(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 101366299 B
(45)授权公告日 2012.12.05

(21)申请号 200580037634.3

(22)申请日 2005.09.06

(30)优先权数据
60/608,305 2004.09.08 US
11/218,885 2005.09.02 US

(85)PCT申请进入国家阶段日
2007.04.29

(86)PCT申请的申请数据
PCT/US2005/032337 2005.09.06

(87)PCT申请的公布数据
WO2006/036521 EN 2006.04.06

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 J·森普尔 G·G·罗斯 M·帕登 P·M·霍克斯

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邵亚丽

(51)Int.Cl.
H04L 9/32(2006.01)
H04W 12/04(2006.01)

(56)对比文件
DE 10128300 A1,2003.01.09,参见说明书第23,27-29,40-50段、附图3.
US 6711400 B1,2004.03.23,参见说明书第3栏第58行至第5栏第12行、附图3-4.
US 6711400 B1,2004.03.23,参见说明书第3栏第58行至第5栏第12行、附图3-4.
CN 1349723 A,2002.05.15,全文.
DE 10128300 A1,2003.01.09,参见说明书第23,27-29,40-50段、附图3.

审查员 苗雨

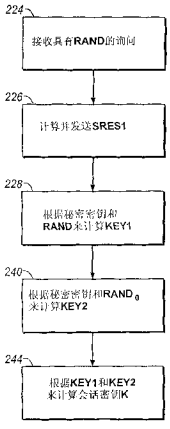
权利要求书 2 页 说明书 7 页 附图 6 页

(54)发明名称

使用特殊随机询问的引导认证

(57)摘要

本发明公开了一种使移动台认证引导和建立安全加密密钥的通信系统和方法。在通信网络的一个实施例中,特殊随机询问被保留以用于生成安全加密密钥,其中特殊随机询问不被用于移动台的认证。特殊随机询问被存储在移动台的移动设备处并被用于生成安全加密密钥,并且网络中的引导功能使用正常随机询问来认证移动台并使用特殊随机询问来生成安全加密密钥。



CN 101366299 B

1. 一种用于在无线通信网络中进行通信并使用询问 - 响应认证过程的移动台，包括 ：

接收器，其被配置成从所述无线通信网络接收形成第一询问值的至少一个认证数据参数 ；

存储器，其存储形成第二保留的询问值的固定数据参数值，该第二保留的询问值用于生成在所述移动台和通信网络之间通信时使用的密钥，其中所述保留的询问值未被用于移动台认证 ；

第一处理电路，其被配置成基于所述至少一个接收到的认证数据参数生成第一密钥，并基于所述保留的询问值生成第二密钥 ；和

第二处理电路，其被配置成至少使用所述第一和第二密钥来生成在所述通信中使用的第三密钥。

2. 如权利要求 1 所述的移动台，其中，所述第二处理电路被配置成通过使用所述第三密钥来对通信传输进行加密。

3. 如权利要求 1 所述的移动台，其中，所述至少一个接收到的认证数据参数包括对于所述移动台和所述通信网络之间的不同的通信会话会发生改变的随机数或伪随机数。

4. 如权利要求 3 所述的移动台，其中，在所述移动台被配置成拒绝包含所述固定数据参数值的认证请求。

5. 如权利要求 1 所述的移动台，其中，所述第一处理电路被配置成通过使用至少一个接收到的认证数据参数和秘密密钥来生成认证响应。

6. 如权利要求 5 所述的移动台，其中，所述移动台被配置成通过所述无线通信信道发送用于所述移动台的认证的所述认证响应。

7. 如权利要求 1 所述的移动台，其中，所述第一处理电路包括安全集成电路。

8. 如权利要求 7 所述的移动台，其中，所述安全集成电路包括用户标识模块 (SIM)。

9. 一种在移动台处生成用于保护所述移动台和网络组件之间的通信安全的密钥的方法，所述方法包括 ：

在所述移动台处从所述网络组件接收第一认证询问值作为询问 - 响应认证过程的一部分 ；

将所述认证询问值发送给处理电路 ；

通过至少使用所述认证询问值来生成第一密钥 ；

将第二保留的询问值发送给所述处理电路，该第二保留的询问值用于生成在所述移动台和网络组件之间通信时使用的密钥，其中所述保留的询问值未被用于移动台认证 ；

通过至少使用所述第二保留的询问值来生成第二密钥 ；以及

通过使用至少所述第一密钥和至少所述第二密钥来生成用于保护通信安全的密钥。

10. 如权利要求 9 所述的方法 ：

其中，所述生成所述第一密钥的所述步骤包括生成包括所述第一密钥的值的第一集合，并且所述方法还包括将来自所述第一集合的至少一个值发送给所述网络组件用于认证 ；和

其中所述生成所述第二密钥的步骤还包括生成包括所述第二密钥的值得第二集合。

11. 如权利要求 10 所述的方法，其中，发送给网络组件的值的所述第一集合中的值包括带符号的响应 (SRES)。

12. 如权利要求 9 所述的方法，其中，采用所述处理电路为发送给所述处理电路的每个认证询问值生成带符号的响应和加密密钥。

13. 如权利要求 9 所述的方法，其中，所述第一认证询问值是随机数或伪随机数。

14. 如权利要求 9 所述的方法，该方法被用于通信网络中。

使用特殊随机询问的引导认证

[0001] 根据 35U.S.C. §119 要求的优先权

[0002] 本申请要求 2004 年 9 月 8 日提交的标题为“BOOTSRAPPING GSMAUTHENTICATION AND DISTINGUISHED RANDS”的美国临时专利申请第 60/608,305 号的优先权。由此将上述提交的申请的公开全部引用在此作为参考。

技术领域

[0003] 本申请一般涉及蜂窝通信网络中的认证，并更特别地涉及用于应用安全性的加密密钥的派生。

背景技术

[0004] 移动通信应用通常共同具有在通信被启动或者业务被执行之前通过通信服务器进行用户（用户设备或移动台）认证的需要。一种认证机制是基于通信实体之间共享的秘密，并且存在着许多依靠该预共享秘密的认证协议。

