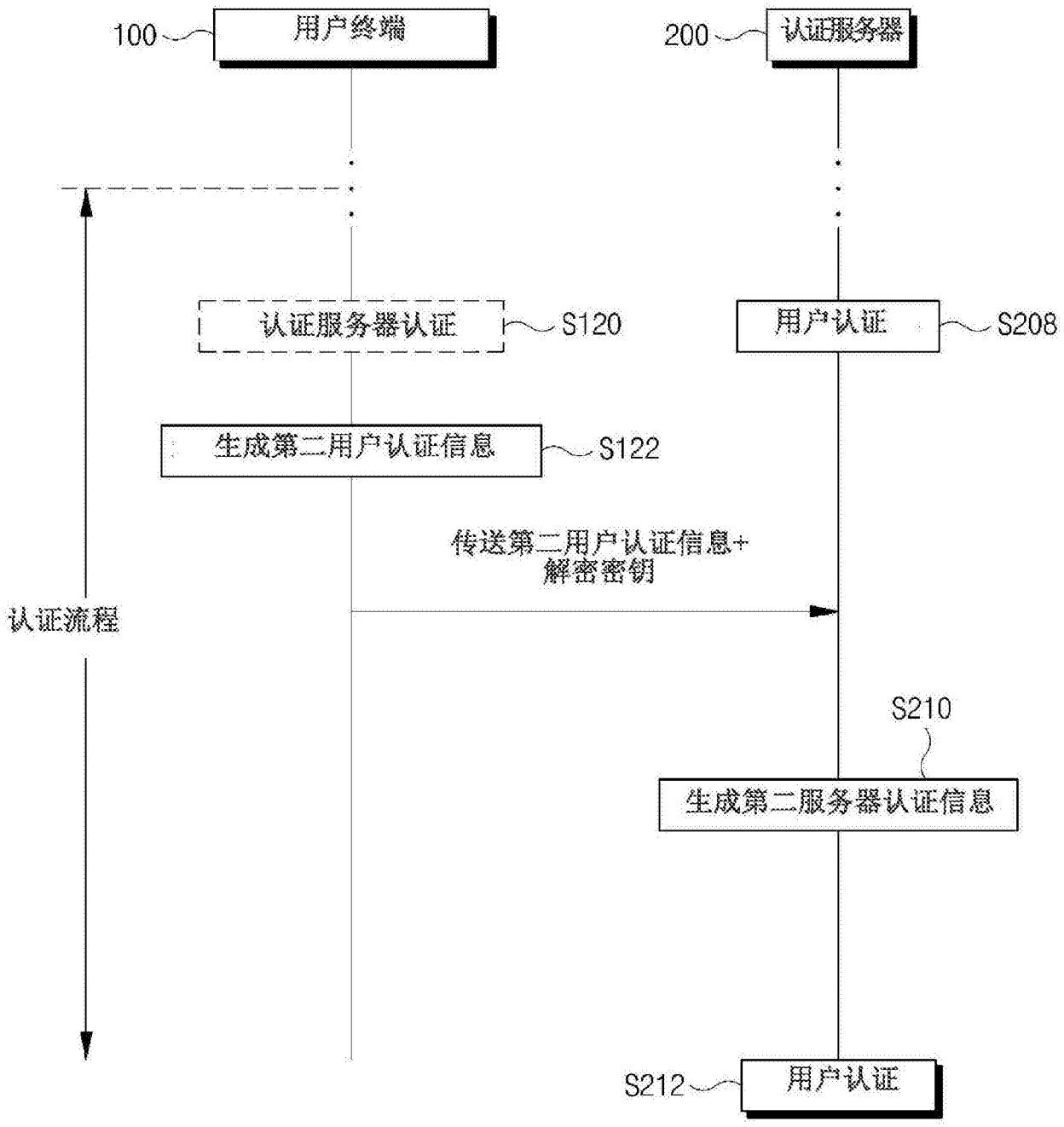
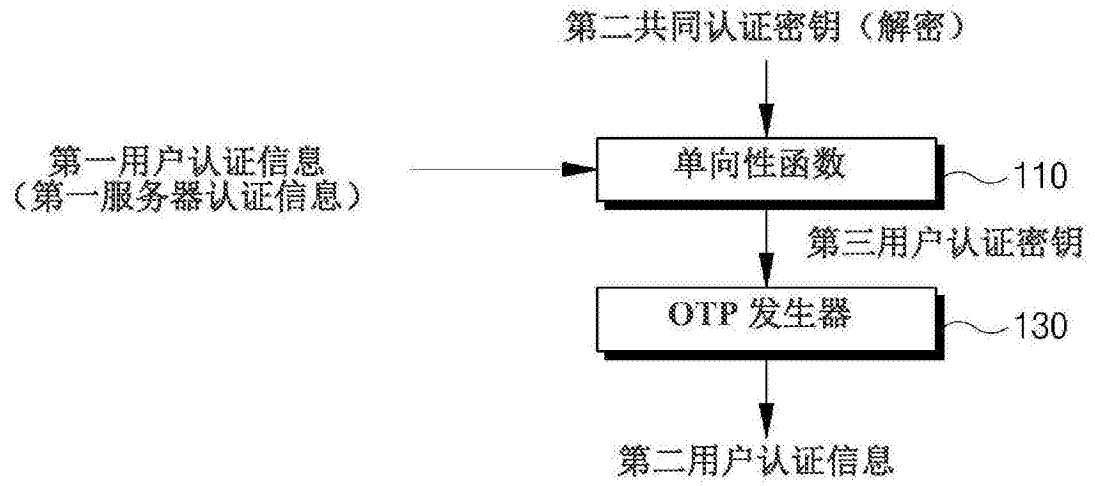
