(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1910882 B
(45)授权公告日 2010.12.08

(21)申请号 200380111042.2
(22)申请日 2003.12.30
(85)PCT申请进入国家阶段日
2006.08.16
(86)PCT申请的申请数据
PCT/EP2003/014956 2003.12.30
(87)PCT申请的公布数据
WO2005/064881 EN 2005.07.14
(73)专利权人 意大利电信股份公司
地址 意大利米兰
(72)发明人 玛纽·里昂 艾托·E·卡普瑞拉
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 董莘
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
WO 02/054210 A1,2002.07.11, 全文.
CN 1205818 A,1999.01.20, 全文.
CN 1138927 A,1996.12.25, 全文.
WO 03/037016 A1,2003.05.01, 说明书第2页4-16、第4页10行－第5页第2行、第7页20行－第8页20行.
CN 1434388 A,2003.08.06, 全文.
审查员 李刚

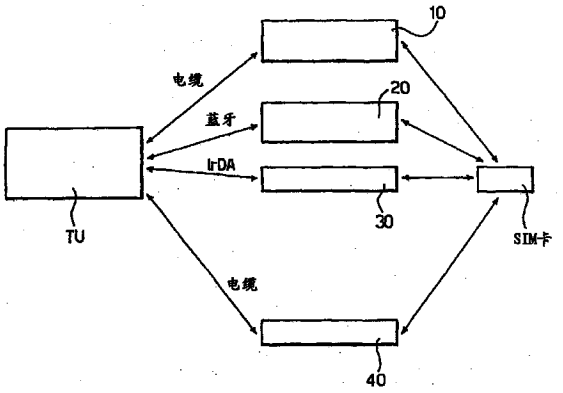
权利要求书 2 页 说明书 10 页 附图 5 页

(54)发明名称

保护数据的方法和系统、相关通信网络以及计算机程序产品

(57)摘要

一种安全地存储用于密码处理的至少一个用户的专有信息项，例如私钥(KID)的方法，包括下述步骤：提供一个通信网络(TU、KR、IWF)，其中所述用户被分配响应的用户身份模块(SIM)，用户身份模块(SIM)存储至少一种保密算法(A8)；借助所述至少一种保密算法(A8)产生密码密钥(K)；和提供所述用户可通过通信网络访问的远程存储位置(KR)，其中用户的专有信息项被存储为借助密码密钥(K)加密的文件。



CN 1910882 B

1. 一种安全地存储至少一个用户的专有信息项的方法，其特征在于，所述方法包括下述步骤：

- 向所述用户分配相应的用户身份模块，所述用户身份模块存储至少一种保密算法；

- 借助所述至少一种保密算法，产生至少一个密码密钥；和

- 提供所述用户通过通信网络可访问的远程存储位置，其中所述用户的专有信息项作为借助所述至少一个密码密钥加密的文件存储在所述远程存储位置中。

2. 按照权利要求 1 所述的方法，其特征在于，所述方法包括下述步骤：

- 通过所述通信网络，接收用户对所述用户的专有信息项的请求 (402)；

- 通过所述通信网络，将所述用户的专有信息项作为所述加密文件发送给所述用户；和

- 利用所述至少一个密码密钥对所述用户处的所述加密文件解密，以检索所述用户的专有信息项。

3. 按照权利要求 1 所述的方法，其特征在于，借助所述至少一种保密算法产生至少一个密码密钥的步骤包括下述步骤：

- 产生至少两个随机值；

- 对所述至少两个随机值应用所述至少一种保密算法，产生至少两个会话密钥；和

- 借助混合函数混合所述至少两个会话密钥，从而产生所述至少一个密码密钥。

4. 按照权利要求 3 所述的方法，其特征在于，所述混合函数是散列函数。

5. 按照权利要求 4 所述的方法，其特征在于，进一步包括将用户特有的秘密信息包括在所述混合函数中的步骤，从而即使根据存储在所述用户身份模块中的任何密钥的知识，所述至少一个密码密钥也是不可预测的。

6. 按照权利要求 1 所述的方法，其特征在于，进一步包括将密码首标包括在所述加密文件中的步骤，所述密码首标包含用于检测所述加密文件的任何未授权修改的密码控制校验和。

7. 按照权利要求 2 所述的方法，其特征在于，进一步包括通过所述远程存储位置接受对所述请求用户的验证有用的所述请求用户的请求 (402)。

8. 按照权利要求 7 所述的方法，其特征在于，通过所述远程存储位置接受对所述请求用户的验证有用的所述请求用户的请求的步骤包括：

依据下述身份项目至少之一，利用所述远程存储位置验证所述请求用户的步骤：用户名称、口令、一次性口令、生物统计系统、基于 SIM 的验证。

9. 按照权利要求 7 所述的方法，其特征在于，通过所述远程存储位置接受对所述请求用户的验证有用的所述请求用户的请求的步骤包括：

由至少一个交互工作功能，利用所述远程存储位置验证所述请求用户的步骤。

10. 按照权利要求 9 所述的方法，其特征在于，由至少一个交互工作功能，利用所述远程存储位置验证所述请求用户的步骤包括下述步骤：

- 使所述用户身份模块与所述交互工作功能相联；

- 检查所述用户身份模块是否包括在于所述通信网络的架构内允许的用户身份模块的列表中；

- 如果所述用户身份模块被允许，那么使所述交互工作功能产生至少一个访问密钥，所

述至少一个访问密钥被用于访问存储为所述远程存储位置中的加密文件的所述至少一个专有信息项。

11. 按照权利要求 10 所述的方法，其特征在于，使所述交互工作功能产生至少一个访问密钥的步骤包括下述步骤：

- 产生至少一个随机数；
- 以验证质询的形式发送所述至少一个随机数；
- 监视对所述验证质询的至少一个对应响应；
- 根据所述至少一个对应响应，确定所述请求用户的成功验证；和
- 根据从这样的组中选择的至少一个实体，产生至少一个所述访问密钥，所述组包括：
- 所述至少一个随机数；和
- 所述至少一个对应响应。

12. 一种安全地存储至少一个用户的专有信息项的系统，其特征在于，所述系统包括：

- 用户身份模块，所述用户身份模块存储至少一种保密算法；
- 包含处理模块的用户终端，所述处理模块能够与所述用户身份模块连接，以便借助所述至少一种保密算法产生密码密钥；
- 可由所述用户经通信网络访问的远程存储位置，所述远程存储位置被配置为将所述用户的专有信息项存储为由所述密码密钥加密的文件。

13. 按照权利要求 12 所述的系统，其特征在于，所述用户终端包括个人计算机、笔记本计算机、膝上型计算机、PDA 或智能电话机。

14. 按照权利要求 12 或 13 所述的系统，其特征在于，所述用户终端通过智能卡阅读器，蓝牙移动终端，IrDA 移动终端或经由电缆的移动终端与所述用户身份模块连接。

15. 一种包括按照权利要求 12-14 任意之一的系统的通信网络。

保护数据的方法和系统、相关通信网络以及计算机程序产品

技术领域

[0001] 本发明涉及保护数据的技术。

背景技术

[0002] 密码术目前被看作在系统和网络中实现安全性的一种基本手段。这种情况下，已对并且正对公钥密码系统加以特别的关注。

[0003] 公钥密码系统建立在只有用户知道他或她的私钥的假定上。该条件是绝对必需的，尤其是在数字签名服务的情况下。为此，用户的私钥通常被存储在特定的保密装置，例如智能卡，USB 令牌或 PCI/PCMCIA 卡中。这些装置的目的是将密钥存储在防窜改存储器中。它们还负责基于这种密钥的所有加密操作，通常目的在于防止密钥本身被传送到外部，以降低泄露秘密的风险。