[0005] 例如，在基于全球移动通信系统 (GSM) 的移动通信网络中，在允许用户接入通信网络之前对用户的身份进行认证。为了使用户的移动台（或用户设备 UE) 能够建立与网络组件的通信会话，移动台通过响应随机数询问而向网络组件证实自己的身份。随机数询问和共享的秘密密钥被用于建立会话加密密钥，该会话加密密钥用于对移动台和网络组件之间的通信传输进行加密。

[0006] 本文中描述的通信系统特征可以实现在要求认证和通信实体之间的加密通信的各种通信网络中。图 1 是 GSM 网络中的用户认证过程中所涉及的通信网络实体的框图。用户的移动台 30 包括安全 IC 32 和移动设备 (ME)34（例如，蜂窝电话手持机）。移动设备 34 包括配置成在移动台 30 处与安全 IC 32 一起执行认证功能的处理器 36。

[0007] 存储在安全 IC 32 上的是用户标识和相关预定信息、用于向通信网络执行认证功能的信息、国际移动用户标识 (IMSI)、偏好的语言，以及 IC 卡识别。安全 IC 可被称为 SIM 卡或智能卡。也存储在安全 IC 32 上的是用于向服务网络的网络组件 40 认证移动台 30 以便接入网络的秘密密钥 Ki 38。秘密密钥 Ki 38 也被存储在移动台的归属网络中的认证中心 (AuC)42 中。认证中心 42 使用秘密密钥 Ki 38 来生成专门用于使用该秘密密钥 Ki 38 的用户的认证数据，并将认证数据发送给网络组件 40。

[0008] 图 1-3 示出了用于移动台认证和加密通信的认证和密钥生成处理，其中图 2 是示出一种在移动台 30 处进行认证和加密密钥生成的方法的流程图，并且图 3 是示出一种在通信网络中进行移动台认证和加密密钥生成的方法的信号流图。参考图 3，移动台 30 在步骤 102 中向网络组件 40 请求通信会话。如果网络组件 40 还不具有为该用户存储的用于认证移动台 30 的安全信息，则网络组件 40 在步骤 104 中向移动台的归属网络中的认证中心 42 发送对安全信息的请求。响应于该安全信息请求，认证中心 42 生成包括随机数询问 RAND、预期认证响应 XRES 和加密密钥 Kc 的一个或多个认证向量。预期响应 XRES 和加密密钥 Kc 是基于 RAND 和秘密密钥 Ki 38 来确定的。在步骤 108 中，认证中心 42 向网络组件 40 发送

认证向量 (RAND，XRES，Kc)。

[0009] 网络组件 40 选择将在认证移动台 30 的身份的过程中使用的认证向量 (RAND，XRES，Kc)，并在步骤 112 中将所选择的认证向量的随机数询问 RAND 发送给移动台 30。参考图 2，移动台 30 在步骤 112 中接收具有询问 RAND 的认证询问，并在步骤 114 中计算和发送认证响应。移动台 30 还在步骤 115 中通过使用秘密密钥 Ki 38 和 RAND 来计算会话密钥。

[0010] 为了产生响应和会话密钥，移动台 30 处的移动设备 34 在步骤 113 中将 RAND 传递给安全 IC。在步骤 114 和 115 中，安全 IC 通过使用接收到的随机询问 RAND 和所存储的秘密密钥 Ki 来计算一个或多个值的集合。这些值通常包括步骤 114 中所示的认证响应 SRES。在步骤 115 中，安全 IC 32 通过使用接收到的随机询问 RAND、所存储的秘密密钥 Ki 38 来计算包括会话加密密钥 Kc 的第二值。在步骤 116 中，安全 IC32 在步骤 116 中将所生成的响应 SRES 和加密密钥 Kc 发送给移动设备 34。移动设备 34 在步骤 117 中将所生成的认证响应 SRES 发送给网络组件 40，并在步骤 118 中将密钥 Kc 存储在移动设备处。网络组件 40 在步骤 119 中将移动台生成的认证响应 SRES 与所选择的认证向量的预期响应 XRES 进行比较。如果认证参数不匹配，则终止认证过程。如果参数匹配，则在步骤 120 中认为移动台 30 是得到认证的，并且网络组件 40 在步骤 122 中开始通过使用加密密钥 Kc 与移动单元进行通信。

[0011] GSM 认证和密钥协商过程易受重放和密码分析攻击。例如，由 GSM 系统使用的对通信进行加密的常规算法是较弱的。确定加密密钥 Kc 并确定用户的通信内容的方法已经被想出。因此在本领域中需要有一种尤其是在移动通信被用于更敏感的数据或者需要更强的认证时，能够使用当前配置的移动台的能力来改善应用安全性的方法。

发明内容

[0012] 在一个方面，本发明包括配置成用于在无线通信网络中通信的移动台。该移动台包括配置成从无线通信网络接收至少一个认证数据参数的接收器，和存储固定认证数据参数的存储器。第一处理电路被配置成基于至少一个接收到的认证数据参数而生成第一密钥，并基于固定认证数据参数而生成第二密钥。第二处理电各被配置成使用至少第一和第二密钥来生成第三密钥。

[0013] 在另一方面，提供了一种无线通信网络的移动组件。该无线通信网络包括多个移动组件和与移动组件通信的多个网络组件。移动组件被配置成通过在认证过程期间响应由通信网络的网络组件提供给移动组件的询问值，来向通信网络证实自己的身份。此外，移动组件包括存储器，该存储器存储未被用于在任何网络组件和任何移动组件之间的认证过程中对移动组件进行认证的保留的询问值。

[0014] 在另一方面，本发明包括在移动台和通信网络组件之间进行通信的方法。该方法包括在网络组件处选择认证询问并将该认证询问传送给移动台。该方法还包括在移动台处通过至少使用认证询问和所存储的密钥来生成包括认证响应的第一值；在移动设备处通过至少使用认证询问和所存储的密钥来生成第二值；在移动设备处通过至少使用与认证询问和所存储的密钥不同的第四值来生成第三值；以及通过至少使用第二和第三值来生成密钥。

