(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 103201998 B
(45)授权公告日 2016.04.27

(21)申请号 201180052672.1
(22)申请日 2011.10.21
(30)优先权数据
10306195.8 2010.10.29 EP
(85)PCT国际申请进入国家阶段日
2013.04.28
(86)PCT国际申请的申请数据
PCT/EP2011/068456 2011.10.21
(87)PCT国际申请的公布数据
WO2012/055786 EN 2012.05.03
(73)专利权人 法国电信公司
地址 法国巴黎
(72)发明人 洛伦佐·赛诺
路易斯-玛丽·勒萨欧克斯
(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 余朦 王艳春
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04W 12/06(2009.01)
G06F 21/42(2013.01)
(56)对比文件
CN 1860818 A,2006.11.08,
CN 1968093 A,2007.05.23,
US 2009125996 A1,2009.05.14,
US 2009/0209232 A1,2009.08.20,
审查员 万沙沙

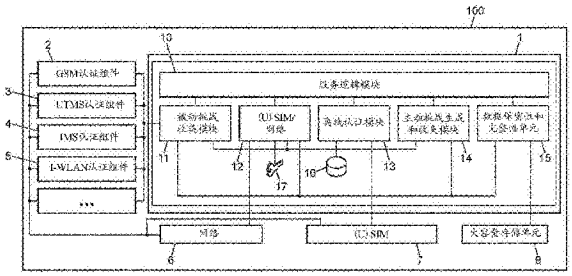
权利要求书3页 说明书16页 附图14页

(54)发明名称

用于保护移动装置中的本地资源的数据处理

(57)摘要

用于保护移动装置(100)中的本地资源的数据处理方法,包括:a)当网络连通时:-联接移动装置(100)与第一识别模块(7),第一识别模块与第一国际移动用户识别码(IMSI)相关联;-在第一识别模块(7)中接收来自通信网络的网络挑战,使用密钥加密所述网络挑战,并向通信网络发出相应的响应以用于随后的成功认证,b)在对通信网络成功认证之后:-将本地资源的至少一部分与第一IMSI关联;以及-在移动装置(100)的数据库(16)中存储与挑战/响应对相关的认证数据;-准予访问与第一IMSI相关联的本地资源,c)当网络不连通时:-联接移动装置(100)与第二识别模块,第二识别模块与第二IMSI相关联;-向第二识别模块发出挑战,其中根据存储在数据库(16)中的认证数据来确定挑战;-接收来自第二识别模块的响应;-将接收的响应与存储的认证数据进行比较,如果来自第二识别模块的响应与数据库(16)中发出的挑战相关联的响应匹配,则准予访问与第二IMSI相关联的本地资源。



CN 103201998 B

1.用于保护移动装置(100)中的本地资源的数据处理方法,包括:

步骤a)当网络连通时:

-联接所述移动装置(100)与第一识别模块(7),所述第一识别模块(7)与第一国际移动用户识别码相关联;

-在所述第一识别模块(7)中接收来自通信网络的网络挑战,使用密钥加密所述网络挑战,并向所述通信网络发出相应的响应以用于随后的成功认证,

步骤b)在对所述通信网络成功认证之后:

-将所述本地资源的至少一部分与所述第一国际移动用户识别码关联;以及

-在所述移动装置(100)的数据库(16)中存储与挑战/响应对相关的认证数据;

-准予访问与所述第一国际移动用户识别码相关联的本地资源,

步骤c)当网络不连通时:

-联接所述移动装置(100)与第二识别模块,所述第二识别模块与第二国际移动用户识别码相关联;

-向所述第二识别模块发出挑战,其中根据存储在所述数据库(16)中的所述认证数据来确定所述挑战;

-接收来自所述第二识别模块的响应;

-将接收的所述响应与存储的所述认证数据进行比较,如果来自所述第二识别模块的所述响应与所述数据库(16)中与发出的所述挑战相关联的响应匹配,则准予访问与所述第二国际移动用户识别码相关联的本地资源。

2.根据权利要求1所述的数据处理方法,其中所述步骤a)包括被动收集认证数据,所述被动收集认证数据包括:

-收集来自所述第一识别模块(7)的响应;以及

-根据所述响应确定离线认证期望响应,以及

所述步骤b)包括将所述网络挑战和相应的离线认证期望响应存储在所述数据库(16)中。

3.根据权利要求1所述的数据处理方法,其中所述步骤b)包括主动收集认证数据,所述主动收集认证数据包括:

-验证出所述第一识别模块(7)已经被所述通信网络认证;

-向所述第一识别模块(7)发送根据所述数据库(16)确定的挑战并收集相应的响应;

-根据所述响应确定离线认证期望响应;以及

-将所述挑战和相应的离线认证期望响应存储在所述数据库(16)中。

4.根据权利要求1所述的数据处理方法,其中存储在所述数据库(16)中的认证数据包括一组记录,其中每个记录包括:

-识别模块的国际移动用户识别码;

-安装有所述识别模块的卡的集成电路卡识别码;

-挑战,用于生成所述认证数据;

-相应的离线认证期望响应,由来自所述识别模块的响应计算得出;

-指示所述认证数据的针对联合的识别模块和网络欺骗攻击的正确性是否被验证的标记;

-指示所述认证数据是否已经被主动或被动地收集的标记；

-所述挑战已在离线背景下被再使用的次数；和/或

-时间戳，与所述挑战/响应对被收集的时间相关。

5.根据权利要求4所述的数据处理方法，其中所述步骤c)包括：

-检查所述第二识别模块的所述国际移动用户识别码，以及检查所述第二识别模块的所述国际移动用户识别码是否与需要被认证的国际移动用户识别码不相符；

-读取安装有所述第二识别模块的卡的集成电路卡识别码的值；

-确定出所述集成电路卡识别码与应该安装有所需的识别模块的卡的集成电路卡识别码的值相符；以及

-选择存在于所述卡上的另一识别模块。

6.根据权利要求1所述的数据处理方法，其中所述步骤a)包括：

-使用所述移动装置(100)认证所述通信网络；以及

-使用所述通信网络认证所述第一识别模块(7)。

7.根据权利要求1所述的数据处理方法，其中所述步骤a)包括：

-使用所述通信网络认证所述第一识别模块(7)；以及

-使用所述移动装置(100)离线认证所述第一识别模块(7)。

8.根据权利要求1所述的数据处理方法，其中如果多于一个的挑战/响应对存储在所述数据库(16)中，则所述步骤c)包括：

-在所述数据库(16)中选择所述国际移动用户识别码的值与所述第二识别模块的国际移动用户识别码相符的所有记录；

-为被选择的每个记录分配安全性索引S_i，所述安全性索引S_i依赖于所述记录已经被再使用的次数和所述记录已经被主动地或被动地收集的事实；

-按所述安全性索引S_i的递减顺序将所有被选择的记录排序；以及

-根据概率分布选择待使用的记录。

9.根据权利要求8所述的数据处理方法，其中所述概率分布的概率密度函数等于：

$$p(i)=\frac{s_i}{\sum_{k=1}^{N} s_k}$$

$i \in N$

$1 \le i \le N \le 10$

其中S_i为在索引i处的所述安全性索引。

10.根据权利要求1所述的数据处理方法，包括使用识别模块安全性算法以生成：

-密钥，用于加密/解密所述本地资源的至少一部分；

-完整性密钥，以生成/验证消息认证码。

11.根据权利要求1所述的数据处理方法，其中所述本地资源的至少一部分还由使用者提供的密码保护。

12.根据权利要求1所述的数据处理方法，其中所述第一识别模块(7)和所述第二识别模块为用户识别模块、全球用户识别模块、可移动用户识别模块、或CDMA用户识别模块。

13.根据权利要求1所述的数据处理方法，其中待认证的识别模块的国际移动用户识别

码是预定的。

14.根据权利要求1所述的数据处理方法，其中待认证的识别模块的国际移动用户识别码为隐含的并且对应于在对所述通信网络成功认证的步骤开始时选择的识别模块的国际移动用户识别码。

15.一种移动装置(100)，包括本地资源和安全性管理器模块(1)，其中所述安全性管理器模块(1)被配置为保护对所述本地资源的至少一部分的访问，所述移动装置(100)被配置为：

a)当网络连通时：

-与第一识别模块(7)联接，所述第一识别模块(7)与第一国际移动用户识别码相关联；

-在所述第一识别模块(7)中接收来自通信网络的网络挑战，使用密钥加密所述网络挑战，并向所述通信网络发出相应的响应以用于随后的成功认证，

b)在对所述通信网络成功认证之后：

-将所述本地资源的至少一部分与所述第一国际移动用户识别码关联；以及

-在所述安全性管理器模块(1)的数据库(16)中存储与挑战/响应对相关的认证数据；

-准予访问与所述第一国际移动用户识别码相关联的本地资源，

c)当网络不连通时：

-与第二识别模块联接，其中所述第二识别模块与第二国际移动用户识别码相关联；

-向所述第二识别模块发出挑战，其中根据存储在所述数据库(16)中的所述认证数据来确定所述挑战；

-接收来自所述第二识别模块的响应；

-将接收的所述响应与存储的所述认证数据进行比较，如果来自所述第二识别模块的所述响应与所述数据库(16)中与发出的所述挑战相关联的响应匹配，则准予访问与所述第二国际移动用户识别码相关联的本地资源。

用于保护移动装置中的本地资源的数据处理

技术领域

[0001] 本发明大体上涉及移动装置的安全性。更具体地，本发明涉及这样的装置和方法，其用于在离线背景下基于识别模块安全信息向移动装置的本地资源提供强制性的访问控制、完整性和保密性。识别模块可以是用户识别模块(SIM)、全球用户识别模块(USIM)、可移动用户识别模块(RUIM)、或CDMA用户识别模块(CSIM)。

背景技术

[0002] 在技术进步和市场需求的推动下，市场上存在的移动电话的平均特征集在近几年里稳步地增加。由于这种趋势，现今，能力最强的移动装置，有时被称为智能手机，除传统的电话服务之外还能够执行大量的任务。这些特征例如包括访问因特网、运行计算相对密集型的应用、播放或录制多个媒体内容以及存储大量数据。随后，由移动装置提供的更大的功能集导致了终端使用者在移动电话的使用方面的变化。

[0003] 这些变化之一体现在使用者存储在其设备上的内容。事实上，终端使用者现在能够在移动电话本地存储越来越多的数据，其中一些还可能非常敏感。示例性的数据包括电子邮件、文件、照片、视频、密码、及其他认证凭证。即使在云计算的背景下，计算和存储的大部分由服务器端应用执行，移动装置仍然存储相当多的敏感信息，如认证凭证和由于性能和可用性原因在本地缓冲的数据。

[0004] 因为装置容易遭到盗窃或遗失，数据的安全性，更一般而言的移动装置的任何其他本地资源(如应用或硬件组件)的安全性是相当重要的事情。为此，移动装置上越来越多的本地可用资源导致对适当地保护的更严格的安全性要求。

[0005] 目前，在符合3GPP标准的移动电话中，可以通过使用安装在抗干扰集成电路卡(有时称为智能卡)上的用户识别模块(SIM)或全球用户识别模块(USIM)来提供安全性。(U)SIM可用于移动用户与移动网络的相互认证以及为移动电话与符合3GPP标准的移动网络之间的数据交换提供保密性、完整性、真实性和不可否认性。

[0006] (U)SIM提供用于访问移动网络服务的适当水平的安全性。事实上，与提供“你所知道的”单因素认证的用户名/密码认证凭证不同，智能卡上的(U)SIM应用提供更强的“你所具有的”认证。此外，可以通过设置个人识别号码(PIN)增加(U)SIM安全性以保护未授权的使用者对卡的访问，因此使得(U)SIM能够提供双因素认证。总之，(U)SIM的另一个显著的安全特性在于移动网络操作者可以远程使其无效的能力。

[0007] 然而，使用基于(U)SIM的认证机制作为保护移动装置上的本地资源的方式还是有相当大的限制的。

[0008] 第一，如果没有可用的网络连接，基于(U)SIM的认证不能被执行。事实上，GSM认证与密钥协商(AKA)协议和UMTS认证与密钥协商(AKA)协议都需要移动网络的可用性以产生认证挑战并验证由(U)SIM提供的响应。

[0009] 第二，攻击者可以在欺骗性的(U)SIM与欺骗性的移动网络之间运行AKA认证以使装置相信该(U)SIM为真，因此授权对本地资源的访问。

[0010] 第三，基于(U)SIM的认证协议不提供适当的机制来加密/解密本地存储的文件和验证其完整性。

[0011] 然而，本领域的技术人员应该认识到这些能力可以由安装在SIM卡或通用的集成电路卡(UICC)上的特别的另外的小应用提供。但是，这将需要发行特殊的卡，这样会对大规模应用提出严重的限制。事实上，这样将需要替换目前使用的卡或通过无线电安装这种小应用，这两种过程都将会相当昂贵。另外，假如还需要在线安全特性，如当网络连通性可用时的远程无效和在线认证，就将需要专用网络设施，进一步增加了资金成本和运营成本。

[0012] 第WO2007/036024号国际专利申请公开了一种用于当接收单元离线时提供认证该接收单元的使用者的方法。该方法包括基于与发送单元的在线通信存储与一个项目相关联的一个或多个挑战-答复组。挑战-答复组的每个包括至少一个挑战答复对，该至少一个挑战答复对用于为了通过接收单元获得特殊资源的使用者的离线认证。