[0004] 在 WO-A-98/44402 中，提供一种版权保护方案，其中数据一般通过因特网从服务器被下载到客户机以便呈现给用户。通过加密和散列，对下载的数据进行加密保护。当被客户机显示时，关于数据有选择地禁止存储和复制功能，以便防止擅自复制。

[0005] US-A-2003/0097341 公开一种加密数据的方法，一种电信终端和一种访问授权卡，它允许与网络运营商或电信终端的制造商无关地利用一个或多个服务提供商的服务。加密的数据通过电信网络在服务提供商和电信终端之间传送。将通过电信网络传送的数据被加密为选择的服务提供商的函数。

[0006] 另外，WO-A-02/052784 公开一种验证客户机的方法，包括将用户身份发送给验证服务器，基于客户机特有的客户机秘密，获得验证服务器的至少一个质询和至少一个第一秘密。其它步骤包括形成第一凭证，利用所述至少一个第一秘密形成第一验证密钥，利用第一验证密钥加密第一凭证，将所述至少一个质询和加密的第一凭证发送给客户机，形成客户机自己的第一验证密钥。利用自己的第一验证密钥对加密的第一凭证解密。按照这种方法，加密的凭证和至少一个质询被发送给客户机，以致只有当客户机能够从所述至少一个质询得出所述第一秘密时，客户机才能够继续进行验证。

发明内容

[0007] 于是，本发明的目的是提供一种适合于展现关于用户的专有信息项，例如用户的私钥和证书，尤其是当这些专有信息项不适合于存储在“自组织 (ad hoc)”装置中时的灵活性和安全性的方案。

[0008] 更具体地说，本发明的目的在于还保证移动用户也具有高的安全级别，总之，保证使用与网络连接的终端，比如笔记本计算机、便携式计算机、个人计算机、PDA、智能电话机等，并且需要他们的密码密钥来访问保密服务的那些用户具有高的安全级别。

[0009] 根据本发明的一个方面，这样的目的由一种安全地存储至少一个用户的专有信息项的方法实现，其特征在于，所述方法包括下述步骤：

[0010] - 向所述用户分配相应的用户身份模块，所述用户身份模块存储至少一种保密算法；

[0011] - 借助所述至少一种保密算法，产生至少一个密码密钥；和

[0012] - 提供所述用户通过通信网络可访问的远程存储位置，其中所述用户的专有信息项被存储为借助所述至少一个密码密钥加密的文件。

[0013] 根据本发明的另一方面，这样的目的由安全地存储至少一个用户的专有信息项的系统实现，其特征在于，所述系统包括：

[0014] - 用户身份模块，所述用户身份模块存储至少一种保密算法；

[0015] - 包含处理模块的用户终端，所述处理模块能够与所述用户身份模块连接，以便借助所述至少一种保密算法产生密码密钥。

[0016] 根据本发明的另一些方面，这样的目的由相关的通信网络，和可装入至少一个计算机的存储器中的计算机程序产品实现，所述计算机程序产品包括当其在计算机上运行时，执行本发明的方法的步骤的软件代码部分。这里对这样的计算机程序产品的引用意图等同于对包含控制计算机系统，从而协调本发明的方法的性能的指令的计算机可读介质的引用。对“至少一个计算机”的引用显然意图突出按照分布式 / 模块化方式实现本发明的系统的可能性。

[0017] 在从属权利要求和下面的说明中描述了本发明的其它优选方面。

[0018] 具体地说，这里描述的方案通过利用在移动通信的环境中具有高扩散度的装置，即用户身份模块或者说 SIM，提供了所需级别的保护。

[0019] 具体地说，在这里描述的方案中，用户的专有信息项（例如私钥和证书）被存储在远程服务器中，借助只可由和安装在用户终端上的特定处理模块一起工作的用户的 SIM 产生的密钥，通过密码算法得到保护。这样，用户可向具有与所考虑的远程服务器的网络连接的任何终端请求他们的专有信息项。这样的专有信息项被加密传送，并且只有拥有正确的 SIM，即在先前的注册阶段加密了这样的专有信息项的 SIM 的用户才能够使用这样的专有信息项。

[0020] 这样，信息项的使用完全由信息项本身的所有者的 SIM 控制。对加密的专有信息项的访问本身不会暴露关于用户的专有信息项的任何信息。另外，在不可获得用户的 SIM 的情况下，甚至存储加密的专有信息项的远程服务器也不能以明文形式访问用户的专有信息项。这样，即使在受到损害的情况下，远程服务器也将不承担任何特定的责任，将降低安全性方面的任何风险。

[0021] 用户的专有信息项的保护机制不是建立在基于口令的机制上的，也不需要“自组织”硬件。这使得能够压制用于损害整个系统的安全性的所有那些攻击。

[0022] 借助这里描述的方案，用户从而可从具有网络连接，比如因特网连接的任何终端访问他或她的私钥（或任何其它专有信息项）。一旦被 SIM 解密，这样的私钥可直接和安装在终端本身中的软件一起使用。这样的软件通常已适合于按照本地方式使用这样的私钥，和多数 Microsoft™ 平台（Internet Explorer，Outlook，Outlook Express，Explorer，Office 等；这些名称中的至少一些是商标）的情况一样。另外，认为适于按照本地方式，而不借助附加软件地利用用户的私钥和证书的应用程序的数目未来将增大是有道理的。

[0023] 为了向客户机提供更高程度的灵活性和机动性，在用户终端上运行的处理模块可

借助诸如 Java Applet 或 ActiveX 之类技术来实现。这样，处理模块不需要被预先安装在用户终端上，因为在运行时间条件下，即当用户请求访问他或她的私钥时，它可从网页上下载（并被自动安装）。通过利用可在 Java 和 ActiveX 环境中使用的数字签名技术，使用户能够检查下载的软件是否合法，和是否未由黑客为了泄露用户的私钥而恶意开发。

附图说明

[0024] 下面参考附图，举例说明本发明，其中：

[0025] 图 1 是如这里所述的系统的体系结构的例证方框图，

[0026] 图 2、4、6 和 7 是根据这里描述的方案的系统的可能操作的例证流程图，

[0027] 图 3 和 5 是表示这里所述的方案中的数据处理的功能方框图。

具体实施方式

[0028] 这里描述的方案允许移动用户，或者使用诸如笔记本计算机、便携式计算机、个人计算机、PDA、智能电话机之类终端的用户具有当与网络连接时可用的一定的专有信息项，比如私钥和证书。

[0029] 这发生于保密条件下，而不必求助于自组织保密装置，比如智能卡、USB 令牌、PCI/PCMCIA 卡等。

[0030] 借助移动网络的用户目前可获得的保密装置，即用户的用户身份模块 (SIM) 实现专有信息项的保护。

[0031] 具体地说，这里说明的方案使任何公钥基础结构 (PKI)，即其服务建立在公钥密码术方案上的基础结构的用户能够在口令方面具有更高的安全度。即使用户并不拥有智能卡或另一令牌，或者专门用于该用途的硬件装置，也能实现该目的。

