(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 106465108 A
(43)申请公布日 2017.02.22

(21)申请号 201480078953.8
(22)申请日 2014.05.20
(85)PCT国际申请进入国家阶段日
2016.11.18
(86)PCT国际申请的申请数据
PCT/FI2014/050383 2014.05.20
(87)PCT国际申请的公布数据
WO2015/177398 EN 2015.11.26
(71)申请人 诺基亚技术有限公司
地址 芬兰埃斯波
(72)发明人 H·贝吉乌斯 S·霍尔特曼斯
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 葛荆 杨晓光
(51)Int.Cl.
H04W 12/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

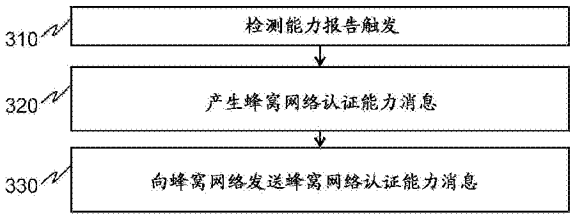
权利要求书5页 说明书8页 附图2页

(54)发明名称

蜂窝网络认证控制

(57)摘要

蜂窝诊断检测任何能力报告触发，并响应于这样的确定而产生蜂窝网络认证能力消息，其指示可用于终端的蜂窝网络认证能力；以及向蜂窝网络传送蜂窝网络认证能力消息。蜂窝网络从蜂窝终端接收网络认证能力消息，基于由网络认证能力消息指示的能力选择蜂窝认证算法；以及使用所选择的蜂窝认证算法执行与蜂窝终端的蜂窝认证。



CN 106465108 A

1.一种蜂窝终端中的方法,包括:

检测任何能力报告触发,以及响应于这样的确定:

产生蜂窝网络认证能力消息,其指示能够用于所述终端的蜂窝网络认证能力;以及

向所述蜂窝网络传送所述蜂窝网络认证能力消息。

2.如权利要求1所述的方法,其中以下事件是能力报告触发:

所述蜂窝终端将要发送下述中的一个或多个:附着请求消息;跟踪区域更新请求;以及路由区域更新请求。

3.如权利要求1或2所述的方法,包括:从所述蜂窝网络接收对认证能力的能力请求消息。

4.如前述权利要求中任一项所述的方法,其中所述能力请求消息的接收形成能力报告触发。

5.如前述权利要求中任一项所述的方法,其中所述蜂窝终端包括安全实体。

6.如权利要求5所述的方法,其中所述安全实体包括安全元件。

7.如权利要求6所述的方法,其中所述安全元件是可移除的、或者被嵌入或集成在现有处理器架构中。

8.如权利要求5至7中任一项所述的方法,其中所述安全实体包括用户身份模块应用。

9.如权利要求5至8中任一项所述的方法,其中所述蜂窝终端包括用户设备。

10.如权利要求9所述的方法,其中所述用户设备配置成通过无线电接口与基站进行通信。

11.如权利要求9或10所述的方法,其中所述用户设备选自:移动终端;膝上型计算机;车辆;汽车;汽车钥匙;便携式设备;手持电子设备;以及具有蜂窝无线电能力的单功能或多功能设备。

12.如权利要求5至11中任一项所述的方法,其中所述安全实体配置成计算用于蜂窝认证的认证密钥管理。

13.如权利要求5至12中任一项所述的方法,其中所述安全实体配置成形成所述能力消息的内容。

14.如权利要求13所述的方法,其中所述安全实体配置成接收对所述能力消息的内容的请求,并响应地产生所述能力消息的内容。

15.如权利要求13或14所述的方法,其中所述安全实体配置成接收认证请求,并响应地产生所述能力消息的内容。

16.如权利要求5至15中任一项所述的方法,其中所述安全实体是基于软件的实体。

17.如权利要求5至16中任一项所述的方法,其中所述安全实体包括处理器,所述处理器配置成独立于所述蜂窝终端的处理器进行操作。

18.如权利要求5至17中任一项所述的方法,其中所述安全实体被包含在集成电路中。

19.如权利要求5至18中任一项所述的方法,其中所述安全实体被包含在下述中:嵌入式通用集成电路卡;通用集成电路卡;片上系统;受信任平台模块;受信任计算模块;受信任元件;或者作为基带芯片的一部分的虚拟安全元件。