[0013] 然而，在该文件中公开的方法没有描述对识别模块环境的适应。换句话说，该方法不准许在单独的模块框架中认证。

[0014] 本发明的实施方式将改进这种情况。

发明内容

[0015] 为了处理这些需求，本发明的第一方面涉及用于保护移动装置中的本地资源的数据处理方法。该方法包括：

[0016] a)当网络连通时：

[0017] -联接所述移动装置与第一识别模块，第一识别模块与第一国际移动用户识别码(IMSI)相关联；

[0018] -在第一识别模块中接收来自通信网络的网络挑战，使用密钥加密网络挑战，并向通信网络发出相应的响应以用于随后的成功认证，

[0019] b)在对通信网络成功认证之后：

[0020] -将本地资源的至少一部分与第一IMSI关联；以及

[0021] -在移动装置的数据库中存储与所述挑战/响应对相关的认证数据；

[0022] -准予访问与第一IMSI相关联的本地资源，

[0023] c)当网络不连通时：

[0024] -联接移动装置与第二识别模块，第二识别模块与第二IMSI相关联；

[0025] -向第二识别模块发出挑战，其中根据存储在所述数据库中的认证数据来确定挑战；

[0026] -接收来自第二识别模块的响应；

[0027] -将接收的响应与存储的认证数据进行比较，如果来自第二识别模块的响应与数据库(16)中与发出的挑战相关联的响应匹配，则准予访问与第二IMSI相关联的本地资源。

[0028] 本方法的目的是加强移动装置的本地资源的安全性。

[0029] 步骤a)可包括被动收集认证数据，被动收集认证数据包括：

[0030] -收集来自第一识别模块的响应；以及

[0031] -根据被加密的挑战确定离线认证期望响应，

[0032] 步骤b)包括将网络挑战和相应的离线认证期望响应存储在数据库中。

[0033] 在本发明的其他实施方式中，步骤b)可以包括主动收集认证数据，其中主动收集认证数据包括：

[0034] -验证出第一识别模块已经被网络认证；

[0035] -向第一识别模块发送根据数据库确定的挑战并收集相应的响应；

[0036] -根据响应确定离线认证期望响应；以及

[0037] -将挑战和相应的离线认证期望响应存储在数据库中。

[0038] 存储在数据库中的认证数据可以包括一组记录，每个记录包括：

[0039] -识别模块的IMSI；

[0040] -安装有该识别模块的卡的集成电路卡识别码(ICCID)；

[0041] -用于生成认证数据的挑战；

[0042] -由来自识别模块的响应计算得出的相应的离线认证期望响应；

[0043] -指示认证数据的针对联合的识别模块和网络欺骗攻击的正确性是否被验证的标记；

[0044] -指示认证数据是否已经被主动或被动地收集的标记；

[0045] -挑战已经被再使用的次数；和/或

[0046] -与挑战/响应对被收集的时间相关的时间戳。

[0047] 步骤c)可包括：

[0048] -检查第二识别模块的IMSI，以及检查其是否与需要被认证的IMSI不相符；

[0049] -读取安装有第二识别模块的卡的ICCID值，以及该ICCID是否与应该安装有所需的识别模块的卡的ICCID的值相符；

[0050] -选择存在于该卡上的另一识别模块。

[0051] 步骤a)可包括：

[0052] -使用移动装置认证通信网络；以及

[0053] -使用通信网络认证第一识别模块。

[0054] 在本发明的其他实施方式中，步骤a)可包括：

[0055] -使用通信网络认证第一识别模块；以及

[0056] -使用移动装置离线认证第一识别模块。

[0057] 如果多于一个挑战/响应对存储在数据库中，则步骤c)可包括：

[0058] -在数据库中选择IMSI值与第二识别模块的IMSI相符的所有记录；

[0059] -为被选择的每个记录分配安全性索引S_i，安全性索引S_i依赖于记录已经被再使用的次数和记录已经被主动地或被动地收集的事实；

[0060] -按安全性索引的递减顺序将所有被选择的记录排序；以及

[0061] -根据概率分布选择待使用的记录。

[0062] 例如，该概率分布的概率密度函数为：

[0063] $$p(i)=\frac{s_i}{\sum_{k=1}^{N} s_k}$$

[0064] $i \in N$

[0065] $1 \le i \le N \le 10$

[0066] 其中i=1对应于列表的第一元素，以及i=N对应于列表的最后的元素，并且S_i为在索引i处的元素的安全性索引。

[0067] 该方法可包括使用识别模块安全性算法以生成：

[0068] -密钥，用于加密/解密本地资源的至少一部分；

[0069] -完整性密钥，以生成/验证消息认证码(MAC)。

[0070] 此外，本地资源的至少一部分还可使用由使用者提供的密码保护。

[0071] 第一识别模块和第二识别模块可以是用户识别模块(SIM)、全球用户识别模块(USIM)、可移动用户识别模块(RUIM)、或CDMA用户识别模块(CSIM)。

[0072] 待认证的识别模块的IMSI可以预先确定。

[0073] 在本发明的其他实施方式中，待认证的识别模块的IMSI可以是隐含的并且对应于在认证步骤开始时选择的识别模块的IMSI。

[0074] 本发明的第二方面涉及计算机程序产品，其包括处理器能够访问的一个或多个存储的指令序列，当由处理器执行时，该一个或多个存储的指令序列致使处理器执行上述方法的步骤。

[0075] 本发明的第三方面涉及一种移动装置，其包括本地资源和安全性管理器模块，其中该安全性管理器模块配置为保护对本地资源的至少一部分的访问，该移动装置配置为：

[0076] A)当网络连通时：

[0077] -与第一识别模块联接，其中该第一识别模块与第一国际移动用户识别码(IMSI)相关联；

[0078] -在第一识别模块中接收来自通信网络的网络挑战，使用密钥加密该网络挑战，并向该网络发出相应的响应以用于随后的成功认证，

[0079] b)在对通信网络成功认证之后：

[0080] -将本地资源的至少一部分与第一IMSI关联；以及

[0081] -在安全性管理器模块的数据库中存储与挑战/响应对相关的认证数据；

[0082] -准予访问与第一IMSI相关联的本地资源，

[0083] c)当网络不连通时：

[0084] -与第二识别模块联接，其中第二识别模块与第二IMSI相关联；

[0085] -向第二识别模块发出挑战，其中根据存储在数据库中的认证数据来确定挑战；

[0086] -接收来自第二识别模块的响应；

[0087] -将接收的响应与存储的认证数据进行比较，如果来自第二识别模块的响应与数据库(16)中与发出的挑战相关联的响应匹配，则准予访问与第二IMSI相关联的本地资源。

附图说明

[0088] 本发明通过示例而非限制的方式进行了说明，在附图中相同的附图标记表示相似的要素，附图中：

[0089] -图1是根据本发明的实施方式的包括安全管理器的移动设备的示意性框图；

[0090] -图2是示出在全球移动通信系统(GSM)中认证和密钥交换(AKA)方法的步骤的流程图；

[0091] -图3是示出在通用移动通信系统(UMTS)中AKA方法的步骤的流程图；

[0092] -图4是示出用于被动收集认证数据的方法的步骤的流程图；

[0093] -图5是用于产生从32比特响应(SRES)和64比特密钥(K_C)获得的连结序列的散列码的系统的示意性框图；

[0094] -图6是示出用于主动收集认证数据的方法的步骤的流程图；

[0095] -图7a和图7b是示出根据本发明的第一实施方式的能够防止攻击的认证示例的示意图，其中该攻击基于联合的(U)SIM和网络欺骗；

[0096] -图8a和图8b是示出根据本发明的第二实施方式的能够防止攻击的认证示例的示意图，其中该攻击基于联合(U)SIM和网络欺骗；

[0097] -图9是示出认证方法的步骤的流程图；

[0098] -图10是示出利用固有的国际移动用户识别码(IMSI)认证方法的步骤的流程图；

[0099] -图11是示出用于离线认证方法的步骤的流程图；

[0100] -图12和图13是示出用于产生文件的消息认证码(MAC)和/或用于加密的方法的步骤的示意图；

[0101] -图14是密钥导出函数的示意性框图；以及

[0102] -图15和图16图是示出用于验证加密文件的MAC和/或用于将其解密的方法的步骤的示意图。

具体实施方式

[0103] 本发明的实施方式涉及加强移动设备(ME)的本地资源的安全性的问题。

[0104] 图1示出安全性管理器1，其嵌在符合3GPP标准的移动设备(ME)100中，该设备100包括被配置为提供认证的一组认证组件，例如GSM(全球移动通信系统)认证组件2，UMTS(通用移动通信系统)认证组件3，IMS(IP多媒体子系统)认证组件4，以及I-WLAN(无线局域网络)认证组件5。

[0105] ME100还包括大容量存储单元8和被配置为允许ME100与电信网络之间进行连接的网络连接块6。

[0106] 在ME100中设有用户识别模块(SIM)或被称为(U)SIM7的通用用户识别模块(USIM)。

[0107] 安全性管理器1可以实施为硬件或软件或其组合。安全性管理器1包括服务逻辑模块10和被动挑战收集模块11，其中服务逻辑模块10用于控制安全性管理器1，被动挑战收集模块11被配置为监视多个认证过程并且收集由网络实体产生的挑战和因此由(U)SIM7提供的响应产生的挑战。

[0108] 安全性管理器1还包括(U)SIM/网络组合反欺骗逻辑12，其被配置为阻止攻击者试图得到对本地资源的未授权访问的攻击。

[0109] 安全性管理器1还包括离线认证模块13与主动挑战生成和收集单元14，其中离线认证模块13配置为执行离线认证，主动挑战生成和收集单元14配置为生成认证挑战以将该认证挑战发送到(U)SIM7并收集相关的响应。

[0110] 安全性管理器1还包括数据保密性和完整性单元15，其被配置为将文件加密/解密并且保证该文件的完整性。

[0111] 安全性管理器1被配置为能够通过网络连接单元6访问网络连接，并且能够通过应

用协议数据单元(APDU)的交换与(U)SIM7通信。

[0112] 另外,安全性管理器1可被配置为能够在大容量存储外部设备8上进行读写并且能够监控涉及(U)SIM7的多个认证过程的执行和从这些多个认证过程获取信息。

[0113] 安全性管理器1包括持续存储能力,例如对关系数据库16的访问以及对密钥材料17的访问以验证远程网络实体如X.509证书的公钥的真实性。

[0114] 安全性管理器1使得ME100能够使用生成的(U)SIM安全信息判定是否允许用户访问ME100上的本地资源如数据和应用。安全性管理器1能够在具有远程网络实体的支持或没有远程网络实体支持的情况下安全地验证(U)SIM7的真实性。因此,(U)SIM认证甚至可以在网络连接性不可用的离线环境下执行。安全性管理器1还能够识别并且阻止攻击者试图通过使用欺骗性的(U)SIM和欺骗性的移动网络的组合获得对ME100的本地资源的未授权访问的攻击。

[0115] 安全性管理器1可以通过执行以下过程来提供这些特征。

[0116] 首先,当网络连通性可用时,安全性管理器1可以主动地执行包括网络实体的认证过程或者可以监控由ME100上的其他组件执行的适当的认证过程。在该阶段,安全性管理器1可以执行多个机制以阻止包括组合的(U)SIM7和网络6的欺骗攻击。如果该认证过程是成功的,则安全性管理器1准予访问ME100的本地资源并且收集在认证过程期间交换的一组信息如网络挑战和(U)SIM响应。这种信息被安全地存储在关系数据库16或任何适当的永久存储装置中,以便以后当相关的认证网络实体不可用时再用于认证(U)SIM7。

[0117] 第二,如果没有适当的网络认验证体可用时,安全性管理器1使用在之前阶段收集的信息验证插入装置100的(U)SIM的正确性。如果该过程成功,则安全性管理器1允许访问装置的本地资源。

[0118] 下文中将对这两个阶段进行详细描述。

[0119] 对用于在离线背景下进行认证的认证数据可以通过两种方式收集:被动或主动。被动收集包括安全性管理器1监控多个认证过程并且收集由网络实体产生的挑战和因此由(U)SIM7提供的响应来进行,如果被监控的过程成功,则处理和保存该挑战和响应。不同地,主动收集通过安全性管理器1本身产生认证挑战,将该认证挑战发送给(U)SIM7并收集相关的响应来进行。

[0120] 被动收集可以通过监控认证过程中的任何一个来实现,其中,认证过程包括执行GSM AKA(认证和密钥交换)机制(有时称为2G AKA)或者UMTS AKA机制(有时称为3GPP AKA)。

[0121] GSM AKA机制允许网络认证实体认证SIM的身份,其被作为若干认证过程如GSM认证、GPRS认证、2G GBA引导(bootstrap)以及EAP-SIM的一部分执行。

[0122] 参照图2描述GSM AKA机制。

[0123] 在步骤S1中,包括ME100和SIM7的移动站(MS)将其IMSI(国际移动用户识别码)提交至网络认证中心(AuC)并且请求认证。

[0124] 在步骤S2中,AuC生成128比特的随机数,该随机数被称为RAND,并将该128比特的随机数发送至MS。

[0125] 在步骤S3中,SIM7使用来自AuC的RAND及其密钥KI生成被称为SRES的32比特的响应和被称为K_C的64比特的密钥。

[0126] 在步骤S4中，MS将由SIM7计算的SRES的值发送至AuC。

[0127] 在步骤S5中，具有SIM7的密钥KI的复制的AuC计算SRES和KC。如果由AuC计算的SRES的值与由SIM7提供的SRES的值相符，则SIM7真实性就被验证。

[0128] 与GSM AKA不同，UMTS AKA提供USIM和网络之间的相互验证。这种机制用于大量的认证过程，例如包括UMTS认证、EAP(可扩展认证协议)-AKA、GBA(通用引导构架)引导、IMS注册和LTE(长期演化)认证。