[0015] 在另一方面，提供了一种在使用询问 - 响应认证过程的通信网络中生成密钥的方

法，该方法包括保存至少一个用于生成会话密钥的询问值，该会话密钥用于通信网络内的移动单元和网络组件之间的通信。该保留的询问值未被用于移动单元认证。

[0016] 在另一方面，提供了一种在移动台处生成用于保护移动台和网络组件之间的通信安全的密钥的方法。在该方面中，该方法包括在移动台处从网络组件接收认证询问值并将认证询问值发送给处理电路。该方法还包括通过至少使用认证询问值来生成一个或多个值的第一集合，将来自第一集合的至少一个值发送给网络组件以用于认证。该方法继续将第二认证询问值发送给处理电路并通过至少使用第二认证询问来生成一个或多个值的第二集合。通过使用第一集合的至少一个值和第二集合的至少一个值来生成密钥。

[0017] 在另一方面，提供了一种通信网络中的移动台，该移动台包括用于从移动网络接收认证询问值的装置，用于响应于接收到的认证询问而生成值的第一集合的装置，用于响应于特殊认证询问值而生成值的第二集合的装置，以及用于通过使用值的第一集合中的至少一个和值的第二集合中的至少一个来生成密钥的装置。

附图说明

[0018] 图 1 是 GSM 网络中对用户进行认证以便进行通信的过程中所涉及的通信网络实体的框图；

[0019] 图 2 是示出在根据 GSM 的移动台处执行的认证和密钥生成处理的流程图；

[0020] 图 3 是示出在 GSM 中用于向网络组件证实用户的身份的认证和密钥协商过程的信号流程图；

[0021] 图 4 是使用特殊认证数据对用户进行认证的过程中所涉及的通信网络实体的一个实施例的框图；

[0022] 图 5 是示出在移动台处通过使用特殊认证数据而执行的认证和特殊密钥生成处理的一个实施例的流程图；并且

[0023] 图 6 是示出通过使用特殊认证数据而在移动台和通信网络之间建立安全通信会话的方法的一个实施例的信号流程图。

具体实施方式

[0024] 如上所述，GSM 加密算法 A5/1 和 A5/2 易受攻击，并且已经发现了获得对加密密钥的认识并从而从移动台 30 获得未授权的信息的方法。因此，在本文中将描述得到改善的认证和密钥生成过程，其中认证和密钥生成过程被实现在这样的一个实施例中：由移动用户的安全 IC 32 执行的功能仍与图 2-3 中所示的过程相同，但是由移动设备 ME 执行的功能是不同的。具体而言，本文中描述的认证和密钥生成过程的实施例可以通过使用已经配置好的安全 IC 32 而实现在新移动台终端中，以便派生出不受 GSM 无线电接口加密的弱点连累的用于应用安全性的密钥。

[0025] 图 4 是使用特殊认证数据对用户进行认证的过程中所涉及的通信网络实体的一个实施例的框图。图 4 中所示的通信网络包括类似于图 1 的移动台 30 的移动台 202，其中图 3 的移动台 202 包括存储秘密密钥 38 的安全 IC 32。然而，移动台 202 的移动设备 204 与图 1 的移动台 30 的移动设备 34 的不同之处在于，移动设备 204 在其存储器中存储特殊的或保留的认证数据，诸如特殊随机数询问 RAND 206。移动设备 204 还包括处理器 208。

[0026] 除了响应于从网络接收到的RAND而产生的值的集合外，移动设备204还使用特殊RAND 206来生成值的第二集合作为认证处理的一部分。移动台通过使用根据从网络接收到的询问RAND而产生的值和根据存储在移动台中的特殊RAND而产生的值，来计算“特殊的”会话密钥K。特殊RAND具有为网络和移动设备所知的预定的固定值。例如，其可以具有全零值，并在本文中被指定为$RAND_0$。认证中心42也存储特殊RAND使得网络也能够计算特殊密钥K。特殊密钥K在其被生成后可用于各种目的，包括对将来的通信、业务等中的消息认证代码进行加密或上锁。特殊密钥K可被用于通过诸如GPRS、蓝牙或WLAN的各种承载，为要求增加安全性的应用（诸如银行应用）保护移动台202和网络组件之间的通信的安全。特殊RAND由系统保留以用于生成特殊密钥K，并且特殊RAND不被用于初始认证过程，使得$RAND_0$和对$RAND_0$的带符号的响应($SRES_0$)都不通过无线通信链路传递。

[0027] 图5-6示出了用于图4的网络实体的认证和安全密钥生成处理，其中图5是示出在移动台202处进行认证和安全密钥生成的方法的一个实施例的流程图，并且图6是示出用于在网络中建立安全通信的认证和安全密钥生成处理的一个实施例的信号流程图。

[0028] 参考图6，网络组件40从用户的归属网络中的认证中心(AuC)42获得专门用于用户的认证数据。在步骤214中，认证中心42使用随机询问RAND和秘密密钥Ki来生成一个或多个认证向量(RAND，XRES，Kc)。认证中心42还通过使用特殊随机询问$RAND_0$ 206和秘密密钥Ki，来生成一个或多个特殊认证向量($RAND_0$，$XRES_0$，Kc_0)。在步骤216中，认证中心通过使用Kc、Kc_0、XRES和$XRES_0$来计算特殊会活密钥K。在一个实施例中，特殊密钥K是Kc、Kc_0、XRES和$XRES_0$的散列。在步骤220中，认证中心42将认证向量和特殊认证向量都发送给网络组件40。利用该信息，网络组件也可以基于认证中心所提供的信息来计算特殊密钥K。

[0029] 本领域的技术人员将可以理解，特殊密钥K可以基于值的多种组合而被生成，而并不限于本文中所描述的那些。例如，特殊密钥K可以除了Kc、Kc_0、XRES和$XRES_0$之外还基于RAND和$RAND_0$而被生成，或者可以基于RAND和$RAND_0$而不基于Kc、Kc_0、XRES和$XRES_0$而被生成。此外，各种变形例可以用于通过使用密钥K而向网络组件提供与移动台通信所必要的信息。网络组件40可以直接从认证中心接收形成特殊密钥K的散列值而不是上述的特殊认证向量。可替换地，网络组件可以为不同的用户标识（例如，IMSI）保持$XRES_0$和Kc_0的数据库。

[0030] 图4是示出通过使用特殊认证数据来对移动用户进行认证的引导方法的一个实施例的信号流程图。根据图4中所示的方法的由网络组件执行的一些过程，类似于根据图2中所示的方法而执行的过程。