[0032] 这里描述的方案要求用户具备 SIM，并且这样的 SIM 可与用户终端连接。这样的用户终端可以是笔记本计算机、便携式计算机、个人计算机、PDA、智能电话机等。

[0033] 目前，使这样的设备与 SIM 连接的方式有几种。

[0034] 例证的列表和图 1 的方框图有关。

[0035] 具体地说，在图 1 中所示的方案中，可借助几种方法使 SIM 与用户终端 TU 连接，例如（但不限于）：

[0036] - 标准的 PCSC 阅读器 10；

[0037] - 经由蓝牙通道的移动电话机 20（用作无线 SIM 阅读器）；

[0038] - 经由 IrDA 通道的移动电话机 30，或者

[0039] - 经由与串行 / 并行 /USB/ 火线端口连接的电缆的移动电话机（用作有线 SIM 阅读器）。

[0040] 技术进展预期将提供连接 SIM 和计算机系统的新装置和协议。本发明包含这样的新装置和协议的可能使用。

[0041] 借助相应的 SIM 并求助于这里描述的方案，用户（下面称为 U）能够：

[0042] - 利用其中加密地存储相应私钥（或者任何其它专有信息项）的密钥仓库 (KR) 验证他或她自己；

[0043] - 请求和下载他或她自己的加密私钥；

[0044] - 借助 SIM 对这样的私钥解密 ;和

[0045] - 本地利用这样的私钥,并且一旦结束使用,可删除所述私钥。

[0046] 本质上,这里描述的方案规定下述部件的存在 :

[0047] SIM :这里使用的 SIM 表示在移动网络,例如 GSM 或 UMTS 网络中分别用于控制和保护用户对网络资源的访问的 SIM 卡或 USIM 卡。具体地说,为了可以接入移动网络,用户必须被验证。在 GSM/UMTS 网络中,这种验证被实现成传统的质询 - 回应机制。网络向用户移动电话机发送称为 RAND 的随机值,用户移动电话机又将该值转发给 SIM。包含称为 Ki 的唯一私钥的 SIM 用称为 A3 的随移动电话运营商而定的算法对该 RAND 加密,以便产生验证回应 SRES。该验证回应 SRES 被返回给网络,知晓 SIM 密钥 Ki 的网络进行相同的计算,并对照用户供给的 SRES 检查其 SRES。如果这两个值相符,那么准许用户接入,否则,接入请求被拒绝。在前一情况下,SIM 也可利用称为 A8 的另一随移动电话运营商而定的算法以及密钥 Ki 对 RAND 值加密,从而产生称为 Kc 的会话密钥。该密钥将被传送给移动电话机,以便保护移动电话机和移动网络收发机站之间的无线电链路。

[0048] 用户 (U) :用户是 SIM 和待保护的私钥 (或者更一般地说,专有信息项) 的所有者。用户 U 可能需要用多种终端,比如笔记本计算机、便携式计算机、个人计算机、PDA、智能电话机等使用这样的私钥。

[0049] 用户终端 (TU) :这里使用的用户终端是与网络连接的终端,所述网络使用户 U 能够联系其中存储有他或她的私钥的密钥仓库 KR。这样的终端还与用户的 SIM 连接 (参见图 1)。适合于供这里描述的方案之用的用户终端 TU 包括 (但不限于) 个人计算机、笔记本计算机、膝上型计算机、PDA、智能电话机。终端可通过各种技术与 SIM 连接,例如,通过智能卡阅读器,蓝牙移动终端,IrDA 移动终端,经由电缆的移动终端。

[0050] 另外,在用户终端 TU 上安装处理模块,所述处理模块适合于与在一侧的密钥仓库 KR,以及在另一侧的用户的 SIM 连接和交换信息。

[0051] 密钥仓库 (KR) :如前所述,密钥仓库是加密存储用户的私钥的远程服务器。这样的远程服务器适合于由用户 U 的终端到达,以便允许访问相应的加密私钥。

[0052] 交互工作功能 (IWF) :它是适合于核实请求访问私钥的那些 SIM 在使用并且有效 (即,它们未被报告为被偷窃、丢失等) 的服务器 (一般在发出 SIM) 的移动电话运营商的控制下)。这样的服务器能够与相应的网络 (例如 GSM 或 UMTS 网络) 连接,具体地说,与所谓的 AuC(验证中心) 连接,以便执行用户 U 的验证功能,或者更准确地说,执行 SIM 的验证功能。从而,它起 IP 网络和 GSM/UMTS 网络之间的验证网关的作用。如下详细所述,交互工作功能 IWF 的存在对这里所说明方案的操作的目的不是必不可少的。但是,本领域的技术人员会认识到互连工作功能的存在可提高整个系统的安全级别。

[0053] 下面的说明只是基于 GSM 网络和相关的 SIM 基础结构,举例说明这里描述的方案的一个可能实施例。本领域的技术人员易于认识到通过采用相关的 USIM 基础结构,这里描述的方案可适用于例如 UMTS 网络的架构内的操作。所述方案可应用于由建立在质询 - 回应方案上的基于加密的用户身份识别基础结构,或者说基本和 SIM 基础结构类似的用户身份识别基础结构支持的任何其它网络架构。

[0054] 于是,这里使用的术语“SIM”意图包含基于相同操作原理的所有这些备选基础结构。

[0055] 表示为TU、KR、IWF的部件（如果存在的话）借助网络技术和协议连接。为此，可以使用标准方案或者专用方案。下面的说明只是作为例子涉及由IETF（因特网工程任务组）定义的标准技术和协议，IETF是负责在IP网络内使用的协议的标准化的主要国际机构。

[0056] 在下面说明的方案中提供的用于查找和解密用户的私钥的步骤可由存在于用户终端TU上的处理模块实现。如所述那样，这样的处理模块不必预先安装在终端上。它可容易地从用户U所连接的网站在线下载。

[0057] 各种技术，比如Java和ActiveX可被用于此用途。这些技术允许借助TAG，直接将可执行目标代码包括在网页内。在检测到Java或ActiveX小程序的存在之后，适合于支持这种技术的浏览器，比如Internet Explorer、Netscape Navigator或Opera能够本地下载对应的代码，并提供所述代码的执行。

[0058] 这两种策略都允许定义当下载可执行代码时的安全策略。具体地说，存在以这样的方式配置浏览器的可能性，即只下载带有数字签名的Java或ActiveX小程序。这主要是为了减少下载所谓的“maleware”，即，编写目的仅仅在于泄露用户的数据或者未经授权地访问用户的终端TU的软件的风险。

[0059] 其它解决方案适合于同样的用途，例如借助网络协议，比如FTP、TFTP、HTTP下载可执行代码。另一方面，所需的代码可借助其它装置，例如CD、软盘、USB令牌等被预先安装。当然，就保证更宽的设备作用范围来说，在线下载可能是更可取的。

[0060] 下面将讨论两个基本过程，即：

[0061] -用户注册过程，和

[0062] -用户对私钥的访问

[0063] 用户注册过程目的在于利用密钥仓库KR创建借助SIM加密的包含私钥的那些文件与SIM本身的联系。

[0064] 执行这样的过程最初是为了注册用户U，随后每当用户U希望修改由SIM产生的他或她的私钥时，所述过程又保护所述私钥（或者更一般地说，用户的专有信息项）。