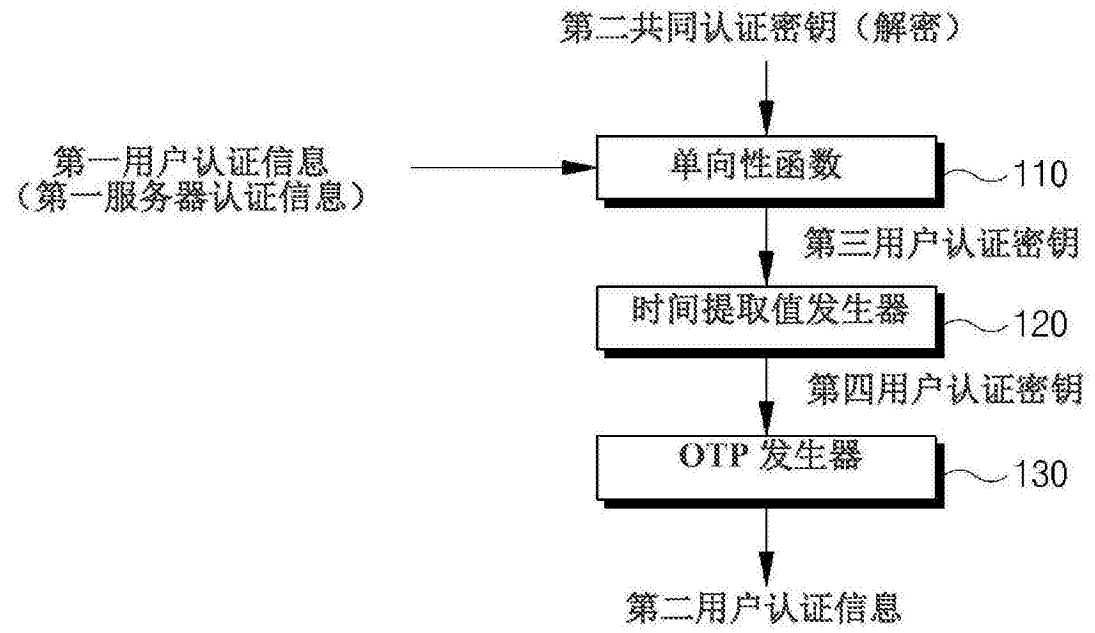