[0031] 为了认证移动台并生成会话密钥，网络组件40在步骤220中将认证请求发送给移动用户的移动设备204，其中认证请求仅包括随机数询问RAND，并且特殊$RAND_0$并不通过无线电网络从网络组件40传送到移动台202。参考图5，在移动台202处执行的认证和会话密钥生成处理开始于步骤224，在该步骤224中，移动设备204接收具有询问RAND的认证询问。在步骤226中，安全IC 32计算认证响应SRES1，并且移动设备204将该响应发送给网络组件40。在步骤228中，安全IC通过使用所存储的秘密密钥Ki和询问RAND来计算第一密钥KEY1。在步骤240中，安全IC 32通过使用存储在移动设备204处的特殊询问$RAND_0$和存储在安全IC 32处的秘密密钥Ki，来计算第二密钥KEY2。在步骤244中，移动设备204

根据 KEY1 和 KEY2 计算会话密钥 K。该密钥可以用在将来的通信或业务中。

[0032] 将参考图 6 中的网络组件 40 更详细地说明在安全 IC 32 和移动设备 204 处执行的认证和密钥生成处理。在接收到随机数询问 RAND 后，移动设备 204 在步骤 224 中将 RAND 发送给安全 IC 32。在步骤 226 中，安全 IC 通过使用 RAND 和秘密密钥 Ki 38 来生成认证或带符号的响应 SRES，并且安全 IC 在步骤 228 中通过使用 RAND 和秘密密钥 Ki 来计算密码密钥 Kc。安全 IC 32 在步骤 230 中将认证响应 SRES 和密码密钥 Kc 都发送给移动设备 204，并且移动设备 204 在步骤 230 中将认证响应 SRES 传送给网络组件 40。网络组件 40 在步骤 234 中将来自移动组件 204 的认证响应 SRES 与所选择的认证向量中的预期响应 XRES 进行比较，这类似于图 3 中的步骤 119。

[0033] 在步骤 236 中，移动设备 204 将存储在移动设备 204 处的特殊随机询问 $RAND_0$206 发送给安全 IC 32，安全 IC 32 在步骤 238 中基于特殊 $RAND_0$ 计算特殊认证响应 $SRES_0$，这类似于使用秘密密钥 Ki 的步骤 226。安全 IC 32 还在步骤 240 中通过使用秘密密钥 Ki 来计算特殊密码密钥 Kc_0。安全 IC 32 然后在步骤 242 中将特殊认证响应 $SRES_0$ 和特殊密码密钥 Kc_0 传送给移动设备 204。这样，根据图 6 中所示的本发明的实施例，可以使用图 3 的认证处理中所使用的相同的安全 IC 来生成特殊密码密钥 Kc_0。

[0034] 响应于特殊认证响应 $SRES_0$ 和特殊密码密钥 Kc_0 的接收，移动设备 204 在步骤 244 中生成特殊会话密钥 K。在一个实施例中，基于由安全 IC 32 在步骤 226 和 228 中通过使用 RAND 而生成的密码密钥 Kc 和认证响应 SRES，以及由安全 IC 32 在步骤 238 和 240 中通过使用 $RAND_0$ 而生成的特殊密码密钥 Kc_0 和特殊认证响应 $SRES_0$，来生成特殊密钥 K。移动设备在步骤 246 中存储特殊密钥 K。利用存储在移动设备 204 和网络组件 40 二者处的特殊密钥 K，可以在将来的通信和业务中使用密钥 K。在一些实施例中，移动设备 204 被配置成拒绝包括特殊 RAND 值的认证请求，以确保对保留的 RAND 值的带符号的响应从未通过无线通信链路被发送并且所得到的密码密钥 Kc_0 不被用于无线链路上的加密。

[0035] 因此，根据图 4-6 中所示的认证和密钥生成处理，允许密钥 K 供应用使用，从而再利用了现有的 GSM SIM、认证中心以及移动终端和 SIM 之间的接口，而密钥不会由 GSM 空中接口的安全性弱点所暴露。

[0036] 在一个实施例中，移动设备 204 被配置成生成特殊认证响应 DRES 以替代认证响应 SRES，而向网络组件 40 证实移动台 202 的身份。例如，可以将移动设备 204 配置成基于 XRES、XRES0、Kc、Kc_0 而生成特殊密钥 DRES。在这样的实施例中，网络组件 40 接收在认证中心 42 处生成的预期特殊认证响应 DRES，或者网络组件 40 被配置成基于接收到的参数 SRES、SRES0、Kc 和 Kc_0 而生成预期特殊响应 DRES。网络组件 40 还被配置成将移动设备 204 所生成的特殊认证数据 DRES 与用于认证移动台 202 的预期特殊响应进行比较。

[0037] 在一些实施例中，参考图 4-6 讨论的认证和密钥生成处理还采用移动台的归属网络中的引导功能来引导认证和密钥生成处理。引导的处理可以与要求提高安全性的通信会话（诸如移动台和电子商务网络应用功能之间的通信会话）一起用于认证和密钥生成。在这样的实施例中，移动台与引导功能一起执行认证和密钥生成处理，而不是与网络组件 40 一起执行认证和密钥生成处理，在这种情况下，引导功能从认证中心 42 接收认证向量和会话密钥 K。在移动台的认证之后，引导功能接着将会话密钥 K 发送给电子商务网络应用功能以用于加密与移动台的通信。

[0038] 在采用引导处理的通信网络中，可以将移动设备 204 配置成采用图 2-3 中所示的安全 IC 32 来执行认证和密钥生成处理以用于语音呼叫，其中密码密钥 Kc 被用于加密与网络组件的通信。可以将移动设备 204 进一步配置成识别要求增加安全性的通信会话类型（诸如电子商务），并相应地采用图 5-6 中所示的安全 IC 32 来执行认证和密钥生成处理，其中会话密钥 K 被用于对通信进行加密。不管移动设备 204 所执行的认证和密钥生成处理如何，由安全 IC 32 执行的处理仍保持不变，即，接收随机询问并基于随机询问和所存储的秘密密钥 Ki 来计算带符号的响应和加密密钥。