20.如前述权利要求中任一项所述的方法,其中所述蜂窝终端包括处理器,所述处理器配置成控制所述蜂窝终端的操作。

21.如权利要求20所述的方法，其中所述蜂窝终端的处理器配置成在非接入层中执行认证相关通信。

22.如权利要求5至21中任一项所述的方法，其中所述蜂窝终端配置成接收更新命令、并响应地更新所述安全实体。

23.如权利要求22所述的方法，其中所述蜂窝终端配置成更新所述安全实体，以支持早先不支持的蜂窝认证算法。

24.如前述权利要求中任一项所述的方法，其中所述能力消息被包含在由所述蜂窝终端针对所述蜂窝网络产生的另一个蜂窝网络认证消息内。

25.如前述权利要求中任一项所述的方法，其中使用认证令牌中的认证管理字段的一组位来传递所述能力消息。

26.如前述权利要求中任一项所述的方法，其中所述能力消息被包含在认证失败消息内。

27.如前述权利要求中任一项所述的方法，其中所述能力消息被包含在认证响应消息内。

28.如前述权利要求中任一项所述的方法，其中所述蜂窝终端配置成支持用于所述蜂窝认证的多个密码算法中的任何一个或多个。

29.如前述权利要求中任一项所述的方法，其中所述密码算法选自：MILENAGE；128位TUAK；和256位TUAK。

30.如前述权利要求中任一项所述的方法，其中所述认证能力消息包括所述蜂窝终端是否支持MILENAGE、128位TUAK、和256位TUAK中的任何一个或多个的指示。

31.一种蜂窝网络中的方法，包括：

从蜂窝终端接收蜂窝网络认证能力消息；

基于由所述网络认证能力消息指示的能力，选择蜂窝认证算法；以及

使用所选择的蜂窝认证算法，执行与所述蜂窝终端的蜂窝认证。

32.如权利要求31所述的方法，包括维护用户数据库。

33.如权利要求31或32所述的方法，其中基于所述网络认证消息来更新所述用户数据库。

34.如权利要求31至33中任一项所述的方法，其中所述用户数据库是归属位置寄存器。

35.如权利要求31至34中任一项所述的方法，其中所述蜂窝网络配置成从非介入层接收所述网络认证能力消息。

36.如权利要求31至35中任一项所述的方法，其中所述蜂窝网络配置成检测是否应该更新所述蜂窝终端的密码能力。

37.如权利要求31至36中任一项所述的方法，其中所述蜂窝网络配置成，如果所述蜂窝终端不能够使用其应该支持的密码算法进行操作、并且针对该密码算法存在与所述蜂窝终端兼容的更新，则检测出所述蜂窝终端的密码能力应该被更新。