[0065] 用户注册过程可在受控和受保护的情况下在本地环境执行，或者远程地在专用或公共网络上执行。在后一情况下，通信的完整性、验证和机密性连同对回应攻击的防护一起被保持。这可根据本领域中已知的各种解密方案，比如IPsec、SSL/TLS、SSH等实现。

[0066] 如图2中所示，用户注册过程涉及前面详述的步骤。

[0067] 在第一步骤100中，用户U使他或她的终端TU与用户的SIM连接。为此，可使用各种解决方案，如图1中所示。

[0068] 具体地说，用户U在他或她的终端TU上激活适合于根据这里描述的机制，借助SIM加密与私钥对应的那些文件的处理模块。处理模块检查SIM是否借助图1中所示的通道10-40之一与用户终端TU连接。

[0069] 一旦检测到SIM，那么处理模块检查保护访问的PIN的可能存在。这种情况下，要求用户U通过例如图形用户界面(GUI)输入对应的PIN。

[0070] 随后，在步骤102中，处理模块访问SIM（可能借助用户U提供的PIN），并在步骤104中产生两个随机值RAND1和RAND2，具体地说两个128位的随机值。这些随机值RAND1和RAND2被转发给SIM。

[0071] 在步骤106中，SIM根据SIM的私钥Ki和A8GSM保密算法，计算两个会话密钥Kc1

和 Kc2，每个会话密钥包括 64 位。A8GSM 保密算法表示存储在 SIM 中的基本保密算法。这方面的具体细节可从GSM Technical Specification GSM 03.20(ETSI TS 100929v8.1.0)："Digital cellular telecommunication system(Phase2+);Security Related network functions", EuropeanTelecommunications Standards Institute, July 2001；或者从 GSMTechnical Specification GSM 11.11(ETSI TS 100977v8.3.0):"Digitalcellular telecommunication system(Phase 2+);Specification of theSubscriber Identity Module-Module Equipment(SIM-ME)interface", European Telecommunications Standards Institute, August 2000 得到。

[0072] 这样的计算基于由处理模块提供的两个随机值 RAND1 和 RAND2。简单地说，Kc1 = A8(RAND1) 和 Kc2 = A8(RAND2)。这两个会话密钥 Kc1 和 Kc2 被回送给处理模块，处理模块在下一步骤 108 中通过对两个会话密钥 Kc1 和 Kc2 的并置应用散列函数 h，计算包括 128 位的加密密钥 K。简单地说，K = h(Kc1, Kc2)。有关这种处理的一般信息可在 A.J.Menezes, P.C.van Oorscot, S.A.Vanstone,"Handbook of Applied Cryptography", CRC Press, ISBN:0-8493-8523-7, October 1996 中找到。

[0073] 不同的函数可被用于此目的，例如（但不限于）SHA-1 函数或 MD5 函数。

[0074] 通过还利用借助验证质询（随机值）RAND1 和 RAND2 获得的验证响应 SRES，还可以不同的方式计算加密密钥 K。一般来说，加密密钥 K 可被计算成两个会话密钥 Kc1 和 Kc2，以及通过验证质询 RAND1 和 RAND2 获得的验证回应 SRES1、SRES2 的函数：K = f(Kc1, Kc2, SRES1, SRES2)。这样，通过作用于处理的输入的数目，能够改变加密密钥长度。例如，通过发送一系列的验证质询 RAND1, RAND2, ..., RANDn，并处理 SIM 的对应输出 Kc1, Kc2, ..., Kcn, SRES1, SRES2, ..., SRESn，能够增大待处理的输入的数目。于是这种情况下，K = f(Kc1, Kc2, ..., Kcn, SRES1, SRES2, ..., SRESn)。

[0075] 另外，用户 U 可加入个人化的私钥 K_U，以便改变加密密钥 K，以致加密密钥 K 不再仅仅取决于 GSM 保密函数。这样，在没有用户的积极合作的情况下，即使是知道关于用户的 SIM 的所有数据的移动网络运营商也不能实现用户 U 的私钥的密钥恢复功能。在后一情况下，产生加密密钥 K 的函数可由公式：$K = f(K_U, Kc1, Kc2, ..., Kcn, SRES1, SRES2, ..., SRESn)$ 表示，其中 K_U 是用户 U 选择的个人化私钥。

[0076] 随后在步骤 110 中，处理模块还可产生一个随机向量（定义的初始化向量 IV，它包括例如 128 位。当使用请求初始化向量的加密方式，例如 CBC（密码块链接），CFB（密码反馈），OFB（输出反馈）时，在密码处理（加密 / 解密）中使用这样的随机向量。根据加密实体的操作模式，初始化向量 IV 也可被省略；例如，在 ECB（电子密码本）的情况下，不需要初始化向量 IV。在前面已提及的 Menezes 等的参考文献中提供了上面涉及的各种密码处理方法的细节）。

[0077] 在步骤 112 中，处理模块借助加密密钥 K 和随机向量 IV，例如在 CBC 模式下通过利用 AES 密码，对与用户私钥（或者专有信息项）对应的文件加密。可以使用任何其它对称加密方法，例如（但不限于）RC6、Twofish、Serpent、3DES。可选的是，在应用加密函数之前，处理模块可压缩包括私钥的文件。为此，可使用各种无损算法，例如（但不限于）：PKZIP、GZIP、RAR、ACE、ARJ、LZH。产生的加密数据由图 3 中的附图标记 ED 表示。

[0078] 处理模块还在加密的文件中插入密码首标 CH 以便解密。

[0079] 如图 3 中所示，所述密码首标 CH 包括下述字段：

[0080] -RAND1 和 RAND2，即发送给 SIM 以便构成加密密钥 K 的两个随机值（验证质询）；

[0081] -IV，即可用于加密（要求这种参数的 CBC 或其它加密方式）并由处理模块产生的随机向量；

[0082] -Version：这是一个辅助字符串，它整理处理模块版本，使用的加密算法 (AES、RC6、3DES 等)，使用的加密方式 (CBC、ECB、OFB 等)，使用的散列函数 (SHA-1、MD5、RIPEMD、Tiger 等)、可能使用的压缩算法 (PKZIP、RAR、ARJ) 和其它有用的信息；和

[0083] -MAC_K(RAND1，RAND2，IV，Version，加密的文件)，它是关于加密的文件及三个在先字段的密码控制校验和。这样的密码控制校验和可利用 MAC（消息验证码）函数来产生。这种 MAC 函数的例子是例如 HMAC-SHA-1、HMAC-MD5、AES-XCBC-MAC。下面将假定使用函数 HMAC-SHA-1。总之，这样的密码控制校验和还检测对加密文件的任何可能的未授权修改。

[0084] 返回图 2 的流程图，在步骤 114 中，加密的文件连同 SIM 标识符一起被传递给密钥仓库 KR，其中加密文件被存储在数据库内。可利用各种元素来充当 SIM 标识符。这些元素的例子是 IMSI（国际移动站身份 - 现在的国际移动用户身份），MSISDN（移动用户 ISDN 号），SIM 序号等。下面将假定使用 IMSI 标识符。最后，密钥仓库 KR 可将 SIM 标识符发送给交互工作功能 IWF（如果存在的话），以便将用户的 SIM 插入可使之提供这样的服务的那些 SIM 的列表中。

[0085] 允许用户 U 访问加密文件的过程意图是允许用户 U 在 SIM 的控制下，保密地访问和本地下载私钥（或者任何其它专有信息项）。这样的访问可从具备前面说明的处理模块，并与密钥仓库 KR、SIM 并且可能与交互工作功能 IWF 连接的任何用户终端 TU 发生。