[0039] 图 4-6 中所示的认证和密钥生成处理的示例性实现方案是移动台和银行机构之间的通信会话，其中移动用户期望与网络应用交换敏感信息，并因此期望增加通信安全性。在本实例中，移动台通过向该移动台的归属网络中的引导功能传送请求，而请求与银行网络应用功能进行通信。引导功能从认证中心获得标准 (RAND, XRES, Kc) 和特殊认证向量 ($RAND_0$, $XRES_0$, Kc_0) 以及会话密钥 K 以用于对请求进行通信的移动台的身份进行认证。引导功能将随机询问 RAND 发送给移动台的移动设备。移动设备将随机询问 RAND 发送给它的安全 IC 以用于计算响应 SRES 和密码密钥 Kc。响应于从安全 IC 接收到响应 SRES 和密码密钥 Kc，移动设备将响应 SRES 发送给引导功能，引导功能通过将 SRES 与 XRES 进行比较，来确定用于生成 SRES 的密钥是否与用于生成预期响应 XRES 的密钥相同。如果两个参数确实匹配，则认为移动台成功得到认证并且引导功能将会话密钥发送给网络应用功能（银行）。

[0040] 在将所生成的响应 SRES 发送给引导功能后，移动设备将存储在移动设备处的特殊 $RAND_0$ 发送给安全 IC 以用于计算特殊响应 $SRES_0$ 和特殊加密密钥 Kc_0。移动设备然后使用 Kc、SRES、Kc_0、$SRES_0$ 来计算特殊会话密钥 K。然后移动台和网络应用功能可以开始通过使用特殊会话密钥 K 对它们的通信传输进行加密，而开始安全的通信。

[0041] 本领域的专业技术人员将会理解，上述的系统和方法仅针对一些具体的实施例，并且本发明可以以许多方式来实施。本领域的专业技术人员可以理解，可以使用许多不同的工艺和技术中的任意一种来表示信息和信号。例如，上述说明中提到过的数据、指令、命令、信息、信号、比特、符号、及码片都可以表示为电压、电流、电磁波、磁场或磁性粒子、光场或光粒子、或以上的任何结合。

[0042] 本领域的专业技术人员还可以进一步意识到，结合本文中所公开的实施例描述的各种示例的逻辑块、模块、电路、方法及算法步骤，能够以电子硬件、计算机软件、或二者的结合被实现。为了说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各种示例的组件、组块、模块、电路、及步骤。这种功能究竟以硬件还是软件方式来实现，取决于整个系统的特定的应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现决定不应被认为超出了本发明的范围。

[0043] 结合本文中所公开的实施例描述的多种示例的逻辑块、模块和电路可以用通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑器件、分立门或晶体管逻辑、分立硬件部件、或设计成执行本文所述功能的以上的任意组合来实现或执行。通用处理器可以是微处理器，但是可替换地，处理器也可以是任何常规的处理器、控制器、微控制器、或状态机。处理器也可以被实现为计算器件的组合，例如，DSP 和微处理器的组合、多个微处理器的组合、一个或多个微处理器与一个 DSP 核心的组合、或任意其它此类配置。

[0044] 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块、或二者的结合来实施。软件模块可置于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的其它形式的存储介质中。可将存储介质连接到处理器，以便处理器可从存储介质读取信息并向存储介质写入信息。可替换地，存储介质可以被集成在处理器中。处理器和存储介质可以置于 ASIC 中。ASIC 可以置于用户终端中。在可选方案中，处理器和存储介质可以作为分立组件置于用户终端中。

[0045] 对所公开的实施例的上述说明，是为了使本领域的任何专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点一致的最宽的范围。