[0129] 参照图3描述UMTS AKA机制。

[0130] 在步骤S101中，包括ME100和USIM7的用户设备(MS)将其IMSI提交至网络认证中心(AuC)并且请求认证。

[0131] 在步骤S102中，AuC生成被称为RAND的随机数(与在GSM AKA的情况中一样)以及认证标记(AUTN)。AUTN通过使用存在于AuC上的密钥材料生成并且由USIM7用于验证网络的真实性。然后AuC将RAND和AUTN发送至认证UE。

[0132] 在步骤S103中，在USIM7接收到RAND和AUTN时，首先检查AUTN的真实性。如果该AUTN是可信的，则USIM7生成长达128比特的响应序列RES、被称为CK的1218比特的密钥以及被称为IK的128比特的完整性密钥。与GSM AKA的情况类似，这些值是基于RAND的值和USIM7密钥K的值产生的。如果该AUTN不可信，则USIM7不计算RES、CK以及IK，并且AKA失败。

[0133] 在步骤S104中，如果AUTN验证成功，UE将通过之前接收的RAND获得的RES的值发送给AuC。

[0134] 在步骤S105中，具有USIM7的密钥K的复制的AuC计算RES、CK和IK。如果由AuC计算的SRES的值与由USIM7提供的SRES的值相符，USIM真实性就被验证。

[0135] 应该注意，3GPP限定一组换算函数，该函数允许从UMTS-AKA的RES导出GMS-AKA的SRES以及从UMTS AKA的CK和IK导出GSM-AKA的KC。分别被称为c2和c3的这些换算函数在3GPPTS33.102第9版第6.8.1.2节中进行了描述。本发明的实施方式使用这些换算函数来对使用UMTS AKA机制得到的结果与使用GSM AKA机制得到的结果进行比较。图4和图5示出了参考换算函数c2和c3的使用。

[0136] 图4示出用于被动收集认证数据的方法。

[0137] 在步骤S201中，安全性管理器1开始监控认证过程。

[0138] 在步骤S202中，安全性管理器1检测认证过程的成功状态。如果认证过程成功，则该方法进行步骤S203，如果不成功，该过程退出。

[0139] 在步骤S203中，安全性管理器1确定一种类型的AKA。

[0140] 如果被监控的过程包括执行UMTS-AKA机制，则方法进行步骤S204。不同地，如果被监控的过程包括执行GSM-AKA机制，则安全性管理器1直接收集SRES和KC并且该方法进行步骤S205。

[0141] 在步骤S204中，安全性管理器1收集RAND、RES、CK以及IK的值。然后，安全性管理器1通过换算函数c2从RES计算SRES并通过换算函数c3从CK和IK计算KC。

[0142] 在步骤S205中，安全性管理器1利用所获得的SRES和KC值通过将SRES和KC连结在一起然后生成从SRES和KC获得的连结序列的散列码以生成离线认证期望响应，在此定义为OFFLINE_RESP，如图5所示：

[0143] $OFFLINE\_RESP=H(SRES||K_C)$

[0144] 在步骤S206中，安全性管理器1将认证数据存储在数据库16中。

[0145] 生成OFFLINE_RESP的理由在本文中解释为，需要用于该操作的SRES和KC以防止攻击者通过在未加密的通信信道上嗅探AKA过程而获得OFFLINE_RESP。事实上，在AKA期间K_C并不在空中接口上交换且仅ME100可获得，并且在某些过程中，K_C通过AuC传送至BSS/RNS（基站子系统/无线电网络子系统）。另外，假如对安全性管理器数据库16的访问被不正当地获得，数据的杂乱性使得不能从OFFLINE_RESP获得SRES和K_C。

[0146] 与被动收集不同，主动收集通过安全性管理器1自身产生随机序列RAND并将其发送至(U)SIM7以获得认证数据来进行。在这种情况下，UMTS AKA不能用于计算给定的RAND的响应。事实上，因为安全性管理器1不知道USIM的密钥K和序列号SQN，便不能生成有效的AUTN。因此，USIM7将拒绝所有的想获得RES、CK和IK的企图。为此，GSM AKA机制被使用并且KC和SRES被作为响应收集。

[0147] 图6示出用于主动收集认证数据的方法。

[0148] 在步骤S301中，安全性管理器1验证出(U)SIM7已通过基于UMTS或GSM AKA的任何认证协议被认证，因此现在就形成了安全背景。这种验证保证(U)SIM7是可信的。

[0149] 在步骤S302中，安全性管理器1将一个或多个随机串RAND发送给(U)SIM7并且收集同样多的SRES/KC对。根据ME100和(U)SIM7的能力，主动收集KC和SRES可以以两种不同的方式执行。

[0150] 如果安全性管理器1设置在启用UMTS的ME100上并且包括(U)SIM7的卡为具有在GSM安全背景中支持操作的USIM应用的UICC，则在步骤S303A中，安全性管理器1向卡发出认证命令APDU（应用协议数据单元），该认证命令APDU附有本地生成的RAND并且将“GSM背景”的值指定为认证背景，如3GPP TS31.102所解释的那样。

[0151] 如果安全性管理器1设置在仅启用GSM的ME100上或包括(U)SIM7的卡为没有UICC的SIM卡，则在步骤S303B中，安全性管理器1向卡发出RUN_GSM_ALGO命令APDU，将生成的RAND附加至消息。

[0152] 在步骤S304中，如上所述，安全性管理器1获得作为发出的认证或RUN_GSM_ALGOAPDU消息的响应的KC和SRES，并生成期望的离线响应OFFLINE_RESP，如与被动认证数据收集的情况一样。

[0153] 在安全性管理器1成功地收集预期的认证数据之后，无论是主动或被动，其都将这些数据存储在关系数据库16中以便需要时再次使用。数据库16的每个记录可以包括以下领域：

[0154] -认证数据涉及的(U)SIM7的IMSI，

[0155] -其上安装有(U)SIM7的卡的ICCID（集成电路卡ID）。如在下文中详细描述的，假如UICC（通用的集成电路卡）卡具有多个USIM应用，则IMSI和ICCID的组合使用使得能够适当地离线执行认证。然而，还可以将ICCID和IMSI的匹配信息存储在单独的表中，

[0156] -用于生成认证数据的RAND，

[0157] -由SRES和KC计算的OFFLINE_RESP，

[0158] -指示阻止组合的(U)SIM和网络的欺骗攻击的认证数据的正确性是否被验证的标记，

[0159] -指示认证数据是否已经被主动或被动地收集的标记，

[0160] -在离线背景下RAND已经被重复使用的次数，该值最初被设置为0，之后每次RANDOFFLINE_RESP对被使用，该值就由安全性管理器1更新一次，

[0161] -与RAND/OFFLINE_RESP对被收集的时间相关的时间戳。

[0162] 上述的挑战/响应收集机制易受到这样的攻击，在该攻击中，共同使用欺骗性的(U)SIM和欺骗性的网络以模拟成功的AKA认证。事实上，在这种情况中，攻击者可以将具有欺骗性的IMSI的(U)SIM插入ME100，并且基于UMTS或者GSM AKA利用欺骗性的网络运行认证，从而导致欺骗性的网络和欺骗性的(U)SIM在不知道可信的(U)SIM的真实密钥的情况下自认为成功认证了彼此。因此，无论是在执行主动收集还是执行被动收集的过程中，安全性管理器1都将收集由攻击者插入的伪造的认证数据并且相信其为可信的。因此，添加在数据库中的数据是有毒的并且系统的安全性被损害。

[0163] 如果基于联合的(U)SIM和网络的欺骗攻击被认为可能发生并且需要被阻止，则可选地采取两种解决方案以有效地处理这种问题。

[0164] 如图7A和图7B所示，第一解决方案包括ME100认证运行AKA的网络实体，即网络服务器发布RAND(在UMTS AKA情况下，还发布AUTN)并且验证(U)SIM的RES。例如，这种认证可以利用分给包括在AKA中的网络实体的X.509证书的验证来执行，在AKA中ME100已知该证书的公钥并且可以验证其正确性。作为示例，该过程可以作为GBA引导的一部分来执行。事实上，在这种情况下，运行引导过程的ME100的组件可以与GBA BSF(引导服务器功能)建立TLS(传输层安全性)连接并且可以在执行引导之前验证其证书。如果由ME100进行的服务器身份的验证成功并且随后的AKA(无论GSM或者UMTS)也成功，则ME100可以认为网络和(U)SIM7是真的。甚至，利用该过程，无论使用GSM或UMTSAKA，ME100认证网络(如用箭头$A_{ME\rightarrow N}$表示的那样)，并且网络认证(U)SIM7。网络和USIM7利用UMTS AKA相互认证，如图7A中箭头A_{N-USIM}表示的那样，并且网络利用GSM AKA认证(U)SIM7，如图7B中箭头$A_{N\rightarrow(U)SIM}$表示的那样。因此，ME100能够可靠地验证(U)SIM7的真实性。

[0165] 可替代地，如上所述，假如ME100由于任何原因不能验证运行AKA的网络实体的真实性，则可以采用第二解决方案来阻止联合的(U)SIM和网络的欺骗。图8A和图8B中示出的这种解决方案包括两个步骤。首先，(U)SIM7和网络基于GSM AKA或者UMTS AKA运行认证过程。网络和USIM7利用UMTS AKA相互认证(如图8A中的箭头A_{N-USIM}所示)，并且网络利用GSM AKA认证(U)SIM7(如图8B中的箭头$A_{N\rightarrow(U)SIM}$所示)。其次，如果认证成功并且安全性管理器1在其数据库16中具有可以认为是可靠的(即没有由联合的USIM/网络的欺骗攻击毒害)的包括RAND/OFFLINE_RESP对的至少一个记录，则安全性管理器1主动向(U)SIM7发出挑战并且对响应与存在于数据库16中的OFFLINE_RESP的值进行比较，如图8A中的箭头$A_{ME\rightarrow USIM}$和图8B中的箭头$A_{ME\rightarrow(U)SIM}$所示的那样。如果这些值相互匹配，则安全性管理器1可以可靠地认为(U)SIM和网络是可信的。下文将描述用于选择RAND/OFFLINE_RESP对、并将其发送至(U)SIM7以及比较所获得的结果与所期望的结果的方法。

[0166] 如果上述两个解决方案中的任一种或两者已经与成功的GSM AKA或者UMTS AKA一起执行，则(U)SIM7可以被认为是可信的。因此，通过被动地监控这种机制获得的认证数据的收集被保护以免受到联合的(U)SIM和网络的欺骗攻击。另外，在通过这两个解决方案中的一个或两者建立安全背景之后，安全性管理器1可以在免受联合的(U)SIM和网络的欺骗攻击的保护下主动地收集来自(U)SIM7的认证数据。当安全性管理器1利用这些方法存储收

集的认证数据时，无论主动或被动，其必须设置标记，该标记指示被收集的RAND/OFFLINE_RESP受到保护以免受联合的(U)SIM和网络的欺骗。

[0167] 下文将描述这样的过程，通过该过程可以基于(U)SIM7的身份的验证实施对ME100的本地资源的访问控制。使用的术语“资源”旨在表示ME100上存在的使用者可以使用或者从其获得益处的任何物理实体或逻辑实体。这种资源的示例包括但并不限于，软件组件如文件、目录、应用、操作系统、虚拟机图像，以及硬件组件如存储设备和输入/输出，外部设备如照相机、麦克风、传感器和网络接口。

[0168] 首先，为了执行加强访问控制的认证方法，旨在由这种保护覆盖的ME100的所有资源必须标记有(U)SIM的IMSI，该(U)SIM的IMSI的所有者被授权访问该资源。可选地，资源还可以利用被授权的IMSI能够在其上执行的操作的列表来标记。可替代地，这些资源还可以利用可替代的标识符标记，该标识符可以唯一地与一个IMSI对应。如果ME100上的所有本地资源被认为具有相同访问条件，则被授权的IMSI的列表可以被集中。用于表示被授权的IMSI的列表以访问资源的可能的方法以及其所有者被允许在其上执行的活动对本领域的技术人员而言是公知的并且超出了本发明的范围。

[0169] 图9示出了完整的认证过程。当使用者请求访问由访问控制保护的特殊的资源时，安全性管理器1启动认证过程。可替代地，其可以在引导时或在发生任何其他事件时启动该过程。

[0170] 在步骤S401中，安全性管理器1验证SIM或UICC卡是否插在ME100中。如果没有卡可用，则对资源的访问被拒绝(步骤S414)并且该过程退出。否则，如果卡被插入，该方法进行步骤S402。

[0171] 在步骤S402中，安全性管理器1检查当前选择的(U)SIM应用的IMSI。如果该IMSI与需要被认证的IMSI不匹配，该方法进行步骤S403。如果其匹配，该方法进行步骤S407。

[0172] 在步骤S403中，安全性管理器1读取卡的ICCID的值。如果该ICCID与安装有需要的(U)SIM应用的卡的ICCID的值不匹配，则意味着插入了不同的卡。在这种情况下，对资源的访问被拒绝(步骤S414)并且该过程退出。

[0173] 不同地，如果ICCID与安装有需要的(U)SIM应用的卡的ICCID的值匹配，则可能意味着该卡具有多个(U)SIM应用并且所要求的应用现在没有被选择。在这种情况下，方法进行步骤S404。

[0174] 在步骤S404中，安全性管理器1检测未被选择的其他(U)SIM应用的状态。假如没有其他(U)SIM，则对资源的访问被拒绝(步骤S414)并且过程退出。假如存在其他(U)SIM，则该方法进行步骤S405。

[0175] 在步骤S405和S406中，安全性管理器1一个接一个地选择卡上存在的所有(U)SIM应用直到发现具有所需要的IMSI的(U)SIM应用。了解卡是否具有多个(U)SIM应用和如何选择的方法对于本领域的技术人员是公知的并且这在本发明的范围之外。如果预期的(U)SIM应用没有被发现，则对资源的访问被拒绝(步骤S414)并且过程退出。