100
用户终端
200
认证服务器
认证服务器认证
S120
用户认证
S208
生成第二用户认证信息
S122
传送第二用户认证信息+
解密密钥
认证流程
S210
生成第二服务器认证信息
S212
用户认证

图6

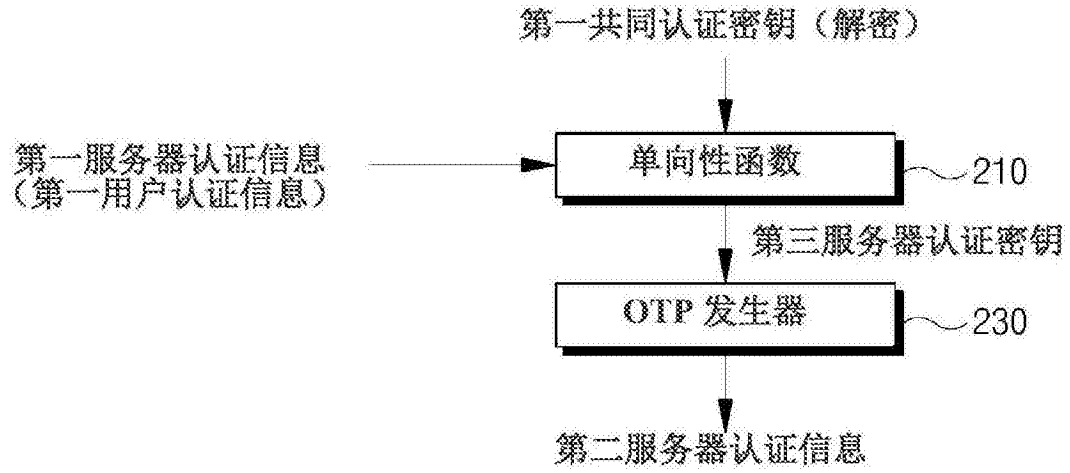

第二共同认证密钥（解密）
第一用户认证信息
（第一服务器认证信息）
单向性函数
110
第三用户认证密钥
OTP 发生器
130
第二用户认证信息

(a)

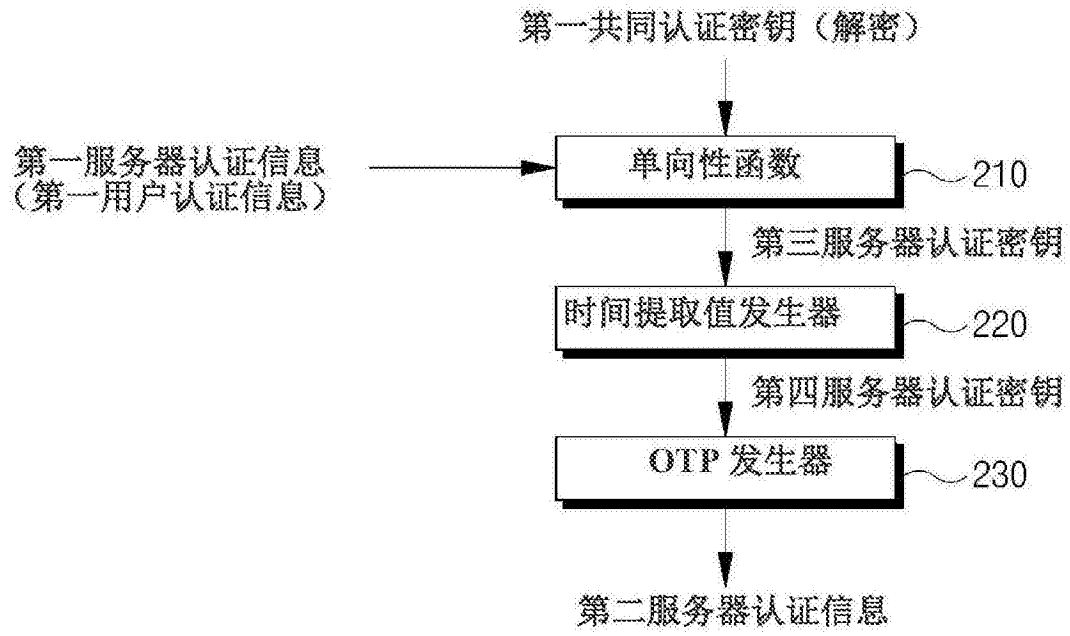

第二共同认证密钥（解密）
第一用户认证信息
（第一服务器认证信息）
单向性函数
110
第三用户认证密钥
时间提取值发生器
120
第四用户认证密钥
OTP 发生器
130
第二用户认证信息

(b)