[0086] 具体地说，如图 4 中所示，这里描述的方案的优选实施例提供用户 U 和交互工作功能 IWF 之间的第一交互作用。这样的交互作用目的在于借助 SIM 验证用户，并和用户 U 和交互工作功能 IWF 共同创建随后将用于与密钥仓库 KR 通信的访问密钥 K_{IWF}。图 4 中图解说明的步骤也可在共享网络上实现。

[0087] 下面将假定用户 U 恰当地使他或她自己的终端 TU 与 SIM 连接。这可通过借助于图 1 中图解说明的各种技术方案来实现。

[0088] 在步骤 200 中，用户 U 在他或她的终端上激活处理模块，该处理模块借助诸如 SSL/TLS 之类的协议与交互工作功能 IWF 连接。利用诸如 SSL/TLS 之类的协议使用户 U 能够借助目前可和各种平台，比如 Windows 9X/Me/NT/2000/XP/PocketPC/CE，Linux，Sun Solaris 等中的网络浏览器（例如 Internet Explorer，Netscape Navigator，Opera）使用的常规技术（例如数字证书）来验证交互工作功能 IWF。

[0089] 还可使用适合于提供服务器的验证（即，交互工作功能 IWF 的验证），通信机密性，通信完整性和防范回应攻击的任何其它等同协议。

[0090] 此时分别在两个步骤 202 和 204 中，用户终端 TU 请求并从 SIM 获得标识符。由 IMSI 表示的 SIM 标识符在步骤 206 中被发送给交互工作功能 IWF。

[0091] 交互工作功能 IWF 通过将由随机产生的数字构成的两个验证质询 RAND1 和 RAND2 发送给用户 U，执行两个典型的 GSM 验证步骤，并控制对应的验证响应 SRES1 和 SRES2。这在随后的步骤中发生。在步骤 208 和 210 中，这两个验证质询通过用户终端 TU 从交互工作功能 IWF 发送给 SIM。在接下来的两个步骤 212 和 214 中，验证响应 SRES1 和 SRES2 通过用

户终端 U 从 SIM 回送给交互工作功能 IWF。

[0092] 在步骤 216 中，成功的 GSM 验证由交互工作功能 IWF 传送给用户终端 TU，（当然该步骤也可传送异常中断的 GSM 验证的信息，这种情况下，该过程被中断）。

[0093] 如果继续该过程，那么交互工作功能 IWF 和用户 U 本地产生计算为 K_{IWF} = h(Kc1，Kc2) 的访问密钥 K_{IWF}。各个步骤基本上和前面结合图 2 的步骤 104-108 描述的那些步骤类似。

[0094] 交互工作功能 IWF 将访问密钥 K_{IWF} 存储在 IWF 数据库中。

[0095] 另外，交互工作功能 IWF 将访问密钥 K_{IWF} 与 SIM 标识符，即 IMSI 的联系，连同其它日志信息，比如最后的访问数据 LA，前一访问密钥 $K_{old-IWF}$ 等存储在 IWF 数据库中。图 5 中表示了对应的数据结构，它是适合于被存储在 IWF 数据库中的例证典型记录。

[0096] 另外在这种情况下，存在根据不同策略产生访问密钥 K_{IWF} 的可能性。例如，访问密钥 K_{IWF} 可被计算为 K_{IWF} = f(K_{U-IWF}，Kc1，Kc2，...，Kcn，SRES1，SRES2，...，SRESn)，其中 K_{U-IWF} 是在用户 U 和交互工作功能 IWF 之间的用户注册过程中共享的个人化私钥 K_U，而 SRES1，...，SRESn，Kc1，Kcn 是作为 n 个验证质询 RAND1，..，RANDn 的函数通过 A3 和 A8GSM 保密算法获得的 N 个验证响应和 n 个会话密钥。还可以使用基于 SIM 或不基于 SIM 的其它验证策略。

[0097] 用户终端 TU 中的处理模块随后借助 SSL/TLS 协议等与密钥仓库 KR 连接。这实质上涉及图 6 中的信号交换步骤 300。

[0098] 利用诸如 SSL/TLS 之类的协议使用户 U 能够借助目前可在各种平台 (Windows 9X/Me/NT/2000/XP/PocketPC/CE，Linux，Sun Solaris 等）的网络浏览器（例如 Internet Explorer，Netscape Navigator，Opera) 中可用的常规技术（数字证书）来验证密钥仓库 KR。为此，还可使用适合于提供服务器的验证（即，密钥仓库 KR 的验证），通信机密性，通信完整性和防范回应攻击的任何其它功能等同的协议。

[0099] 随后，处理模块借助请求消息执行对用户私钥的访问请求。为此，在图 6 中的两个步骤 32 和 304 中，用户终端 TU 请求并从 SIM 获得相应的 SIM 标识符 (IMSI)。随后在步骤 306 中，该 SIM 标识符和其它参数一起被发送给密钥仓库 KR，所述其它参数例如是：

[0100] - 被请求的私钥的标识符 ID；这样的参数可识别和相同用户相关的一个或多个私钥；

[0101] - 请求的时间戳记（如果存在的话）；该参数 T 按照各方达成一致的格式，例如 UTC 识别时间；

[0102] -Nonce N_u，即适合于抑制可能的回应攻击的参数；这一般由随机值，序号或时间参数构成。

[0103] 密钥仓库 KR 检查指定的 SIM 是否被注册，在检查结果肯定的情况下，检查参数 T 的一致性。

[0104] 如果检查产生肯定的结果，那么密钥仓库 KR 产生相应的 NonceN_u，并在步骤 308，将由下述信息：IMSI、ID、T、N_U、N_{KR} 构成的消息回送给用户终端 TU。

[0105] 此时，处理模块在收到的消息内检查各种参数的存在和正确性，随后根据访问密钥 K_{IWF} 计算接收的消息的密码控制校验和 MAC_{KIWF}。简单地说，MAC_{KIWF}(IMSI、ID、T、N_U、N_{KR})。这种密码控制校验和随后被返回给密钥仓库 KR（步骤 310）。

[0106] 在下一步骤 312 中，密钥仓库 KR 通过保密通道将下述消息：IMSI、ID、T、N_U、N_{KR}、

MAC_{KIWF}(IMSI、ID、T、N_U、N_{KR}) 发送给交互工作功能 IWF。

[0107] 可借助不同的解决方案保护密钥仓库 KR 和交互工作功能 IWF 之间的通信。例如包括（但不限于）TLS/SSL、IPsec、SSH、专用链路。

[0108] 交互工作功能 IWF 通过使用和 SIM 提供的 IMSI 对应的主搜索关键字访问 IWF 数据库，检查密码控制校验和 MAC_{KIWF} 的正确性。

[0109] 如果检查产生肯定的输出，那么交互工作功能 IWF 从存储在 IWF 数据库中的记录中提取访问密钥 K_{IWF}，并根据接收的数据计算密码控制校验和 MAC_{KIWF}，以便相对于密钥仓库 KR 提供的密码控制校验和 MAC_{KIWF}，检查其正确性。