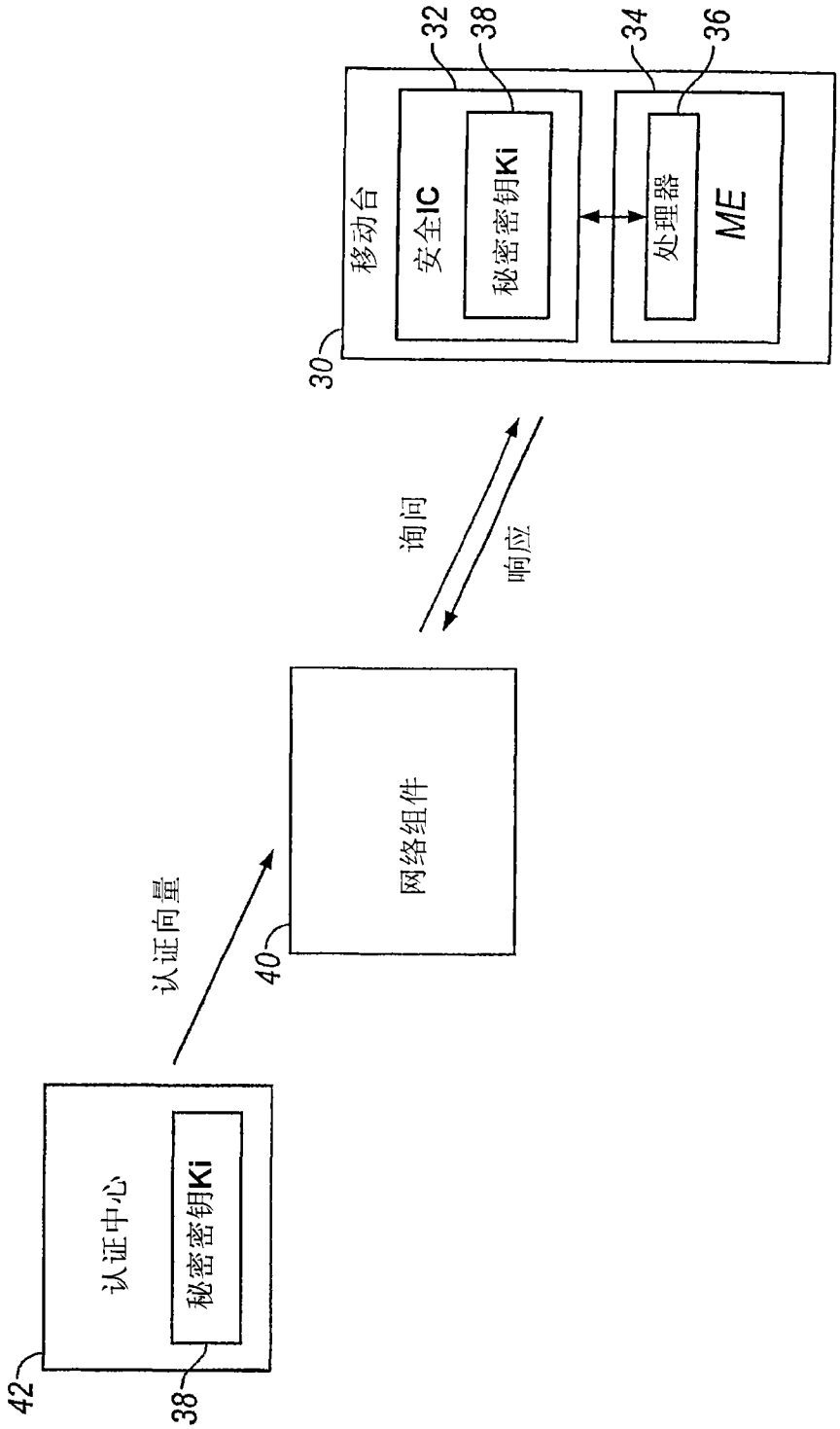

移动台
安全IC
秘密密钥Ki
处理器
ME
32
38
34
36
30
询问
响应
网络组件
40
认证向量
认证中心
秘密密钥Ki
42
38

图1

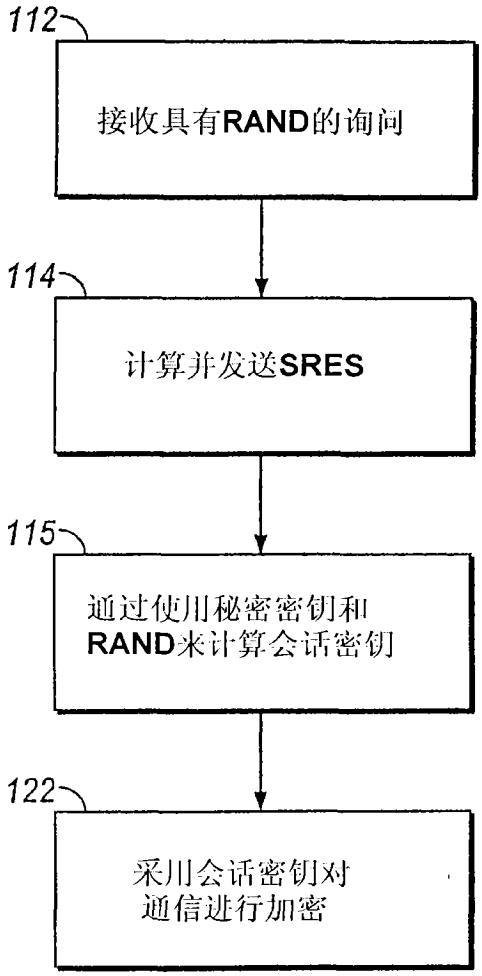

112
接收具有RAND的询问
114
计算并发送SRES
115
通过使用秘密密钥和RAND来计算会话密钥
122
采用会话密钥对通信进行加密

图 2

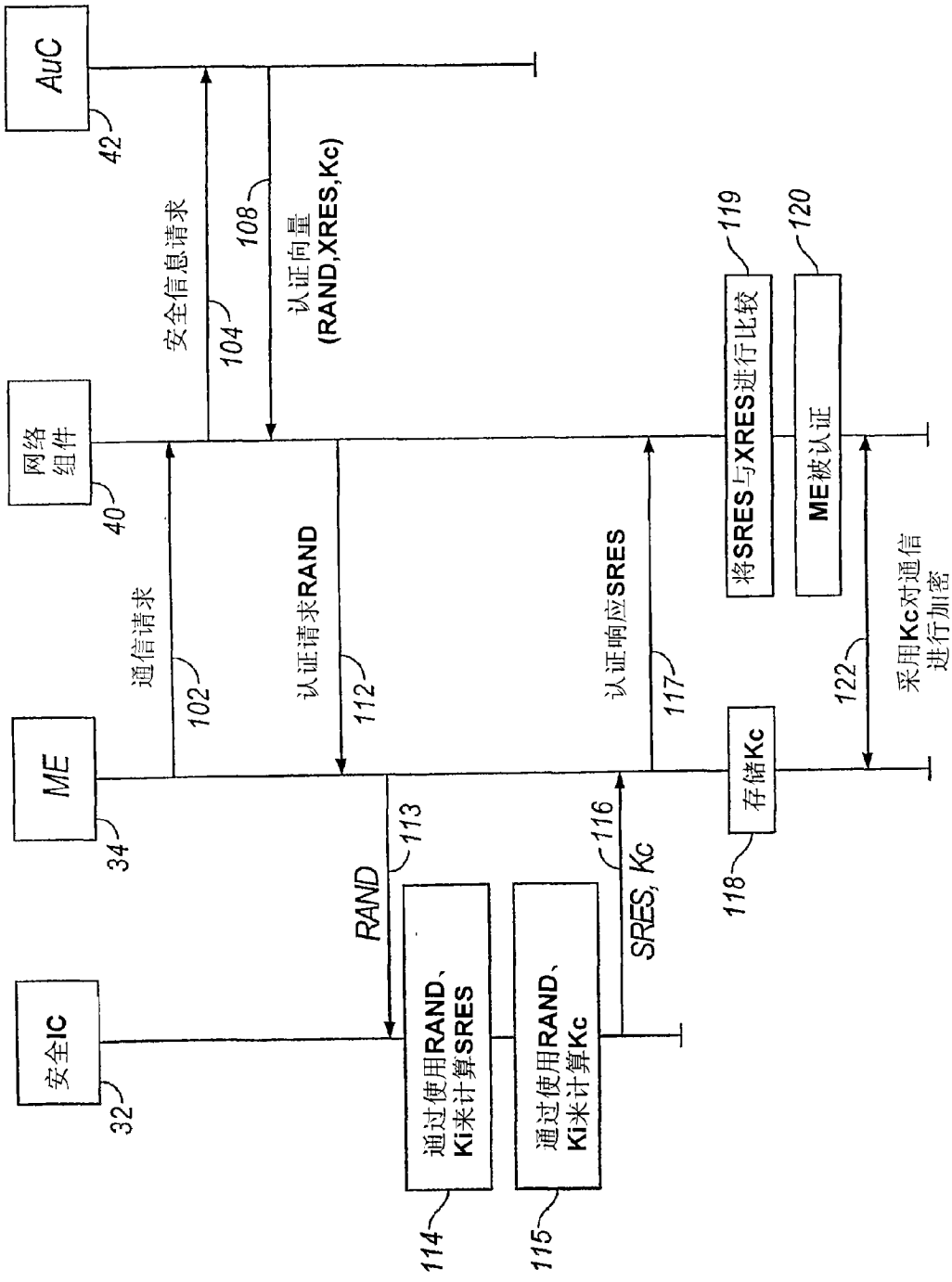

AuC
42
网络组件
40
ME
34
安全IC
32
安全信息请求
104