图7

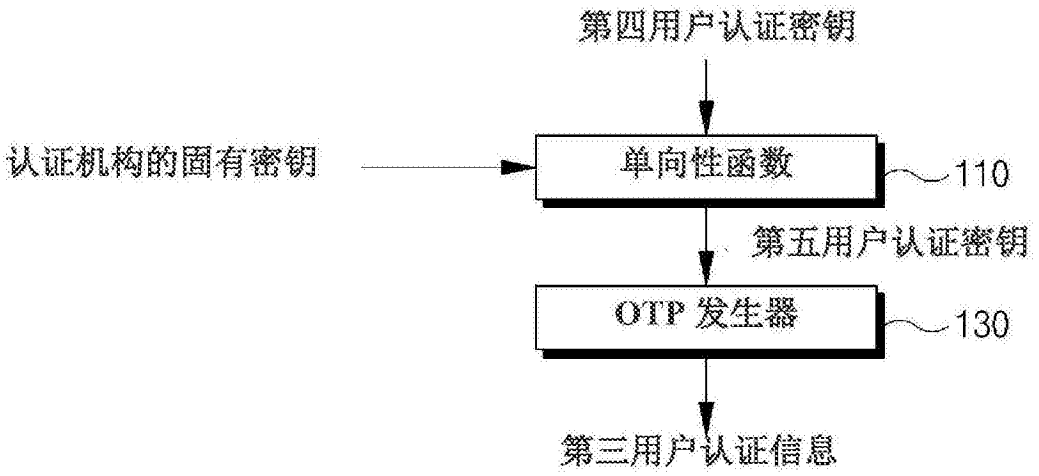

第一共同认证密钥（解密）
第一服务器认证信息
（第一用户认证信息）
单向性函数
210
第三服务器认证密钥
OTP 发生器
230
第二服务器认证信息

(a)

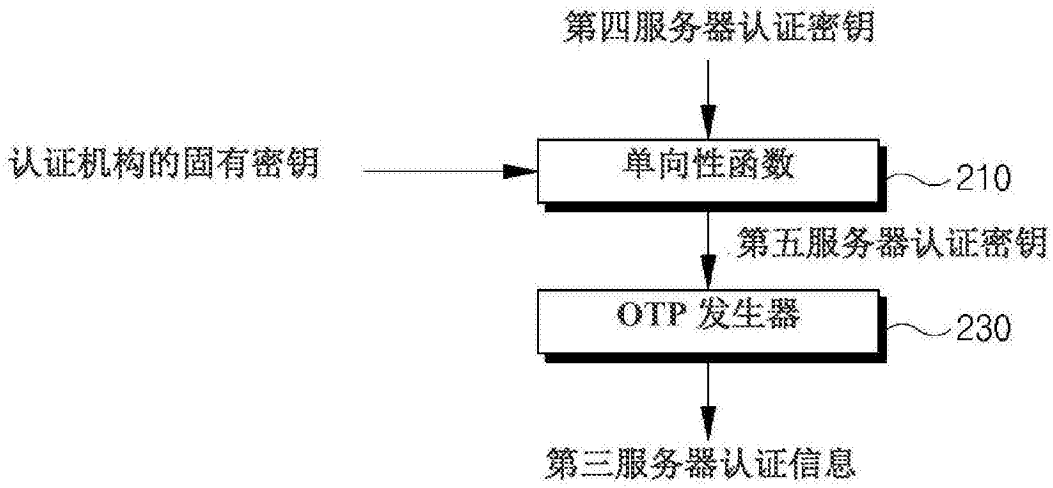

第一共同认证密钥（解密）
第一服务器认证信息
（第一用户认证信息）
单向性函数
210
第三服务器认证密钥
时间提取值发生器
220
第四服务器认证密钥
OTP 发生器
230
第二服务器认证信息

(b)

图8


第四用户认证密钥
认证机构的固有密钥
单向性函数
110
第五用户认证密钥
OTP 发生器
130
第三用户认证信息

(a)


第四服务器认证密钥
认证机构的固有密钥
单向性函数
210
第五服务器认证密钥
OTP 发生器
230
第三服务器认证信息

(b)