[0110] 在步骤 314，比较的结果被返回给密钥仓库 KR，同时该操作被存储在对应的日志文件中。

[0111] 当然，上面提及的任意检查的失败导致该过程被异常中断，同时对应的警报被发送给用户 U。

[0112] 在验证成功的情况下，密钥仓库 KR 利用对应于 SIM 提供的 IMSI 的主搜索关键字访问其数据库，以便检索用户 U 请求的，并且在数据库中存在于加密文件中的私钥 K_{ID}。私钥 K_{ID} 随后被回送给用户 U。

[0113] 用户 U 接收加密的文件，并通过使 SIM 根据包含在密码首标 CH 中的信息重构加密密钥 K 的值，对加密文件解密。

[0114] 具体地说，在图 7 的流程图中，步骤 400 和 402 表示基本上和图 2 中的步骤 100 和 102 相同的访问步骤。

[0115] 在步骤 404 中，位于用户终端 TU 的处理模块读取密码首标 CH 中的分别表示两个随机值 RAND1 和 RAND2 的字段 RAND1 和 RAND2 的内容。随机值 RAND1 和 RAND2 被传送给 SIM。

[0116] 在步骤 406 中，SIM 执行两个会话密钥 Kc1 = A8(RAND1) 和 Kc2 = A8(RAND2) 的计算。这两个会话密钥 Kc1 和 Kc2 随后被返回给处理模块。

[0117] 在步骤 408 中，处理模块通过计算应用于两个会话密钥 Kc1 和 Kc2 的并置的散列函数 h，重构加密密钥 K。简单地说，K = h(Kc1,Kc2)。对前面说明的加密密钥 K，还可使用备选的构成技术，从而，加密密钥 K 一般可被表示成 $K = f(K_U, Kc1, Kc2, \ldots, Kcn, SRES1, SRES2, \ldots, SRESn)$。

[0118] 在步骤 410 中，处理模块访问加密文件，并根据刚刚（重新）构成的加密密钥 K，加密文件的内容和包含在密码首标 CH 中的字段 RAND1、RAND2、IV 和 Version，重新计算密码控制校验和 MAC_K。随后比较该值和存在于密码首标 CH 中的密码控制校验和 MAC_K。

[0119] 在比较结果是肯定的情况下，处理模块从密码首标 CH 读取字段 IV（步骤 412），并在步骤 414 中，利用选择的随机向量 IV 和 SIM 重构的加密密钥 K，例如在 CBC 方式下借助 AES 算法对加密的文件解密。

[0120] 用户 U 的私钥 K_{ID} 现在为明文形式，可在存在于用户终端 TU 中的任何兼容软件模块中使用。

[0121] 如前所述，这里描述的方案还可在不提供交互工作功能 IWF 的情况下工作。这种情况下，用户注册过程被修改，以便定义密钥仓库 KR 和用户 U 的验证方法。

[0122] 访问包含私钥的加密文件的过程直接终止于密钥仓库 KR。

[0123] 具体地说，在用户注册过程中，密钥仓库 KR 将按照传统的方式，例如通过借助于共享的用户名 / 口令方案验证用户 U。此时，根据该请求期间的验证阶段的输出，密钥仓库 KR 将确定包含私钥的加密文件是否将被发送给用户 U。

[0124] 这种情况下，验证处理的安全级别较低。但是，由于加密文件一旦被发送并被用户 U 收到，那么该加密文件只能由保护它的 SIM 解密，因此实质上保持了一般的安全级别。

[0125] 当然，密钥仓库 KR 可求助于其它机制，例如（但不限于）一次性口令，生物统计系统，基于 SIM 的验证等验证用户 U。

[0126] 密钥仓库 KR 还可被配置成与交互工作功能 IWF 连接，唯一目的在于检查和接收的 IMSI 对应的 SIM 的状态。换句话说，密钥仓库 KR 中只向交互工作功能 IWF 请求关于与 IMSI 相关的 SIM 是否仍然有效和现用，或者是否被移动电话运营商或用户 U 废除（例如由于丢失，偷窃，发生故障等）的指示。

[0127] 即使不可获得相应的 SIM，这里描述的方案也允许用户恢复私钥。在后一情况下，一旦知道包含私钥 / 信息项的加密文件的密码首标，就能够启动重构加密密钥 K 的过程。

[0128] 这可通过例如保密地将与加密文件相关的密码首标，或者只将两个验证质询（随机值）RAND1 和 RAND2 传送给移动网络的运营商，同时获得对应的验证响应 SRES1 和 SRES2 及两个会话密钥 Kc1，Kc2 来实现。

[0129] 根据这些参数，连同随机向量 IV，字符串 Version 和可能个人化的私钥 K_U，用户 U 将能够重构加密密钥 K，从而对他或她的私钥解密，该私钥可用新的 SIM 保护。

[0130] 本领域的技术人员易于认识到这里描述的方案可用于保护用户 U 存储为机密的任何信息。事实上，这里描述的方案不允许密钥仓库 KR 访问用户文件的明文内容。这使系统进一步使任何种类的文件或数字信息安全，并且适合于保护所述任何种类的文件或数字信息。

[0131] 如同所述那样，这里描述的方案还适合于和其它类似的 SIM 卡，比如 UMTS SIM（目前称为 USIM）一起工作。USIM 包含和 GSM 系统的保密功能类似的保密功能 :基于使密码密钥的产生能够如前所述那样使用的一个或多个验证质询 RAND。

[0132] 另外，在 UMTS 的情况下，单个验证质询 RAND 适合于产生几个密钥 (CK、IK 等)，从而使得能够将单个随机质询 RAND 用于构成加密密钥，以便用于保护用户的私钥。

[0133] 另外，要认识到这里使用的在专有信息项和通过至少一个密码密钥加密的对应文件之间的“密码处理”转换意图适用于对专有信息项加密，产生对应的加密文件，或者通过解密对应的加密文件恢复专有信息项，或者甚至组合上述加密和解密。

[0134] 于是，在不损害本发明的基本原理的情况下，细节和实施例可变化，而不会脱离如下面的权利要求中限定的本发明的范围，另外重要的是，前面描述的只是对本发明的举例说明。