[0176] 应该注意到在这些步骤中，假设安全性管理器1了解期望的ICCID-IMSI对应。如上所述，可以从包括用于离线认证的RAND/OFFLINE_RESP对的列表的数据库表或者从单独的表收集该信息。

[0177] 一旦具有需要的IMSI的(U)SIM被选择，在步骤S407中，安全性管理器1就检测是否

存在有效的安全背景以及是否已经成功地执行反欺骗机制。如果在具有需要的IMSI的(U)SIM与网络之间存在有效的安全背景，并且如果反欺骗机制已经成功地执行，则该方法进行步骤S413。否则该方法进行步骤S408。

[0178] 在步骤S408中，安全性管理器1检测网络连通性是否可用。如果网络连通性可用，该方法进行步骤S411。否则该方法进行步骤S409。

[0179] 在步骤S409中，安全性管理器1检测是否存在可用于运行离线认证的认证数据。如果存在可用于运行离线认证的认证数据，该方法进行步骤S410。否则对本地资源的访问被禁止(步骤S414)。

[0180] 在步骤S410中，如果网络连通性不可用或者如果没有用于执行AKA的网络实体，则安全性管理器1执行离线认证，这将在下文进行详细描述。如果离线认证成功(步骤S412)，则对资源的访问将被允许(步骤S413)，否则将被拒绝(步骤S414)。在该阶段之后，验证过程退出。

[0181] 在步骤S411中，安全性管理器1运行任何合适的(U)SIM认证过程，该(U)SIM认证过程包括UMTS AKA或者GSM AKA。另外，安全性管理器1可以执行这些过程之一以防止上述联合的USIM/网络的欺骗攻击。

[0182] 在步骤S412中，安全性管理器1检测认证是否成功。如果认证成功，对资源的访问将被允许(步骤S413)并且该过程退出。如果认证没有成功，对资源的访问被拒绝(步骤S414)并且该过程退出。

[0183] 对于上述的认证过程，可替代地，在该认证过程中待认证的IMSI在方法中被明确地指定并且其对应于访问所需要的特殊资源的所有者，认证过程还可以在隐含的IMSI上执行。事实上，认证过程可以由安全性管理器在过程开始时所选择的(U)SIM应用的IMSI上执行。

[0184] 图10示出具有隐含的IMSI的认证过程的流程图。

[0185] 在步骤S501中，安全性管理器1验证SIM或UICC卡是否插在ME100中。如果没有卡可用，则对资源的访问被拒绝(步骤S511)，并且过程退出。否则，如果卡被插入，该方法进行步骤S502。

[0186] 在步骤S502中，安全性管理器1检测当前(U)SIM是否被选择。如果当前(U)SIM被选择，则该方法进行步骤S504。否则该方法进行步骤S503。

[0187] 在步骤S503中，安全性管理器1选择(U)SIM应用。

[0188] 在步骤S504中，安全性管理器1检测是否存在有效的安全背景以及反欺骗机制是否已经成功地执行。如果存在有效的安全背景并且反欺骗机制已经成功地执行，则该方法进行步骤S510。否则该方法进行步骤S505。

[0189] 在步骤S505中，安全性管理器1检测网络连通性是否存在。如果网络连通性存在，则该方法进行步骤S508。否则该方法进行步骤S506。

[0190] 在步骤S506中，安全性管理器1检测是否存在可用于运行离线认证的认证数据。如果存在可用于运行离线认证的认证数据，该方法进行步骤S507。否则对本地资源的访问被禁止(步骤S511)。

[0191] 在步骤S507中，如果网络连通性不可用或者如果没有用于执行AKA的网络实体，安全性管理器1执行离线认证，这将在下文进行详细描述。如果离线认证成功(步骤S509)，对

资源的访问将被允许(步骤S510),否则将被拒绝(步骤S511)。

[0192] 在步骤S508中,安全性管理器1运行具有反欺骗机制的基于AKA的认证。

[0193] 在步骤S509,安全性管理器1检测认证是否成功。如果认证成功,对资源的访问将被允许(步骤S510)并且该过程退出。如果认证没有成功,对资源的访问被拒绝(步骤S511)并且该过程退出。

[0194] 图11示出离线认证方法的流程图。离线认证包括再使用具有RAND序列的(U)SIM7以及利用存储在安全性管理器的数据库16中的期望的离线响应OFFLINE_RESP的值来验证(U)SIM的响应。这种机制包括三个方面:

[0195] -如果安全性管理器1可用多于一个的RAND/OFFLINE_RESP对,则选择RAND/OFFLINE_RESP对以重新使用;

[0196] -提交RAND至(U)SIM7并收集相关响应;以及

[0197] -利用OFFLINE_RESP的值验证结果。

[0198] 对于选择RAND/OFFLINE_RESP以用于认证,本发明限定了一种算法,假如多个记录存在于安全性管理器1的数据库16中则该算法使系统安全最大化。更具体地,根据是否需要阻止联合的(U)SIM/网络的欺骗,该算法的执行方式不同。

[0199] 假如需要这种保护,则该算法的执行方式如下。

[0200] 在步骤S601中,安全性管理器1选择所有这种记录,即这些记录中IMSI领域的值与必须被离线认证的(U)SIM7的IMSI相匹配。

[0201] 然后,安全性管理器1选择已经使用阻止联合的(U)SIM/网络欺骗的两种方法之一收集的所有记录。这可以通过仅选择具有相关的标记组的记录来实现。

[0202] 在步骤S602中,安全性管理器1检测是否至少一个记录被选择。如果至少一个记录被选择,则该方法进行步骤S603。如果没有留下的记录,则离线认证失败(步骤S612)。

[0203] 在步骤S603中,如果仅存在一个记录,则该样本由于已被使用而被标记。否则,如果可得到多个记录,则待用于认证的记录将按照如下进行选择。为数据库16中的每个被选择的记录分配安全性索引S_i,其中S_i这样计算:

[0204] $$s_i = 2^{-r_i - a_i}$$

[0205] 其中,r_i表示该记录已经被再使用的次数,如果样本被主动收集则a_i等于1,或者如果样本被被动收集则a_i等于0。

[0206] 在步骤S604中,列表的所有被选择的记录按Si的递减顺序排序。如果多个元素具有相同的S_i值,那么这多个元素将被按从收集的最近时间戳到收集的最早时间戳进行子排序。

[0207] 在步骤S605中,安全性管理器1检测该列表是否具有十个以上的记录。在这种情况下,仅选择排序的列表中的前十个记录(步骤S606),否则列表中的所有记录将被选择。

[0208] 在步骤S607中,已经被使用而被标记的记录将被记录为在列表的索引i处的记录,其中i为1到N之间的自然数,N为列表中记录的数目,i为具有随机变量的实现,该随机变量的概率密度函数等于:

[0209] $$p(i)=\frac{s_i}{\sum_{k=1}^{N} s_k}$$

[0210] $i \in N$

[0211] $1 \le i \le N \le 10$

[0212] 其中i=1对应于列表的第一元素以及i=N对应于列表的最后的元素，并且S_i为在索引i处的元素的安全性索引。

[0213] 不同地，假如没有严格要求阻止联合的(U)SIM/网络欺骗，则可以执行上述的相同的算法，但是具有以下两个差别：

[0214] -未设置联合的(U)SIM/网络欺骗保护标记的记录也被选择，以及

[0215] -安全性索引S_i的值按如下这样计算：

[0216] $$s_i = 2^{v_i - r_i - a_i}$$

[0217] 其中如果设置了反欺骗标记，则v_i等于3，如果未设置，则v_i=0。

[0218] 上文对用于选择RAND/OFFLINE_RESP的概率分布作为示例进行了描述。不同的选择法可以同等地使用。

[0219] 在步骤S608中，一旦已经选择了待用于离线认证的RAND/OFFLINE_RESP对，则安全性管理器1就将随机序列RAND发送至(U)SIM7并收集响应。根据ME100和(U)SIM7的能力，该过程可以以两种不同的方式执行。

[0220] 根据第一方法，如果安全性管理器1设置在启用UMTS的ME100上并且该卡为具有在GSM安全背景中支持操作的USIM应用的UICC，则安全性管理器1向卡发出认证命令APDU，该认证命令APDU附有RAND并且将“GSM背景”的值指定为认证背景，如3GPP TS31.102第9版所解释的那样。

[0221] 根据第二方法，如果安全性管理器1设置在仅启用GSM的ME100或该卡为没有UICC(通用集成电路卡)的SIM卡，则安全性管理器1向卡发出RUN_GSM_ALGO命令APDU，将生成的RAND附加至消息。

[0222] 安全性管理器1获得KC和SRES，作为对在上述步骤期间发出的AUTHENTICATE或RUN_GSM_ALGOAPDU命令的响应。

[0223] 在步骤S609中，安全性管理器1产生期望的离线响应OFFLINE_RESP，该离线响应OFFLINE_RESP为：

[0224] $OFFLINE\_RESP=H(SRES||K_C)$

[0225] 在步骤S610中，安全性管理器1检测OFFLINE_RESP是否与预期的值匹配。

[0226] 如果这里计算的OFFLINE_RESP的值与存在于数据库16的被挑选的记录中的OFFLINE_RESP的值匹配，则认证成功(步骤S611)，否则认证失败(步骤S612)。

[0227] 在离线认证已经执行之后，安全性管理器1将已经被使用的记录的再使用计数器加1。另外，如果存在已经被再使用至少三次的记录，则将该记录从数据库16删除，这也是可取的。

[0228] 在此描述的本发明的实施方式提供基于(U)SIM7的真实性的验证来控制对移动装

置100的本地资源的访问的可能性。然而，这些特征的有效的适用性取决于在(U)SIM真实性没有被验证的情况下，移动装置的硬件或软件能够安全地执行对这些资源的访问的拒绝。假如该机制用于控制对位于可移动记忆存储装置如安全数字(SD)卡上的数据的访问，这可以表示较强的限制。事实上，只要该设备被插入装置100中，移动装置100可以限制对这种具有上述机制的可移动存储设备的访问。因此，一旦其从装置100移除，则其上存储的数据可以由没有实施访问控制特征的另一个装置不受控制地读取或写入。因此，必须利用适当的方法为该数据提供足够的安全水平，该方法可以保证数据的保密性和完整性，以便即使该可移动存储装置被移除，存储在其上的数据也不可被理解并且在没有对合法使用者进行检测的情况下不能被更改。

[0229] 更具体地，两种方法可以用于适当地处理这种问题。

[0230] 第一种方法包括：

[0231] -通过本领域的技术人员已经公知的机制实现保密性和完整性，如使用对称加密算法提供保密性和使用消息认证码(MAC)提供完整性控制，该机制可以在一个文件接着一个文件的基础上应用或者可以应用到整个磁盘扇区。

[0232] -存储用于在非可移动存储器上加密/解密以及生成/验证MAC的需要的所有密钥材料，该存储器由上述基于(U)SIM的访问控制机制保护。通过这种方法，可以仅在被授权访问数据的使用者的(U)SIM7存在时进行加密/解密和生成/验证MAC。另外，如果可移动存储组件插入另一装置中，则数据不可以被理解或者伪造。

[0233] 还在这种情况下，数据必须用被允许访问该数据的使用者的(U)SIM的IMSI标记，可选地，补充有每个使用者被准许执行什么操作的指示。

[0234] 第二种方法包括在密钥生成过程中使用(U)SIM安全性算法，以产生：

[0235] -密钥$K_{密钥}$，以加密/解密数据，

[0236] -完整性密钥$K_{完整性密钥}$，以生成/验证用于完整性目的的消息认证码(MAC)，以及

[0237] -初始化与分组密码一同使用的向量IV以增加加密的健壮性。

[0238] 这些值可被用于在一个文件接一个文件的基础上或在整个磁盘扇区上加密/解密文件以及生成和验证消息认证码(MAC)。

[0239] 图12和图13示出用于生成文件的MAC和/或用于加密文件的MAC的方法。

[0240] 在步骤S701中，要求被加密的每个文件$P_{文件}$必须使用要求用于解密的(U)SIM7的IMSI或者使用与该IMSI单一对应的唯一字符串标记。

[0241] 在步骤S702中，该文件使用128比特的随机串标记，该随机串被用作(U)SIM7的AUTHENTICATE/RUN_GSM_ALGO函数的输入。该随机序列可以是存储驱动器的全局非秘密属性并且可以由该驱动器的所有文件使用。可替代地，其可以从存在于存储驱动器自身或者移动装置存储器或者远程实体上的具有很少的128比特随机串的池中选择。另外，文件可以直接地使用该随机序列标记，或者可替代地，使用可以与该随机串对应的标识符标记。必须确保系统中的随机串的总数是有限的。事实上，如下文将要解释的，将该随机串作为用于产生密钥材料的(U)SIM7的输入发出并且，如果大量的文件使用这种机制保护并且与不同的字符串相关联，则其加密解密需要将许多AUTHENTICATE/RUN_GSM_ALGOAPDU命令发送给(U)SIM7。因为在接收了中等数量的认证过程(通常为216)之后，(U)SIM应用停止工作，所以这种方案可以显著减少(U)SIM的生命周期。

[0242] 在步骤S703中，如果希望使用密码(PASSWORD)来保护该文件，则密码由使用者提供并且其用于产生辅助128比特随机串。在图13中，文件$P_{文件-2}$和$P_{文件-3}$由密码保护。该辅助随机串将用于算法的其他部分。在一个实施方式中，该辅助随机串可以从与密码相联系的原始随机串的MD5散列中产生，这里解释为：

[0243] RAND'=MD5(RAND||PASSWORD)

[0244] 在步骤S704中，该随机串被附给AUTHENTICATE或RUN_GSM_ALGOAPDU命令并且发送给(U)SIM7以获得SRES和K_C，这与上述的离线认证的情况类似。然后将SRES和K_C提供至生成仅作为这两个值的函数的万能密钥的函数。在一个实施方式中，该函数可以是与如上所述的用于生成OFFLINE_RESP串相同的函数，因此：