108
认证向量
(RAND,XRES,Kc)
通信请求
102
认证请求RAND
112
RAND
113
通过使用RAND、Ki来计算SRES
114
通过使用RAND、Ki来计算Kc
115
SRES, Kc
116
认证响应SRES
117
存储Kc
118
将SRES与XRES进行比较
119
ME被认证
120
122
采用Kc对通信进行加密

图3

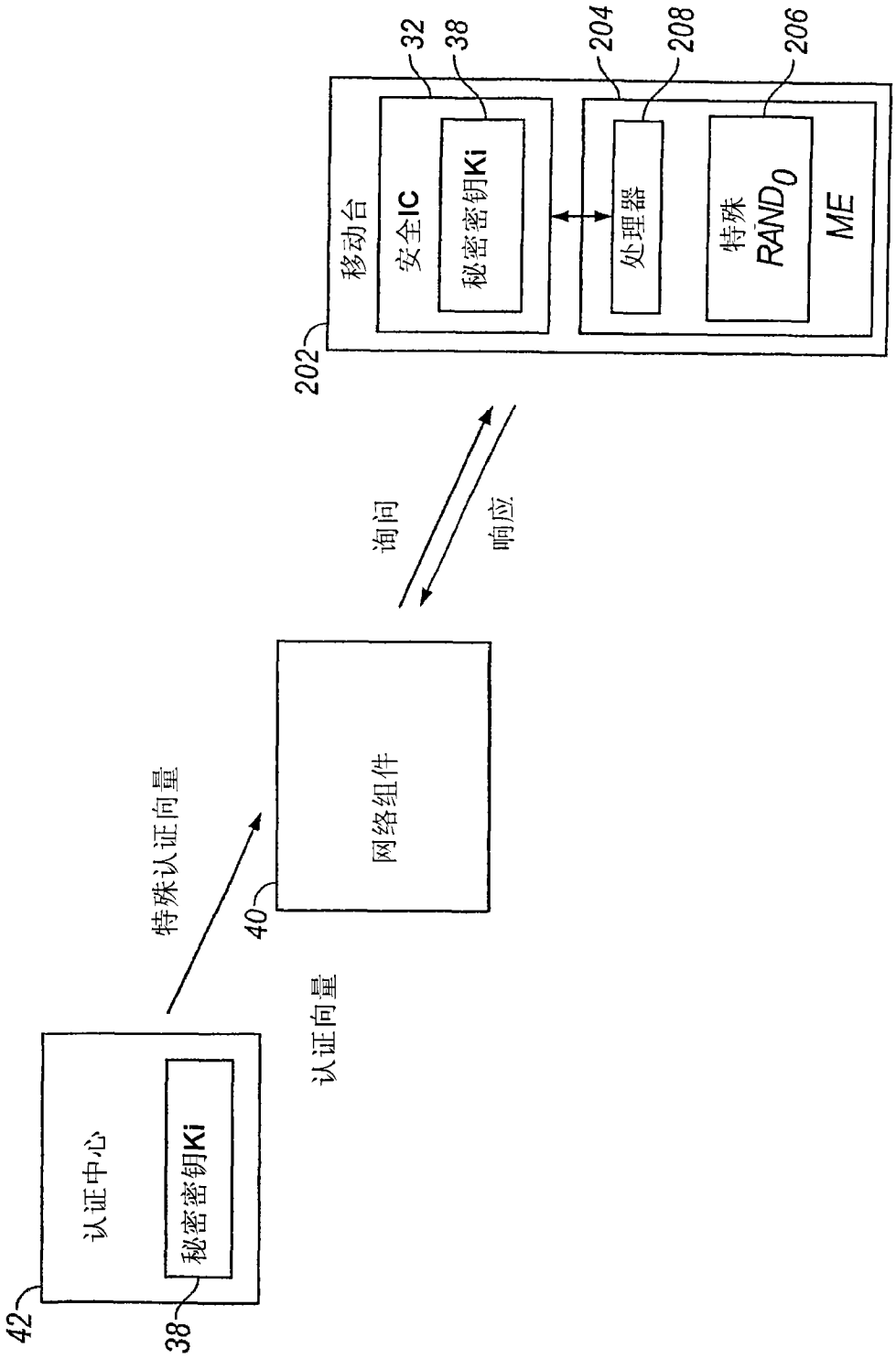

移动台
安全IC
秘密密钥Ki
处理器
特殊
$RAND_0$
ME
32
38
204
208
206
202
询问
响应
网络组件
40
特殊认证向量
认证向量
认证中心
秘密密钥Ki
42
38