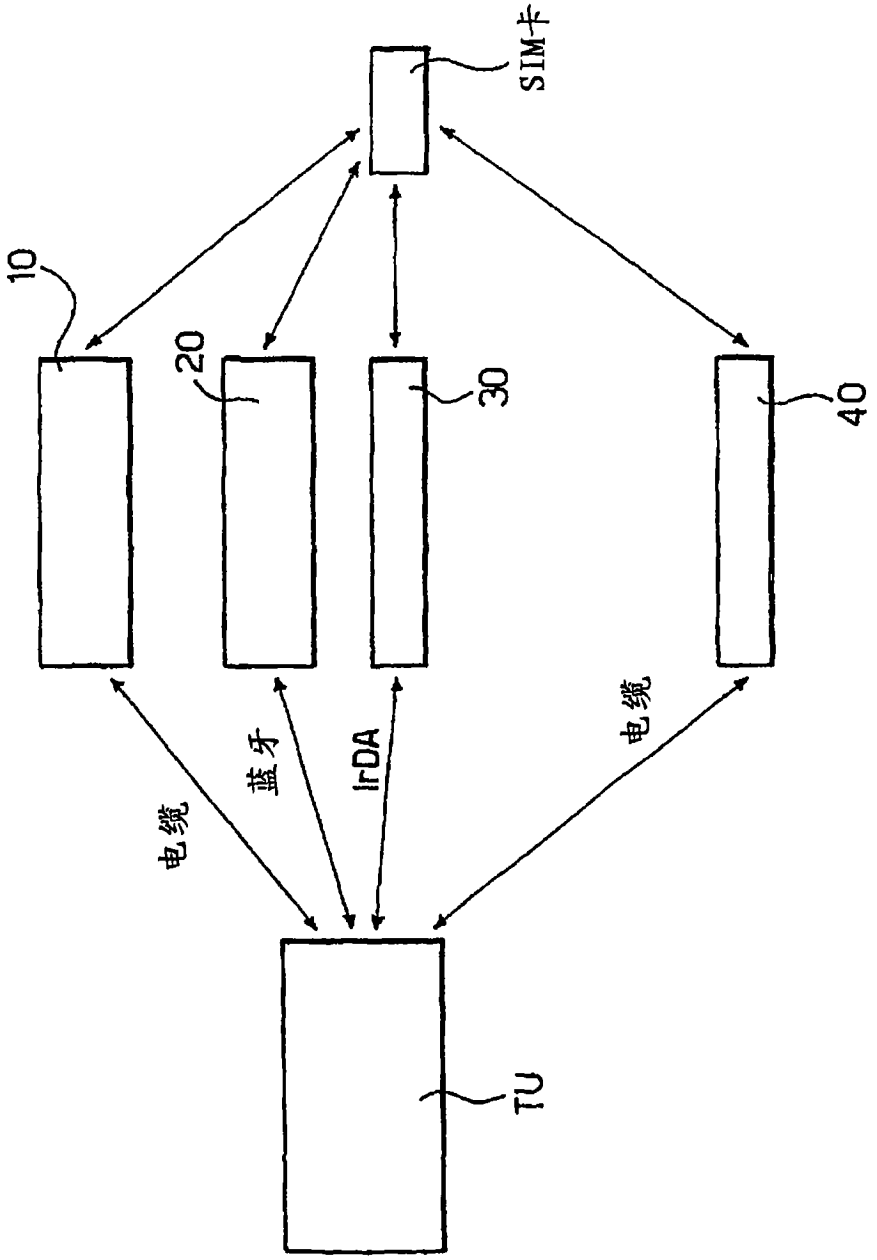


图 1

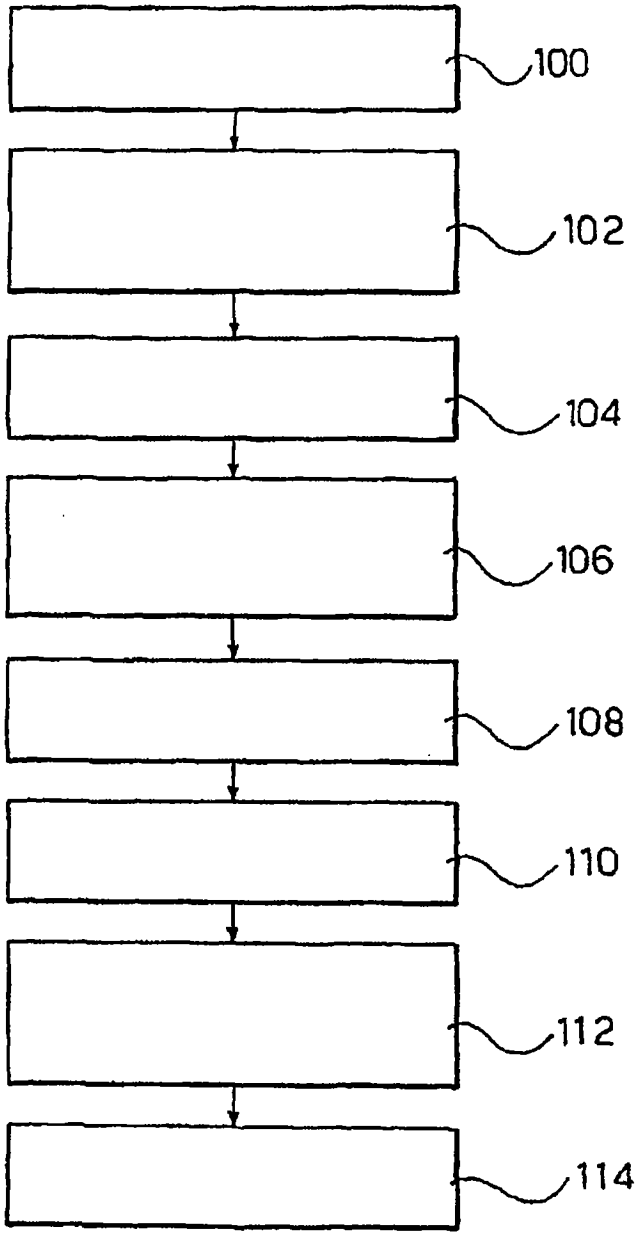


图 2

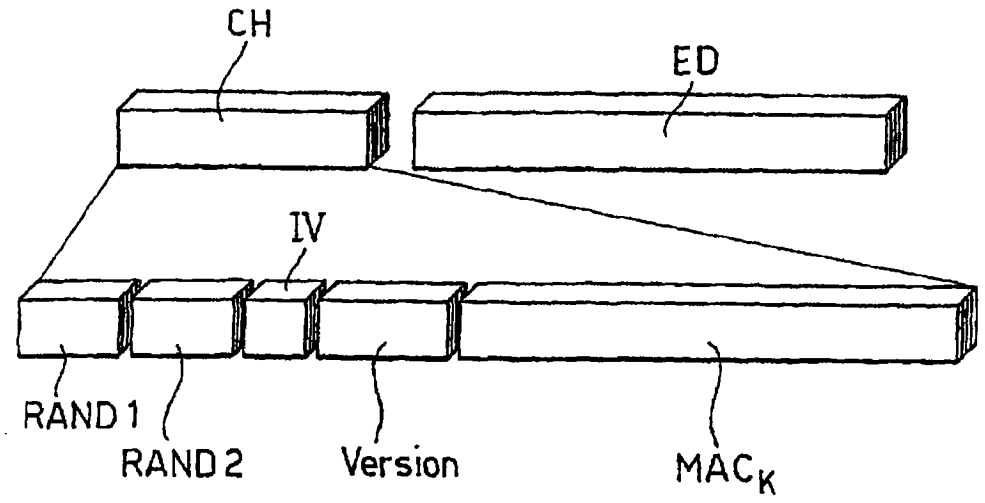

CH
ED
IV
RAND 1
RAND 2
Version
MAC$_K$

图 3

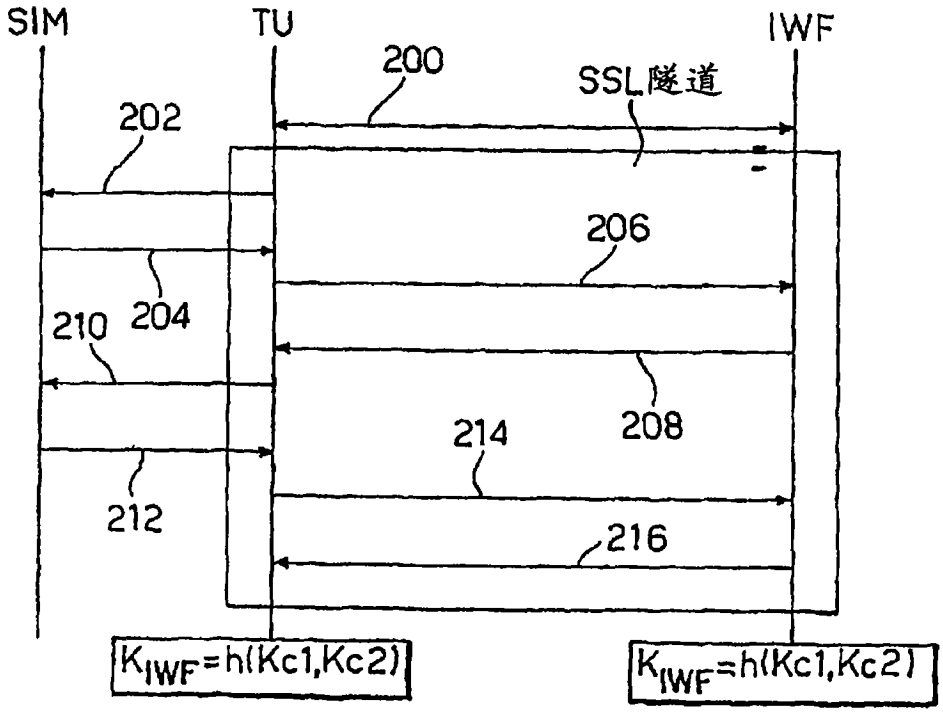

SIM
TU
IWF
200
SSL隧道
202
206
210
204
208
214
212