[0245] MK=H(SRES||K_C)

[0246] 在步骤S705中，如图14所示，该万能密钥被提供至密钥导出函数，密钥导出函数：

[0247] -使用要素生成器140生成“要素(SALT)”，即至少长64比特的随机串，该随机串对于待加密的文件是唯一且特定的，

[0248] -使用要素和万能钥匙以生成K_{CIPHER}($K_{密钥}$)，$K_{INTEGRITY}$($K_{完整性密钥}$)和IV，如：

[0249] K_{CIPHER}=H(SALT||MK||RANDSTR_K_C)

[0250] $K_{INTEGRITY}$=H(SALT||MK||RANDSTR_K_I)

[0251] IV=H(SALT||MK||RANDSTR_IV)

[0252] 其中RANDSTR_KC、RANDSTR_KI和RANDSTR_IV为三个公知的恒定随机串，其用于区分上面的三个输出。

[0253] 在步骤S706中，$K_{INTEGRITY}$可用于生成文件的MAC(例如使用基于散列的消息认证码(HMAC)函数)以保证完整性。另外，如果要求保密性，明文文件和MAC可以将K_{CIPHER}用作密钥来加密(例如使用AES密码)以及将IV用作该密码的初始化向量(例如，如果AES用于密码块链接(CBC)操作模式中)。

[0254] 在步骤S707中，以下属性可以附加至输出文件$C_{文件}$，以允许解密和MAC验证：

[0255] -要素，用来生成密钥，

[0256] -随机串，关联至文件或者关联至可以与其对应的标识符，

[0257] -(U)SIM7的IMSI，用于加密方法或者加密可以与其对应的标识符，以及

[0258] -标记，表示该文件是否需要密码来解密。

[0259] 图15和图16示出用于验证加密文件$C_{文件}$的MAC和/或用于将其解密的方法。

[0260] 在步骤S801中，检索用于加密文件的(U)SIM7的IMSI。如果需要的(U)SIM7不可用，则该过程退出，否则相关的(U)SIM7被选择(如果仍未被选择)。

[0261] 在步骤S802中，检索与文件相关联的128比特的随机串和要素。

[0262] 在步骤S803中，如果该文件$C_{文件}$由密码保护，则该密码由使用者提供并且以在加密方法期间被使用的方式相同的方式来生成辅助128位随机串。在该示例中，文件$P_{文件-2}$和$P_{文件-3}$由密码保护。

[0263] 在步骤S804中，该随机串被附加至AUTHENTICATE或RUN_GSM_ALGOAPDU命令并且发送至(U)SIM7以获得SRES和K_C，这与上述的离线认证的情况类似。然后将SRES和K_C提供至生成仅作为这两个值的函数的万能密钥函数。在一个实施方式中，万能密钥函数可以是与如上所述的用于产生OFFLINE_RESP串相同的函数，因此：

[0264] $MK=H(SRES||K_C)$

[0265] 在步骤S805中，该万能密钥与和该文件相关联的要素一同被提供给密钥导出函数。使用密钥导出函数生成K_{CIPHER}、$K_{INTEGRITY}$和IV，这里描述为：

[0266] $K_{CIPHER}=H(SALT||MK||RANDSTR\_K_C)$

[0267] $K_{INTEGRITY}=H(SALT||MK||RANDSTR\_K_I)$

[0268] $IV=H(SALT||MK||RANDSTR\_IV)$

[0269] 其中RANDSTR_KC、RANDSTR_KI和RANDSTR_IV为三个公知的恒定随机串，其用于区分上面的三个输出。

[0270] 在步骤S806中，K_{CIPHER}和IV用来解密该文件并且$K_{INTEGRITY}$用来验证该文件的MAC。如果该文件已经被伪造或被损坏，则MAC验证失败(步骤S807)。否则，解密成功(步骤S808)。

[0271] 本领域的技术人员应该认识到本发明的实施方式可以明显地扩展到符合3GPP2标准的移动装置，其中可移动用户识别模块(RUIM)或CDMA用户识别模块(CSIM)而不是(U)SIM用于执行移动用户与移动网络之间的认证和密钥交换。

[0272] 虽然上文中已经参考具体实施方式描述了本发明，但是本发明并不限于这些具体实施方式，并且对于本领域的技术人员显而易见的是，可以对本发明做出修改，这些修改仍然在本发明的范围内。

[0273] 通过参考上述说明性的实施方式，许多进一步的修改和变型将呈现给本领域的技术人员，其中上述说明性的实施方式仅通过示例的方式给出但是本发明的范围并不限于此，本发明的范围仅由所附权利要求确定。特别地，不同实施方式的不同特征在适当时可以互换。

[0274] 在权利要求中，术语“包括”并不排除其他部件或步骤，并且不定冠词“一个(a)”或“一个(an)”并不排除多个。在互不相同的从属权利要求中说明不同的特征的这个事实并不指示这些特征的组合不能被有利地使用。权利要求中的任何参考标记不应被理解为限制本发明的范围。

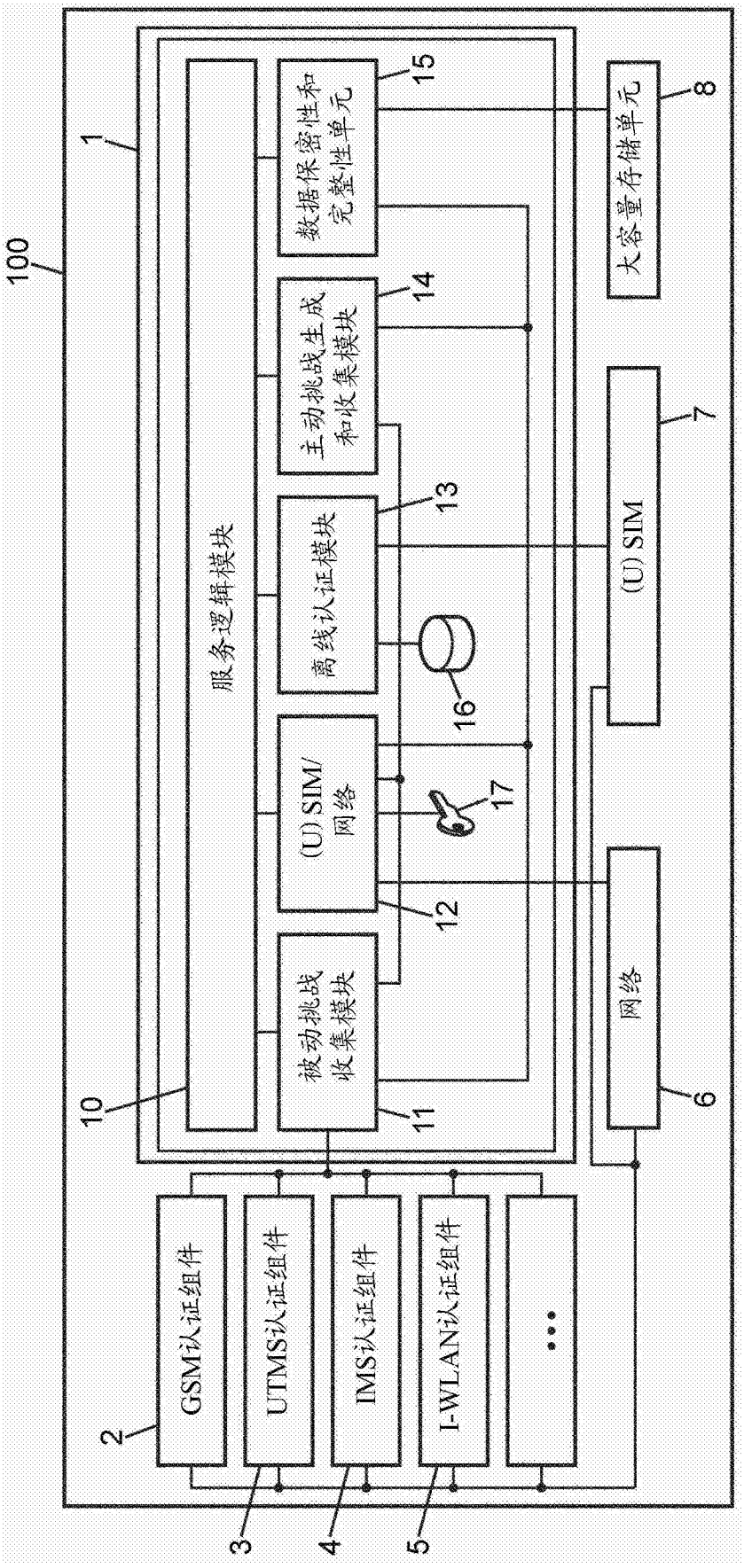

100
1
服务逻辑模块
数据保密性和完整性单元
15
主动挑战生成和收集模块
14
离线认证模块
13
(U) SIM/网络
12
被动挑战收集模块
11
10
大容量存储单元
8
(U) SIM
7
网络
6
16
17
GSM认证组件
UTMS认证组件
IMS认证组件
I-WLAN认证组件
...
2
3
4
5

图1

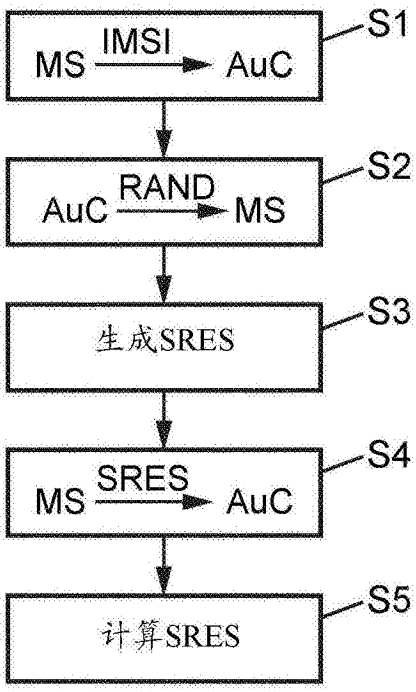

S1
MS IMSI AuC
S2
AuC RAND MS
S3
生成SRES
S4
MS SRES AuC
S5
计算SRES

图2

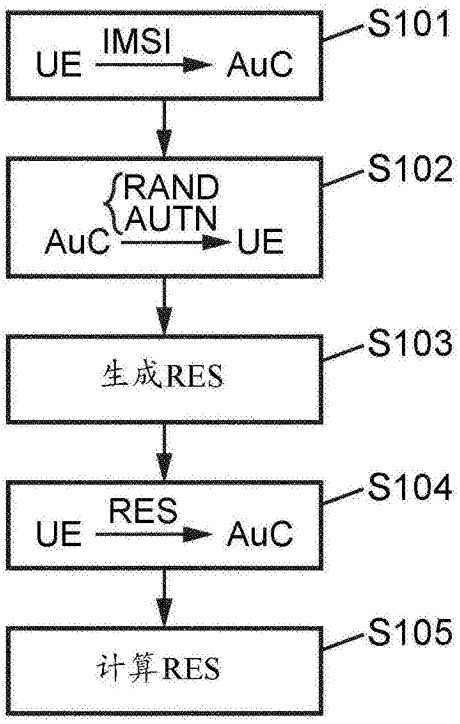

S101
UE IMSI AuC
S102
RAND
AUTN
AuC UE
S103
生成RES
S104
UE RES AuC
S105
计算RES

图3

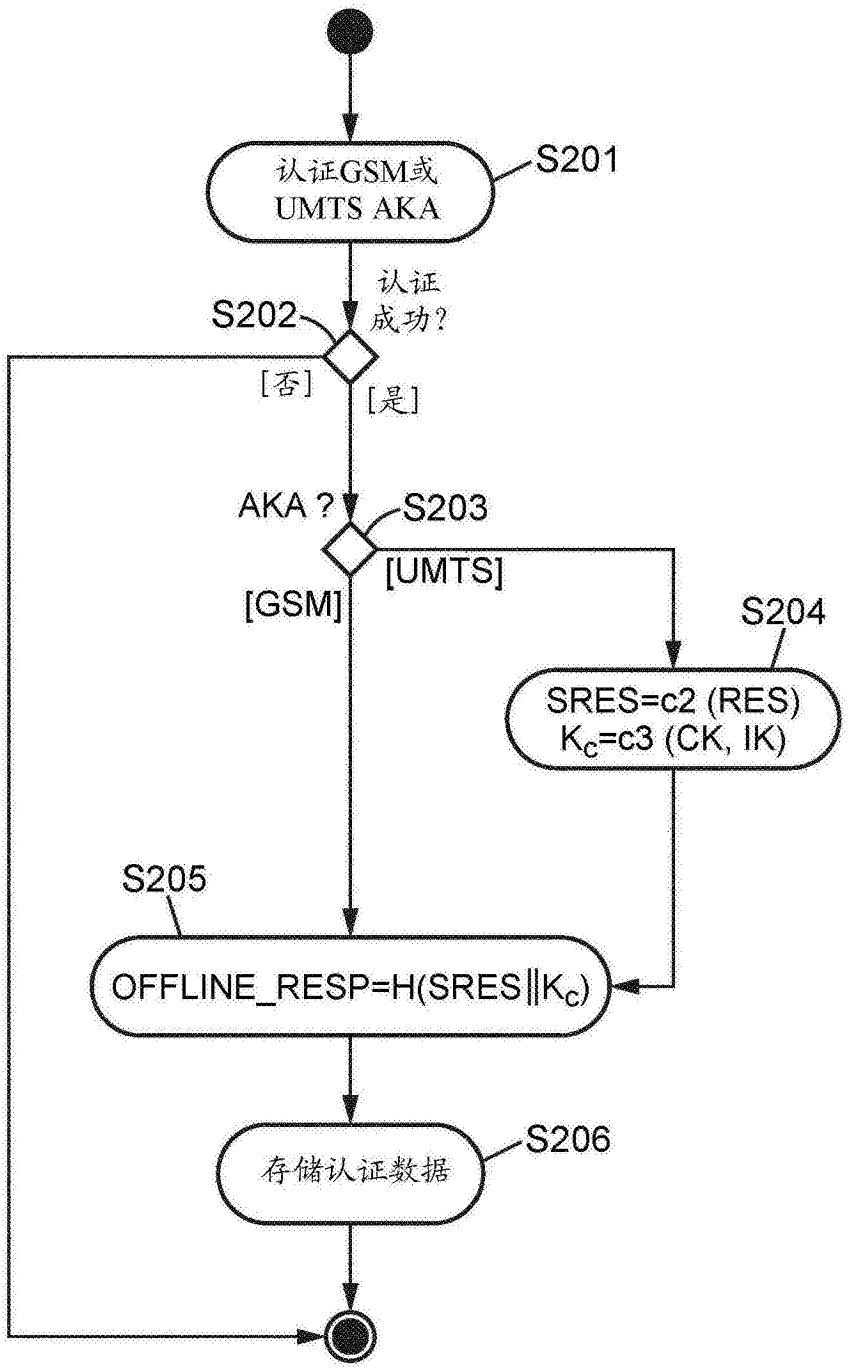

认证GSM或
UMTS AKA
S201
认证
成功?
S202
[否]
[是]
AKA ?
S203
[UMTS]
[GSM]
S204
SRES=c2 (RES)
K_C=c3 (CK, IK)
S205
OFFLINE_RESP=H(SRES||K_C)
存储认证数据
S206