图4

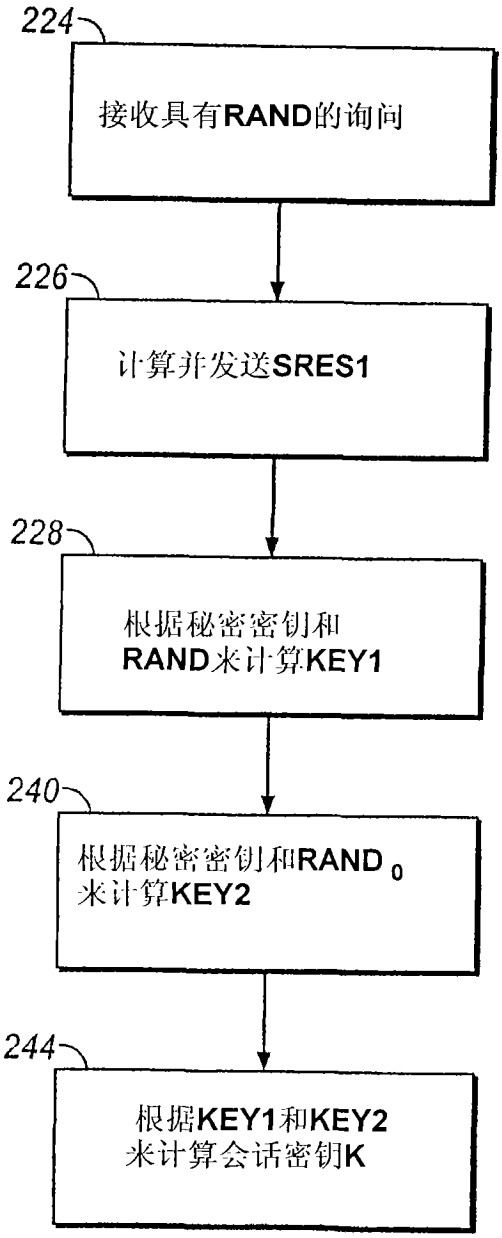

224
接收具有RAND的询问
226
计算并发送SRES1
228
根据秘密密钥和
RAND来计算KEY1
240
根据秘密密钥和RAND 0
来计算KEY2
244
根据KEY1和KEY2
来计算会话密钥K

图 5

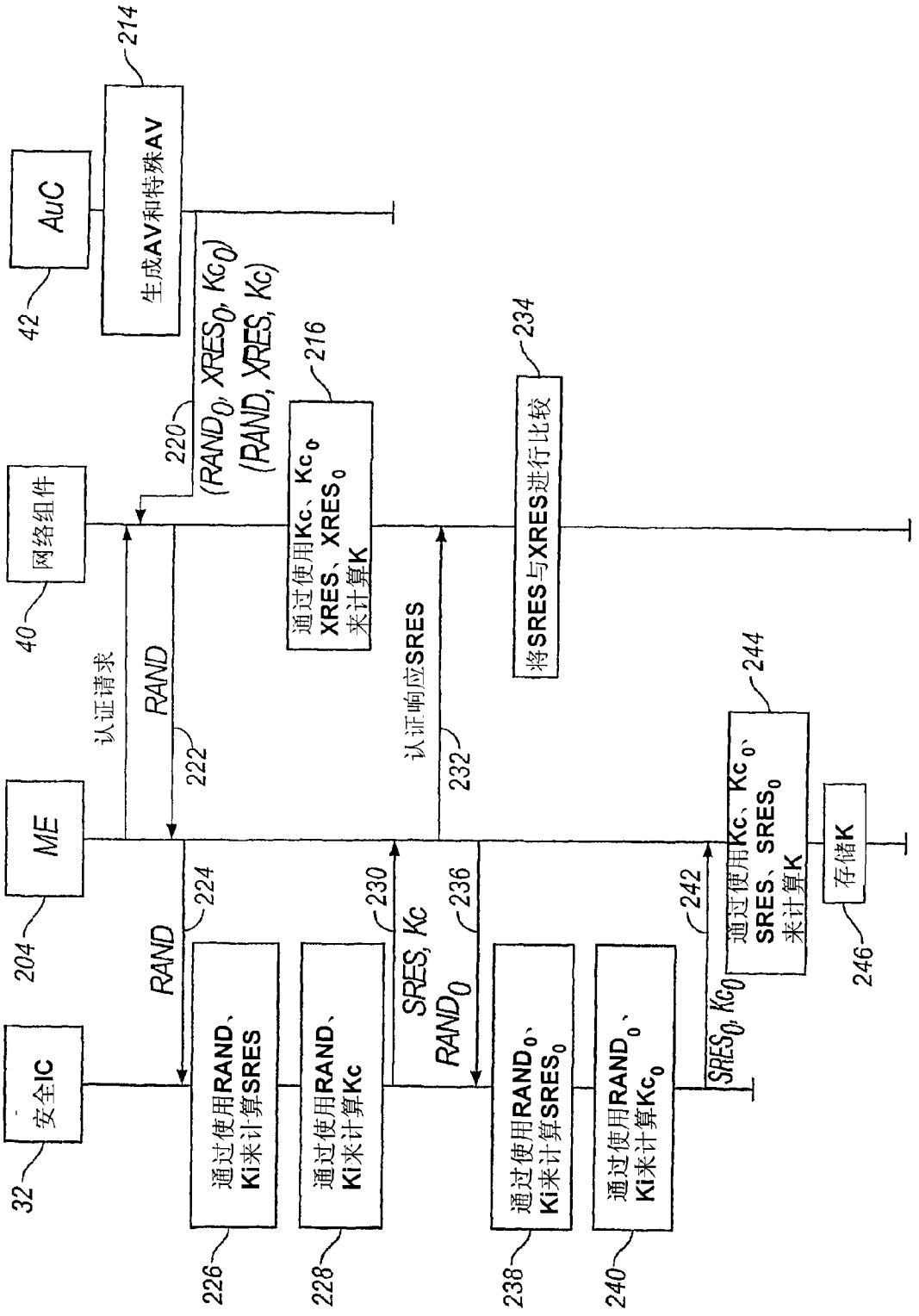

AuC
42
214
生成AV和特殊AV
网络组件
40
220
(RAND0, XRES0, Kc0)
(RAND, XRES, Kc)
216
通过使用Kc、Kc0、XRES、XRES0来计算K
234
将SRES与XRES进行比较
ME
204
认证请求
RAND
222
认证响应SRES
232
安全IC
32
RAND
224
通过使用RAND、Ki来计算SRES
226
通过使用RAND、Ki来计算Kc
228
SRES, Kc
RAND0
230
236
通过使用RAND0、Ki来计算SRES0
238
通过使用RAND0、Ki来计算Kc0
240
SRES0, Kc0
242
通过使用Kc、Kc0、SRES、SRES0来计算K
244
存储K
246

图6