216
K_{IWF}=h(Kc1,Kc2)
K_{IWF}=h(Kc1,Kc2)

图 4

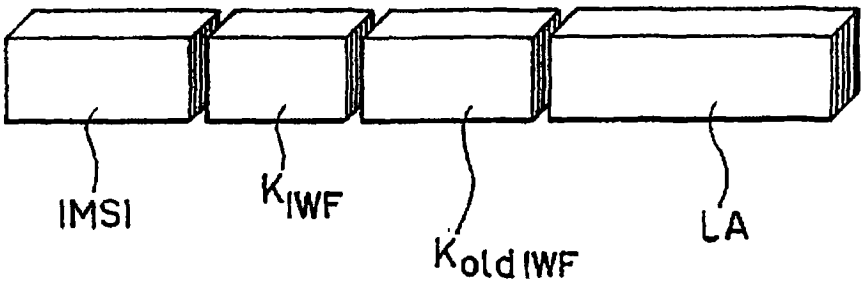

IMSI
K_{IWF}
$K_{old\ IWF}$
LA

图 5

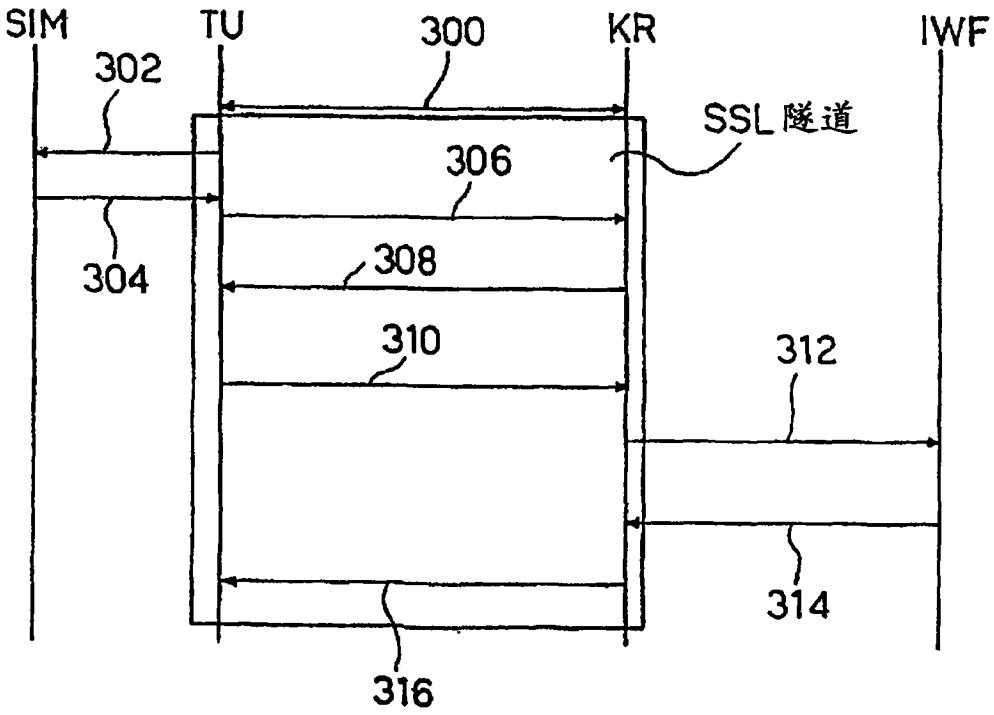

SIM
TU
300
KR
IWF
302
SSL 隧道
306
304
308
310
312
314
316

图 6

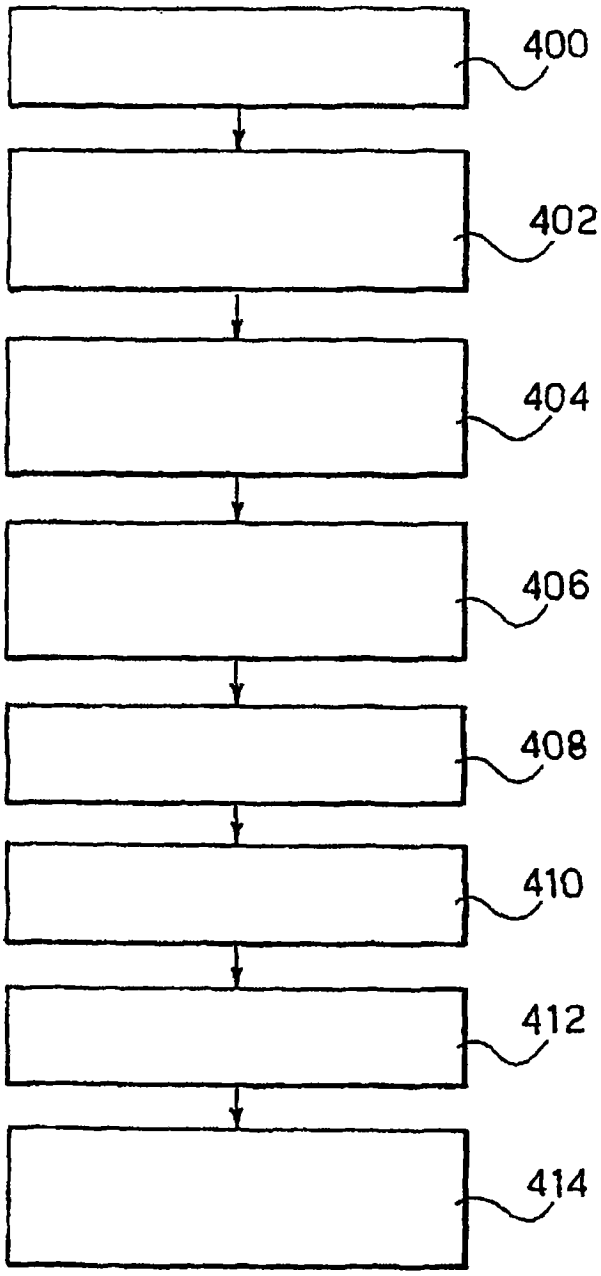


图 7