图4

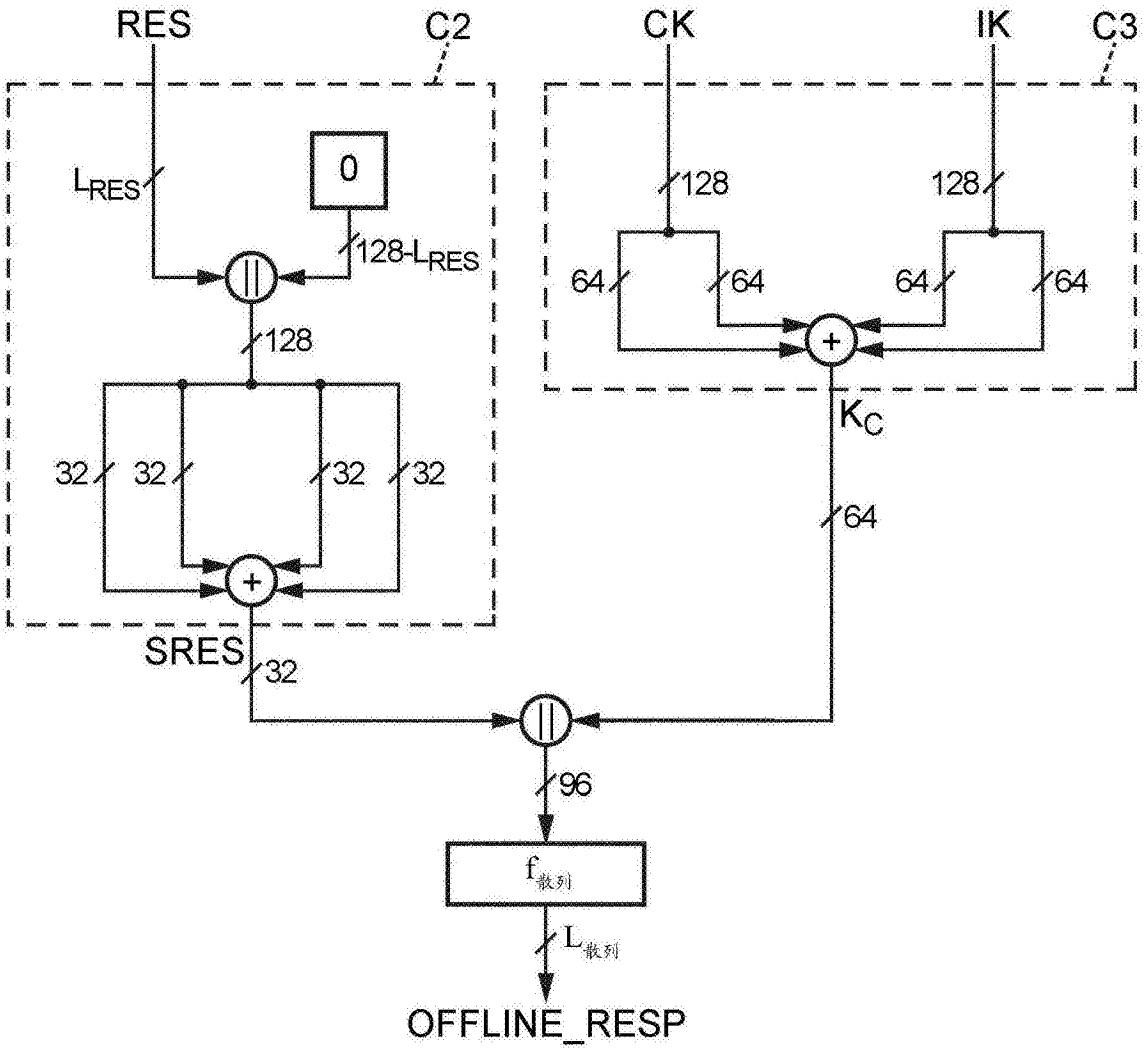

RES
C2
CK
IK
C3
L_{RES}
0
128-L_{RES}
128
128
128
64
64
64
64
32
32
32
32
K_C
64
SRES
32
96
$f_{散列}$
$L_{散列}$
OFFLINE_RESP