图9

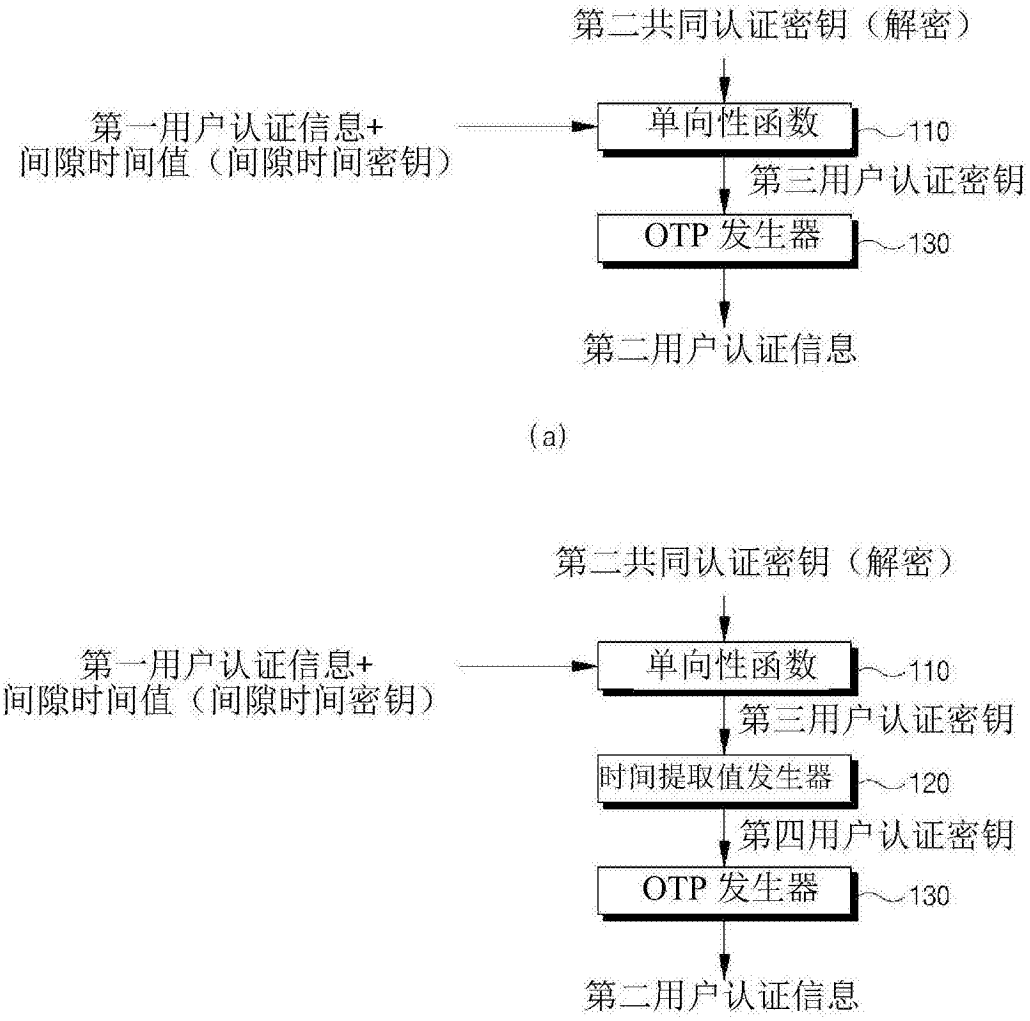
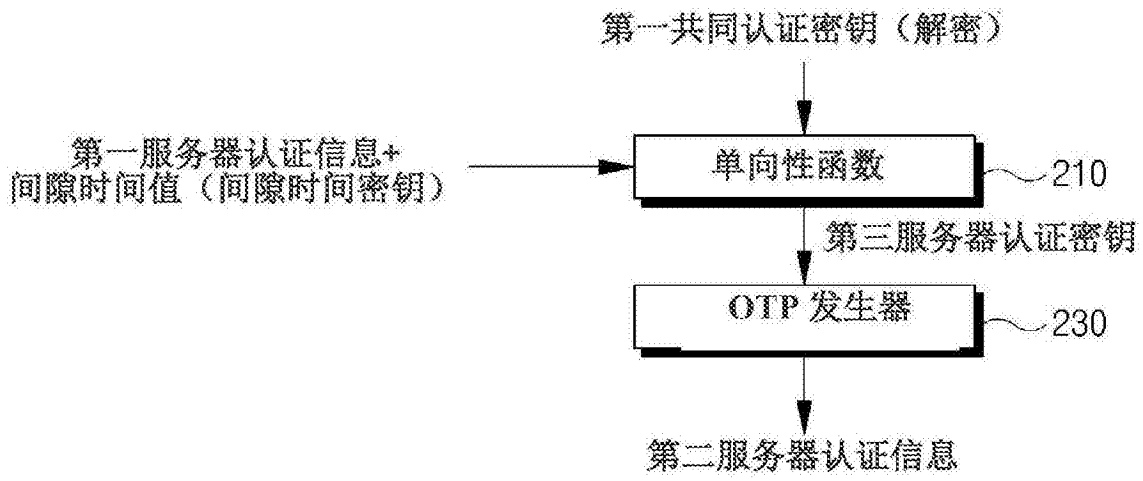
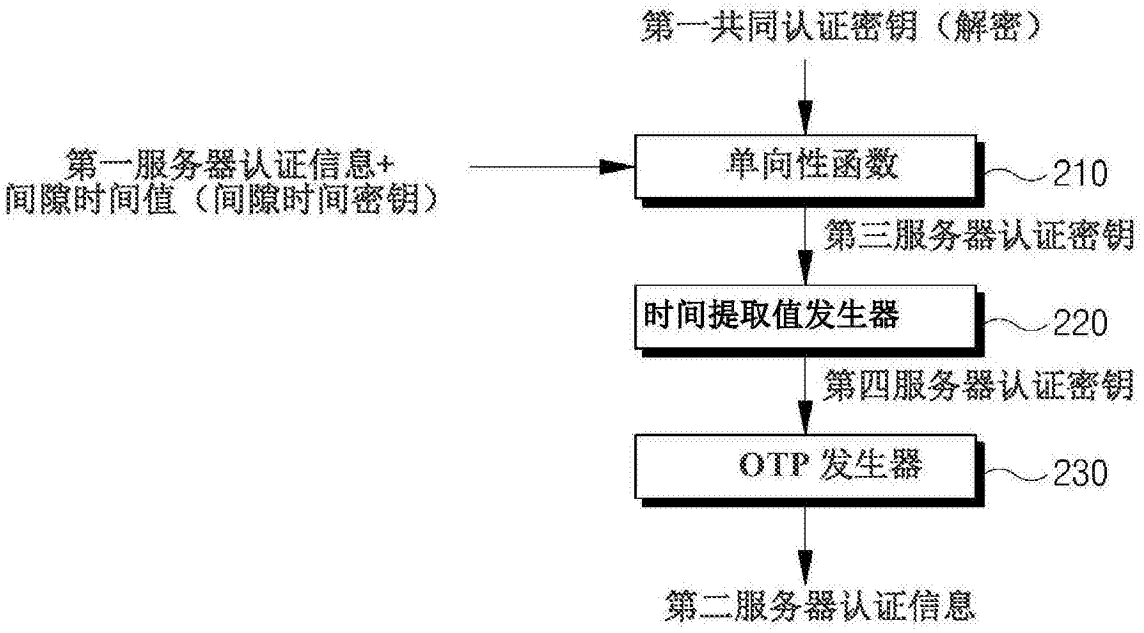