图5

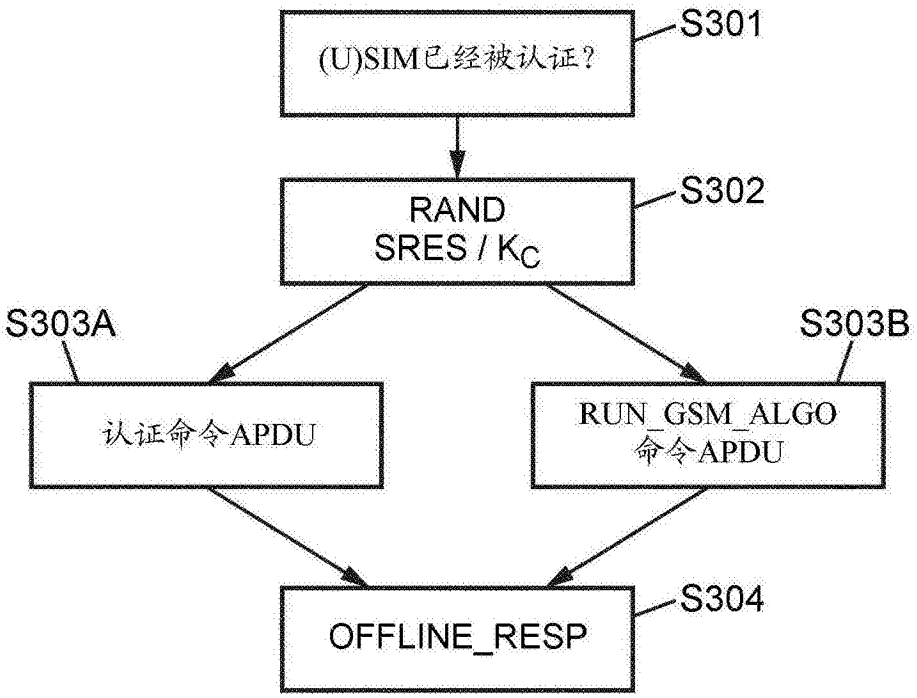

(U)SIM已经被认证？
S301
RAND
SRES / KC
S302
S303A
S303B
认证命令APDU
RUN_GSM_ALGO
命令APDU
OFFLINE_RESP
S304

图6

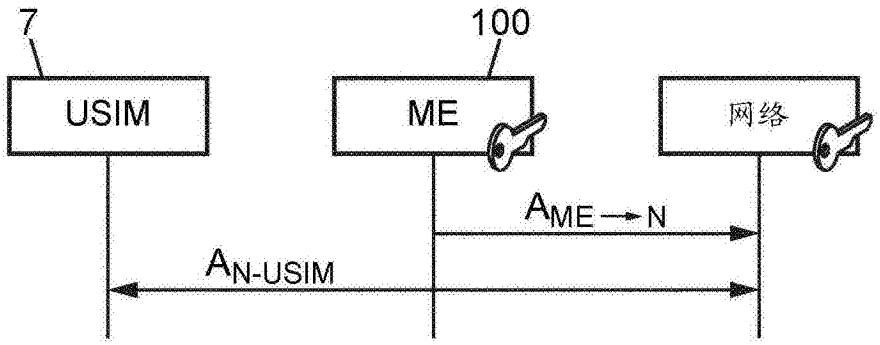

7
100
USIM
ME
网络
AME → N
AN-USIM

图7A

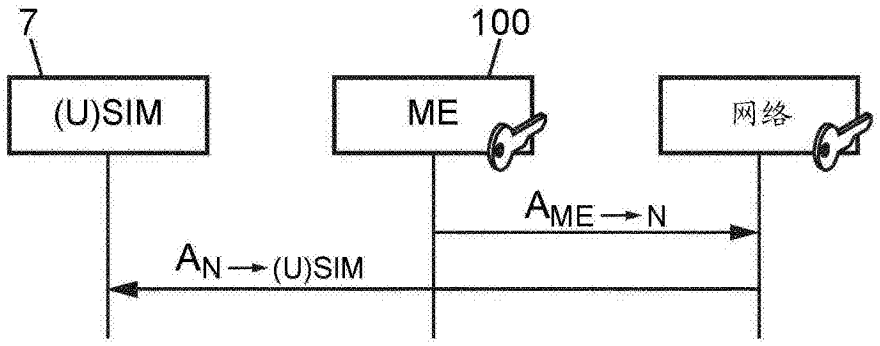

7
100
(U)SIM
ME
网络
AME → N
AN → (U)SIM

图7B

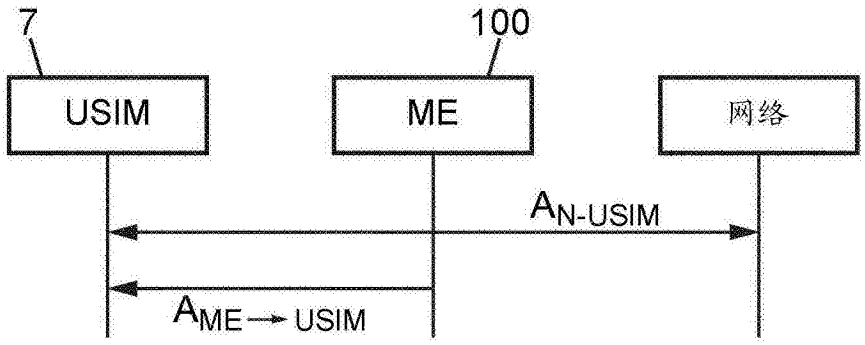

7
100
USIM
ME
网络
$A_{N\text{-}USIM}$
$A_{ME \rightarrow USIM}$

图8A

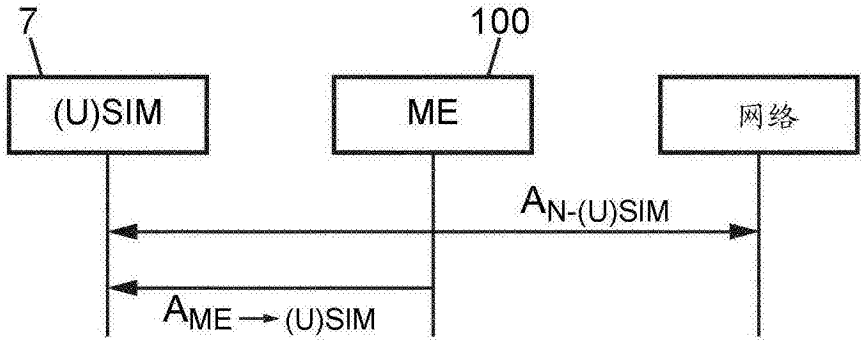

7
100
(U)SIM
ME
网络
$A_{N\text{-}(U)SIM}$
$A_{ME \rightarrow (U)SIM}$

图8B

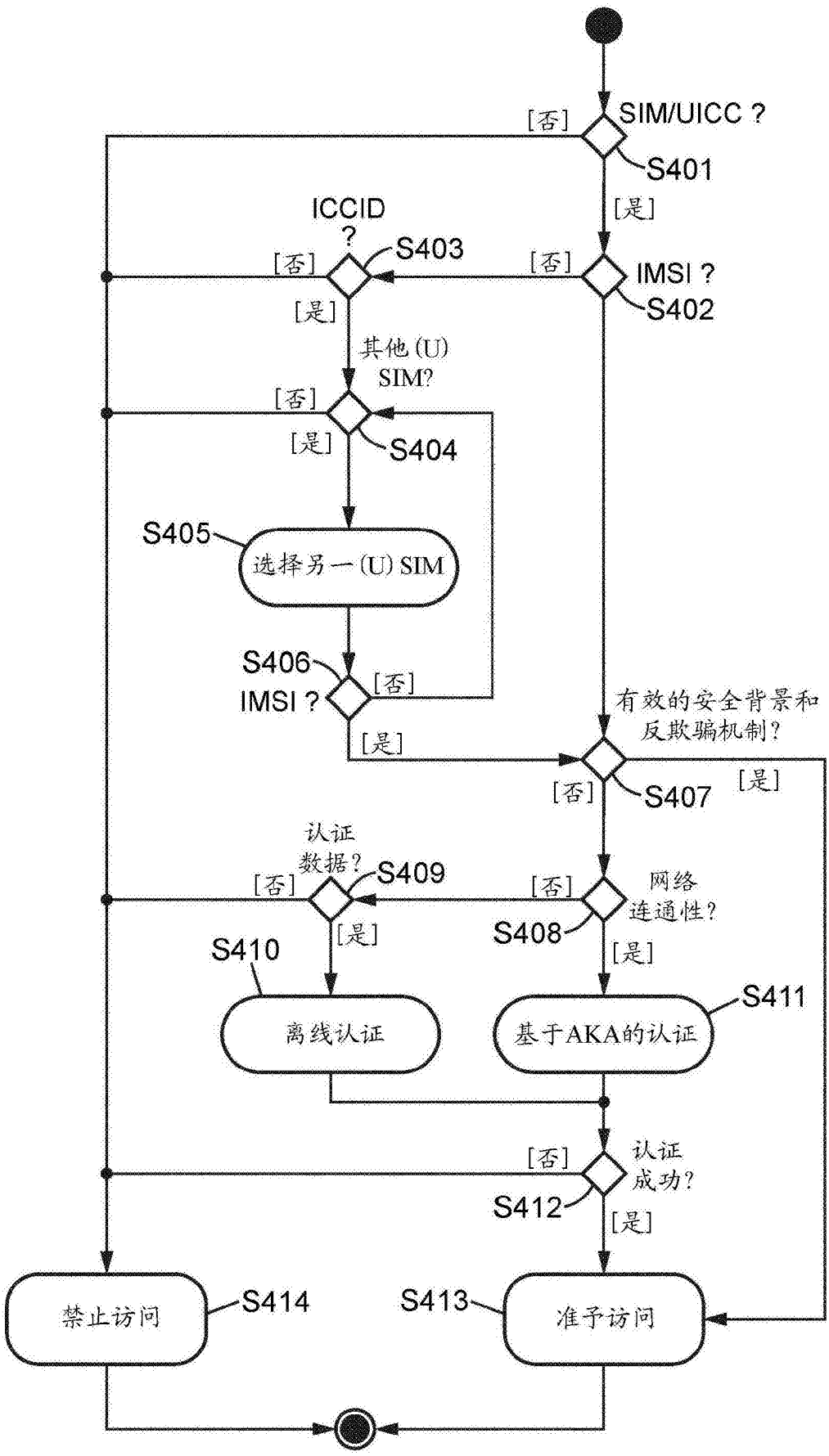

SIM/UICC ?
S401
[否]
[是]
IMSI ?
S402
[否]
ICCID ?
S403
[否]
[是]
其他(U) SIM?
S404
[否]
[是]
S405
选择另一(U) SIM
S406
IMSI ?
[否]
[是]
有效的安全背景和反欺骗机制?
S407
[否]
[是]
网络连通性?
S408
[否]
[是]
认证数据?
S409
[否]
[是]
S410
离线认证
S411
基于AKA的认证
认证成功?
S412
[否]
[是]
禁止访问
S414
S413
准予访问

图9

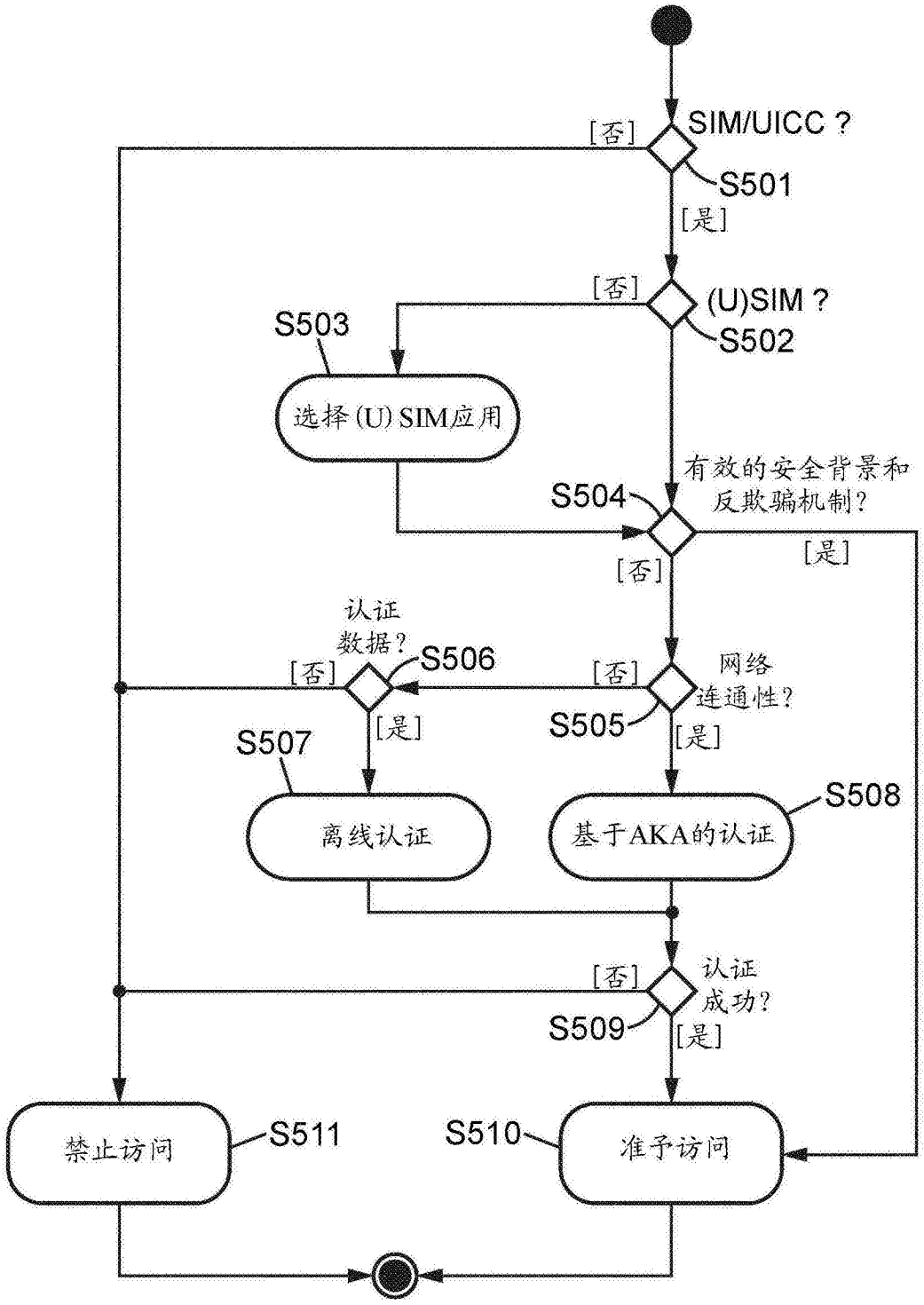

SIM/UICC ?
[否]
S501
[是]
(U)SIM ?
[否]
S502
S503
选择(U) SIM应用
有效的安全背景和
反欺骗机制?
S504
[否]
[是]
认证
数据?
[否]
S506
网络
连通性?
[否]
S505
[是]
[是]
S507
离线认证
基于AKA的认证
S508
认证
成功?
[否]
S509
[是]
禁止访问
S511
S510
准予访问

图10

FIG. 11

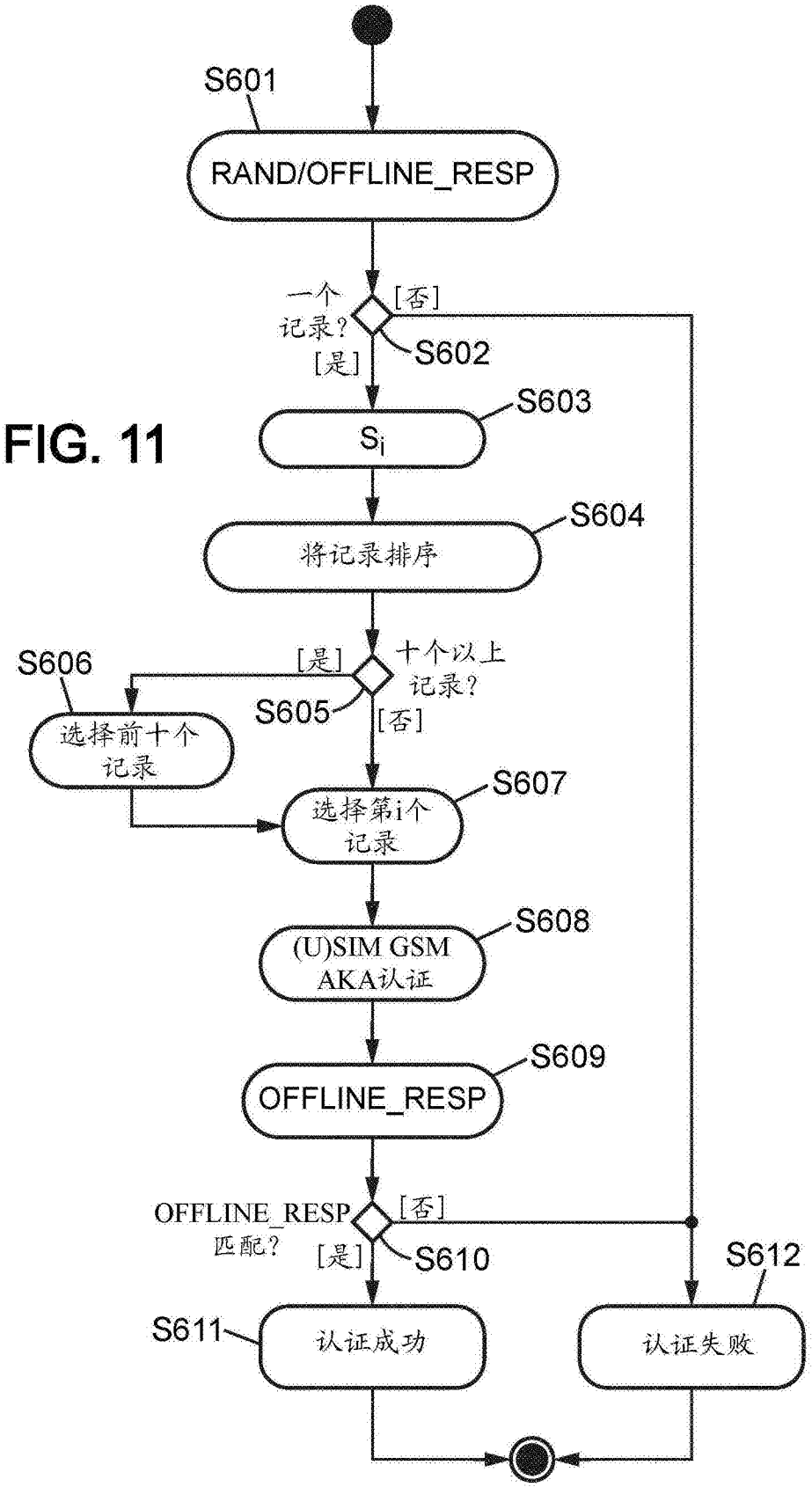

S601
RAND/OFFLINE_RESP
一个记录?
[否]
[是]
S602
S603
Si
S604
将记录排序
S606
[是]
十个以上记录?
S605
[否]
选择前十个记录
S607
选择第i个记录
S608
(U)SIM GSM AKA认证
S609
OFFLINE_RESP
OFFLINE_RESP匹配?
[否]
[是]
S610
S612
S611
认证成功
认证失败

图11

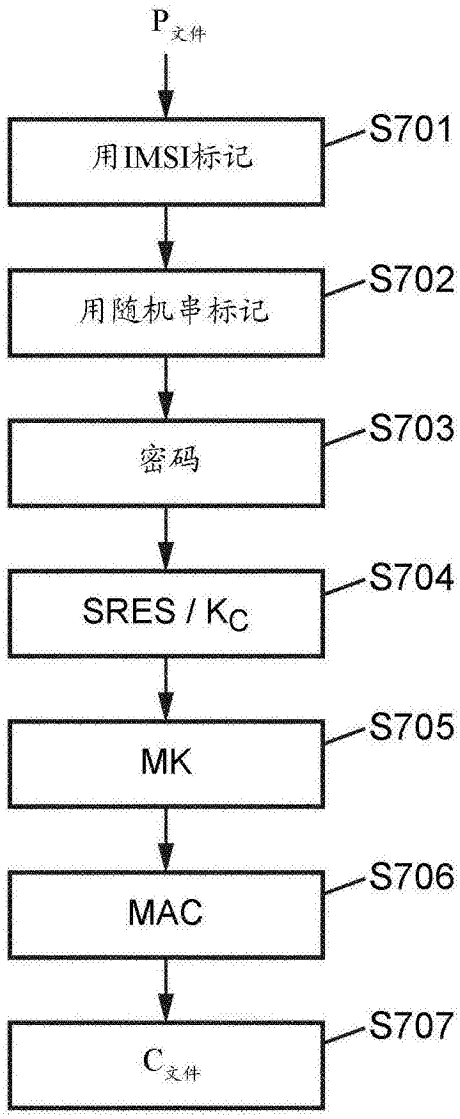

$P_{文件}$
用IMSI标记
S701
用随机串标记
S702
密码
S703
SRES / K_C
S704
MK
S705
MAC
S706
$C_{文件}$
S707