第二共同认证密钥（解密）
第一用户认证信息+
间隙时间值（间隙时间密钥）
单向性函数
110
第三用户认证密钥
OTP 发生器
130
第二用户认证信息
(a)
第二共同认证密钥（解密）
第一用户认证信息+
间隙时间值（间隙时间密钥）
单向性函数
110
第三用户认证密钥
时间提取值发生器
120
第四用户认证密钥
OTP 发生器
130
第二用户认证信息
(b)

图10


第一共同认证密钥（解密）
第一服务器认证信息+
间隙时间值（间隙时间密钥）
单向性函数
210
第三服务器认证密钥
OTP 发生器
230
第二服务器认证信息

(a)


第一共同认证密钥（解密）
第一服务器认证信息+
间隙时间值（间隙时间密钥）
单向性函数
210
第三服务器认证密钥
时间提取值发生器
220
第四服务器认证密钥
OTP 发生器
230
第二服务器认证信息

(b)

图11

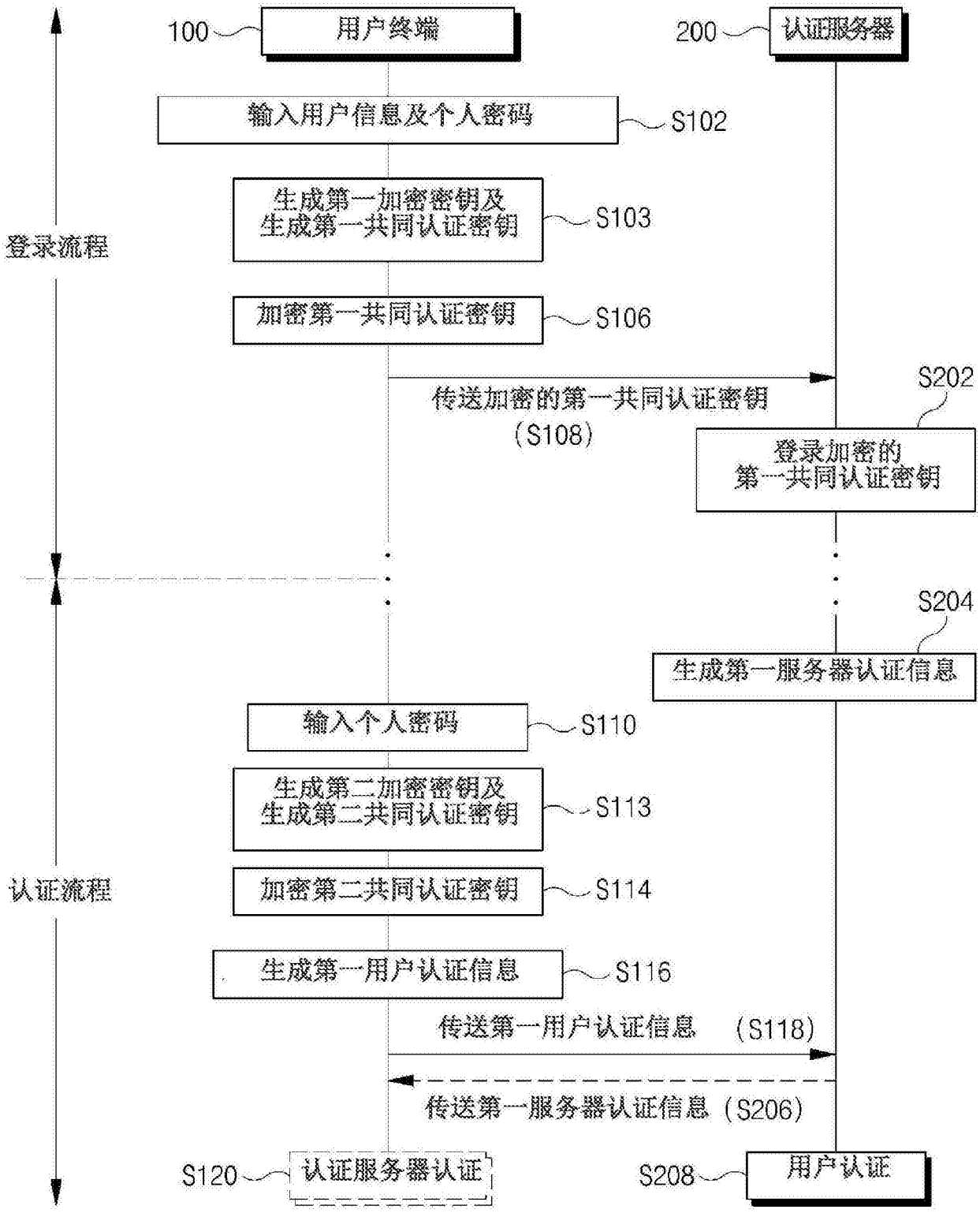

100
用户终端
200
认证服务器
输入用户信息及个人密码
S102
生成第一加密密钥及
生成第一共同认证密钥
S103
登录流程
加密第一共同认证密钥
S106
S202
传送加密的第一共同认证密钥
(S108)
登录加密的
第一共同认证密钥
S204
生成第一服务器认证信息
输入个人密码
S110
生成第二加密密钥及
生成第二共同认证密钥
S113
认证流程
加密第二共同认证密钥
S114
生成第一用户认证信息
S116
传送第一用户认证信息 (S118)
传送第一服务器认证信息 (S206)
S120
认证服务器认证
S208
用户认证

图12

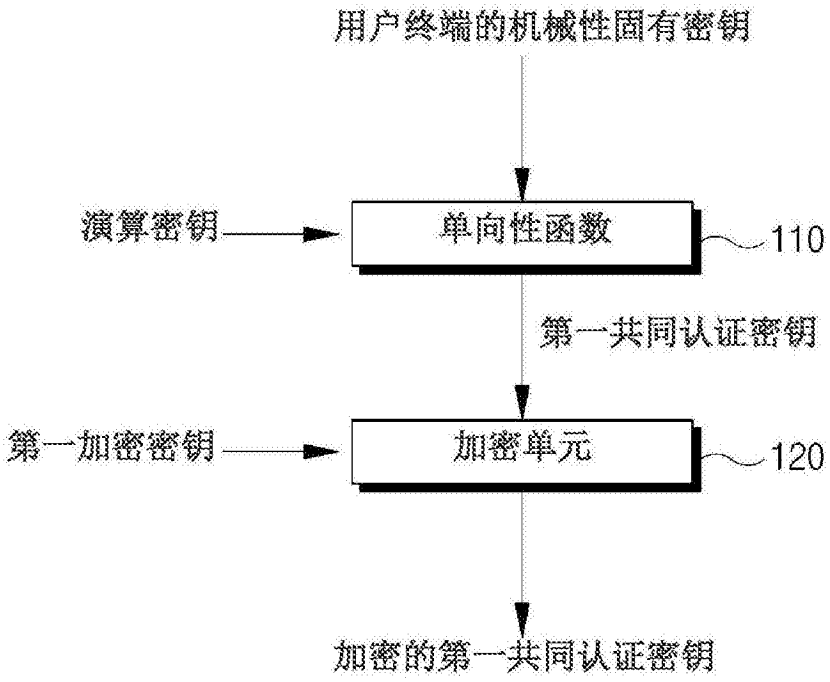

用户终端的机械性固有密钥
演算密钥
单向性函数
110
第一共同认证密钥
第一加密密钥
加密单元
120
加密的第一共同认证密钥

图13

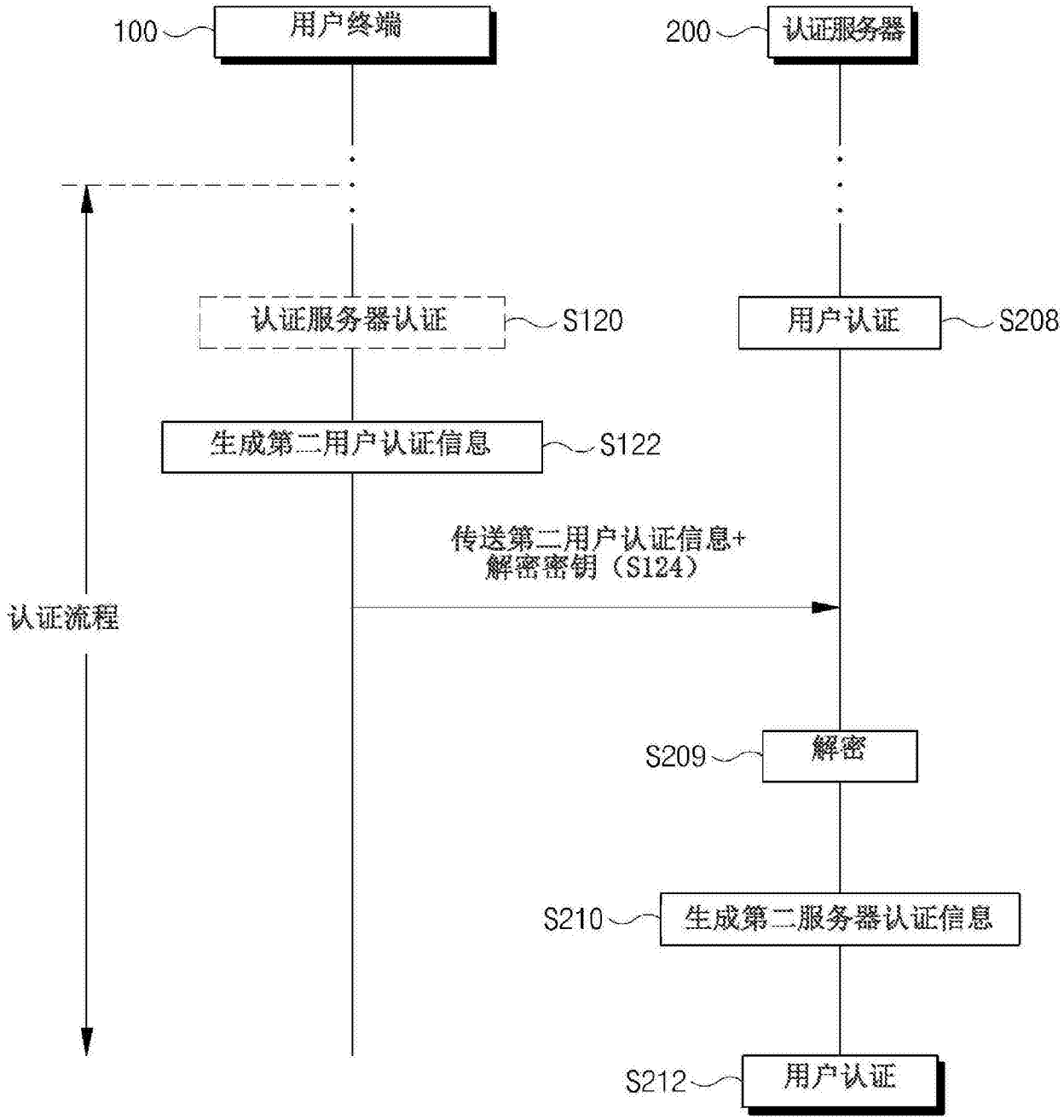

100
用户终端
200
认证服务器
认证服务器认证
S120
用户认证
S208
生成第二用户认证信息
S122
传送第二用户认证信息+
解密密钥（S124）
认证流程
S209
解密
S210
生成第二服务器认证信息
S212
用户认证

图14