图12

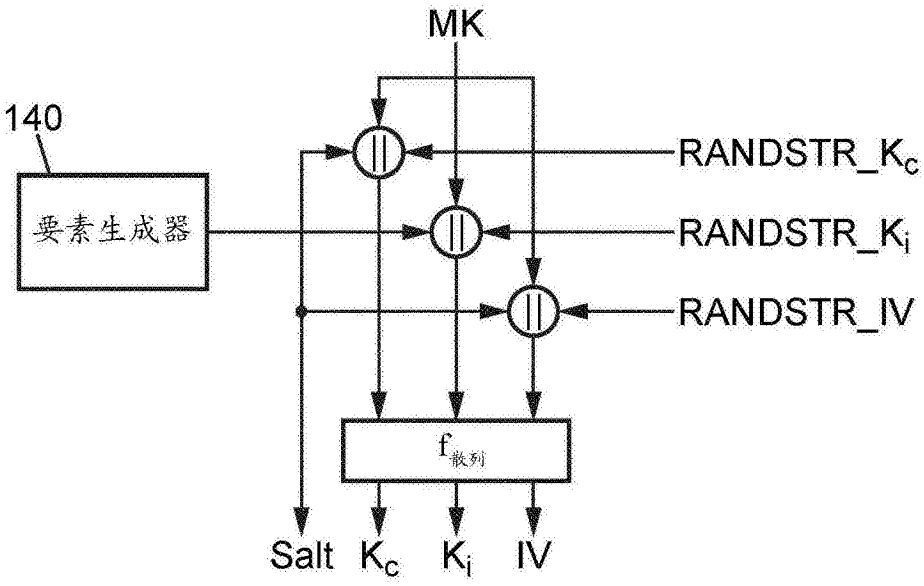

MK
140
要素生成器
RANDSTR_Kc
RANDSTR_Ki
RANDSTR_IV
f散列
Salt
Kc
Ki
IV

图14

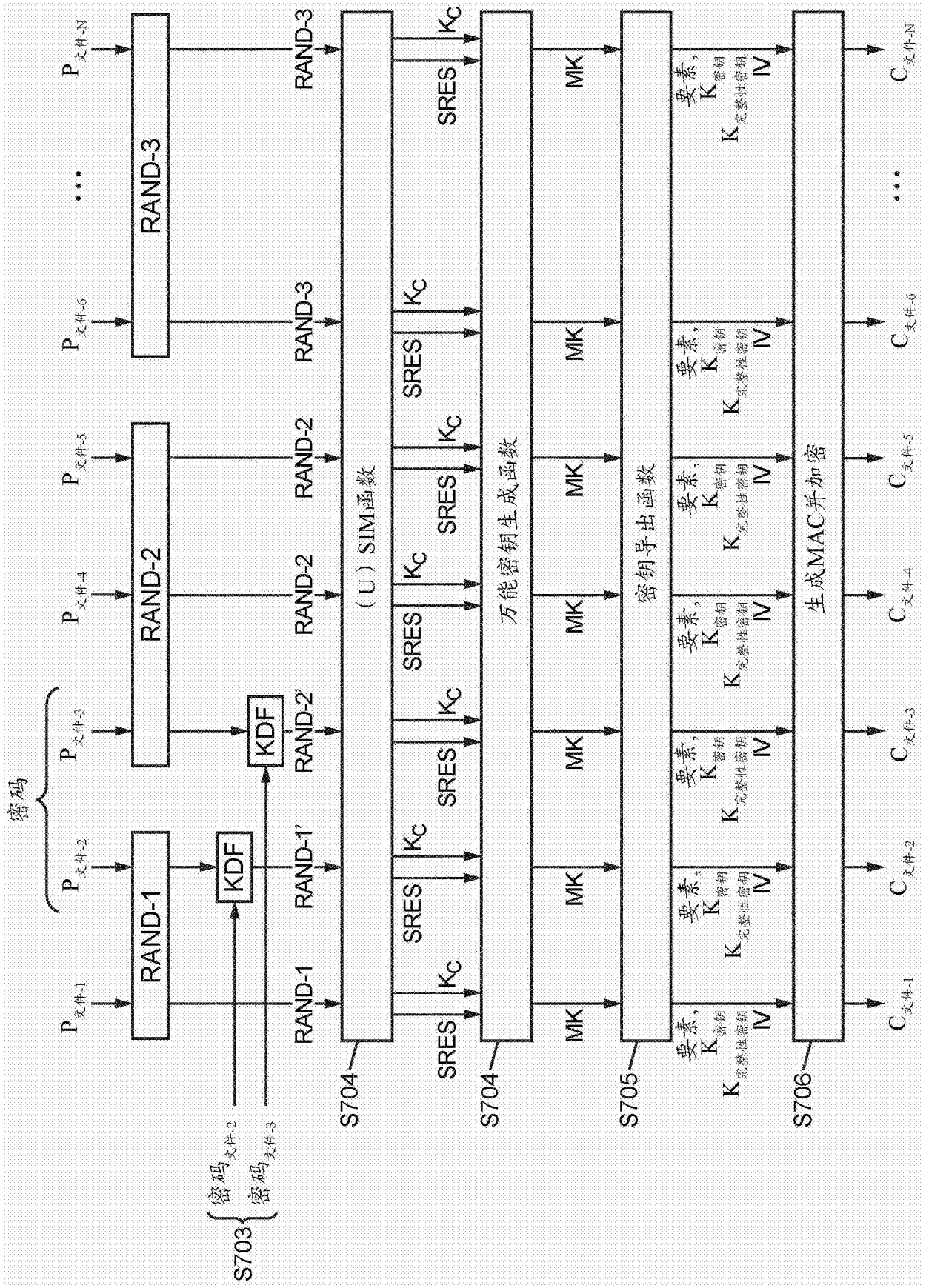

密码
RAND-1
RAND-2
RAND-3
KDF
KDF
RAND-1
RAND-1'
RAND-2
RAND-2'
RAND-3
S703
密码文件-2
密码文件-3
S704
(U)SIM函数
SRES
Kc
S704
万能密钥生成函数
S705
密钥导出函数
MK
S706
生成MAC并加密
要素,
K密钥
K完整性密钥
IV

图13

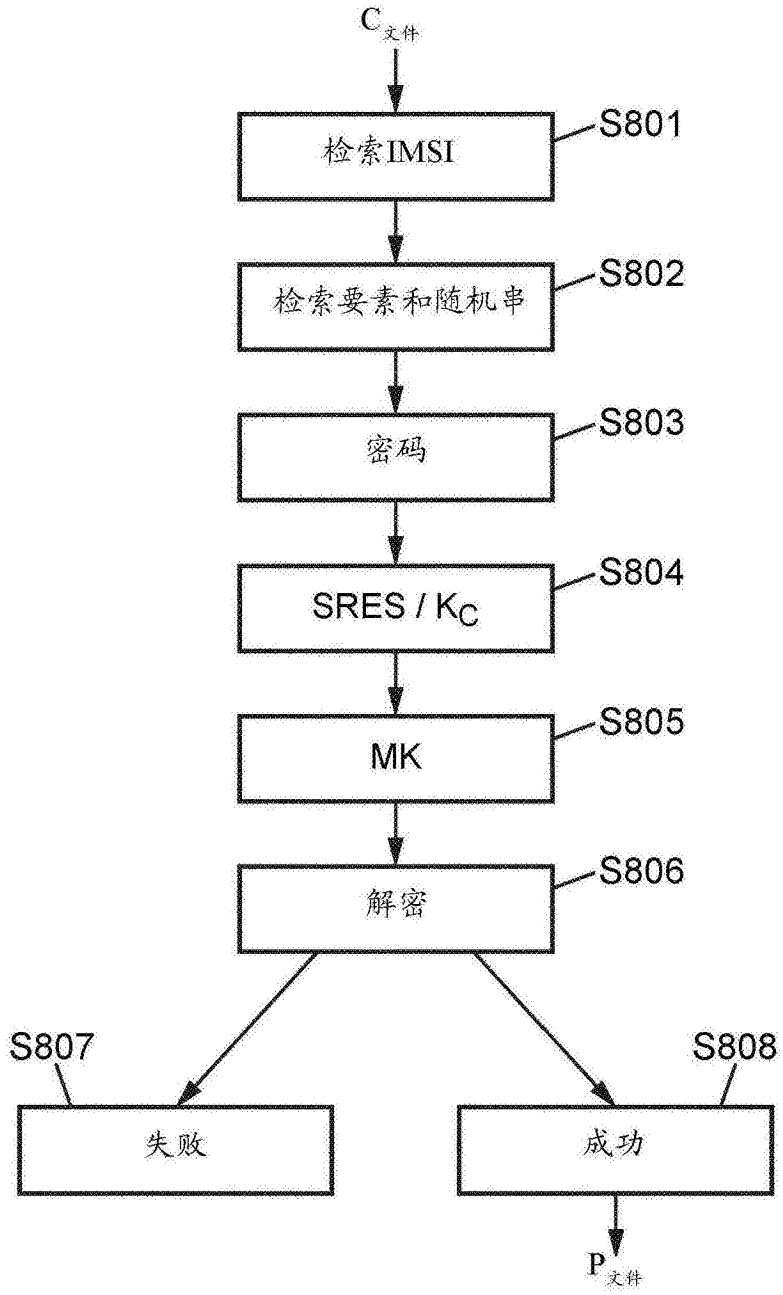

C文件
检索IMSI
S801
检索要素和随机串
S802
密码
S803
SRES / KC
S804
MK
S805
解密
S806
S807
失败
S808
成功
P文件

图15

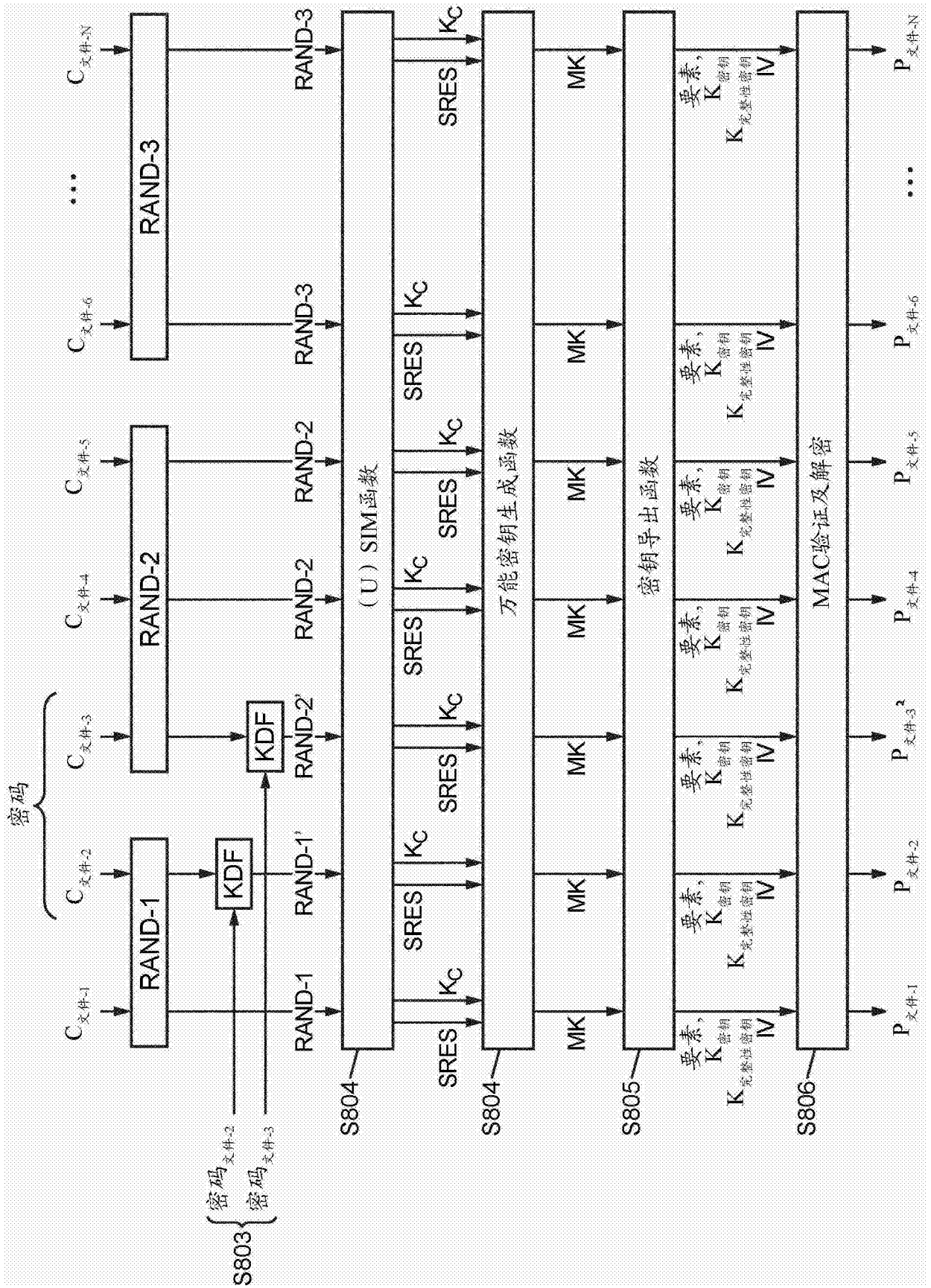

密码
C文件-1
C文件-2
C文件-3
C文件-4
C文件-5
C文件-6
C文件-N
RAND-1
RAND-2
RAND-3
KDF
RAND-1'
RAND-2'
RAND-1
RAND-2
RAND-3
S803
密码文件-2
密码文件-3
(U) SIM函数
S804
SRES
Kc
万能密钥生成函数
MK
密钥导出函数
S805
要素,
K密钥
K完整性密钥
IV
MAC验证及解密
S806
P文件-1
P文件-2
P文件-3'
P文件-4
P文件-5
P文件-6
P文件-N

图16