38.如权利要求31至37中任一项所述的方法，其中所述蜂窝网络配置成向所述蜂窝终端发送更新命令，以促使所述安全实体的更新。

39.如权利要求31至38中任一项所述的方法，其中所述蜂窝网络配置成在更新所述蜂窝终端的密码能力时更新所述用户数据库。

40.如权利要求31至39中任一项所述的方法，其中所述能力消息被包含在由所述蜂窝终端针对所述蜂窝网络产生的另一个蜂窝网络认证消息内。

41.如权利要求31至40中任一项所述的方法，其中使用认证令牌中的认证管理字段的一组位来传递所述能力消息。

42.如权利要求41所述的方法，其中所述认证令牌包括128位、192位、256位或320位。

43.如权利要求41至42中任一项所述的方法，其中所述认证令牌由128位、192位、256位或320位组成。

44.如权利要求43所述的方法，其中在所述认证令牌多于256位的情况下，丢弃超出的位。

45.如权利要求41至44中任一项所述的方法，其中所述认证令牌包括序列号。

46.如权利要求45所述的方法，其中所述序列号由48位组成。

47.如权利要求41至46中任一项所述的方法，其中所述认证令牌包括匿名密钥。

48.如权利要求47所述的方法，其中所述匿名密钥由48位组成。

49.如权利要求41至48中任一项所述的方法，其中所述认证令牌包括认证管理字段。

50.如权利要求49所述的方法，其中所述认证管理字段由16位组成。

51.如权利要求49或50所述的方法，其中所述认证管理字段包括7个备用位。

52.如权利要求51所述的方法，其中所述备用位用于指示密码适配信息。

53.如权利要求52所述的方法，其中所述密码适配信息包括不同密码参数的长度。

54.如权利要求41至53中任一项所述的方法，其中所述认证令牌包括挑战。

55.如权利要求41至54中任一项所述的方法，其中所述挑战由128位组成。

56.如权利要求31至55中任一项所述的方法，其中所述蜂窝认证采用加密密钥。

57.如权利要求56所述的方法，其中所述加密密钥由64位、128位、或256位组成。

58.如权利要求31至57中任一项所述的方法，其中所述蜂窝认证采用完整性密钥IK。

59.如权利要求58所述的方法，其中所述完整性密钥由64位、128位或256位组成。

60.如权利要求31至59中任一项所述的方法，其中所述蜂窝认证采用响应参数。

61.如权利要求60所述的方法，其中所述响应参数由32位、64位、128位或256位组成。

62.如权利要求31至61中任一项所述的方法，其中所述能力消息被包含在认证失败消息内。

63.如权利要求31至62中任一项所述的方法，其中所述能力消息被包含在认证响应消息内。

64.如权利要求31至63中任一项所述的方法，其中所述蜂窝网络配置成支持用于所述蜂窝认证的多个密码算法中的任何一个或多个。

65.如权利要求64所述的方法，其中所述密码算法选自:MILENAGE;128位TUAK;和256位TUAK。

66.如权利要求31至65中任一项所述的方法，其中所述认证能力消息包括所述蜂窝终端是否支持MILENAGE、128位TUAK、和256位TUAK中的任何一个或多个的指示。

67.一种过程，包括如权利要求1至30中任一项所述的方法、以及如权利要求31至66中任一项所述的方法。

68.一种装置，包括：

用于检测任何能力报告触发、以及响应于这样的确定而执行以下操作的模块：

产生蜂窝网络认证能力消息，其指示能够用于所述终端的蜂窝网络认证能力；以及

向所述蜂窝网络传送所述蜂窝网络认证能力消息。

69.如权利要求68所述的装置，包括用于执行如权利要求2至30中任一项所述的方法的模块。

70.一种装置，包括：

处理器，其配置成：

检测任何能力报告触发，以及响应于这样的确定：

产生蜂窝网络认证能力消息，其指示能够用于所述终端的蜂窝网络认证能力；以及

向所述蜂窝网络传送所述蜂窝网络认证能力消息。

71.如权利要求70所述的装置，还包括：包含可执行指令的存储器，所述可执行指令在由所述处理器执行时使所述装置执行如权利要求1至30中任一项所述的方法。

72.一种装置，包括：

至少一个处理器；以及

包括计算机程序代码的至少一个存储器，

所述至少一个存储器和所述计算机程序代码配置成与所述至少一个处理器一起使所述装置至少执行以下操作：

检测任何能力报告触发，以及响应于这样的确定：

产生蜂窝网络认证能力消息，其指示能够用于所述终端的蜂窝网络认证能力；以及

向所述蜂窝网络传送所述蜂窝网络认证能力消息。

73.如权利要求72所述的装置，其中所述至少一个存储器和所述计算机程序代码配置成与所述至少一个处理器一起使所述装置执行如权利要求2至30中任一项所述的方法。

74.一种计算机程序，包括：

当所述计算机程序在处理器上被运行时，用于检测任何能力报告触发、以及响应于这样的确定而执行以下操作的代码：

产生蜂窝网络认证能力消息，其指示能够用于所述终端的蜂窝网络认证能力；以及

向所述蜂窝网络传送所述蜂窝网络认证能力消息。

75.如权利要求74所述的计算机程序，还包括用于使得执行如权利要求2至30中任一项所述的方法的代码。

76.一种计算机可读非暂时性存储介质，包括如权利要求74所述的计算机程序。

77.一种装置，包括：

用于检测任何能力报告触发、以及响应于这样的确定而执行以下操作的模块：

产生蜂窝网络认证能力消息，其指示能够用于所述终端的蜂窝网络认证能力；以及

向所述蜂窝网络传送所述蜂窝网络认证能力消息。

78.如权利要求68所述的装置，包括用于执行如权利要求2至30中任一项所述的方法的模块。

79.一种装置，包括：

处理器，其配置成：

从蜂窝终端接收蜂窝网络认证能力消息；

基于由所述蜂窝认证能力消息指示的能力，选择蜂窝认证算法；以及

使用所选择的蜂窝认证算法，执行与所述蜂窝终端的蜂窝认证。

80.如权利要求79所述的装置，还包括包含可执行指令的存储器，所述可执行指令由所述处理器执行时使所述装置执行权利要求31至66中任一项所述的方法。

81.一种装置，包括：

至少一个处理器；以及

至少一个存储器，其包括计算机程序代码

所述至少一个存储器和所述计算机程序代码配置成与所述至少一个处理器一起使所述装置执行至少以下项：

从蜂窝终端接收蜂窝网络认证能力消息；

基于由所述网络认证能力消息指示的能力，选择蜂窝认证算法；以及

使用所选择的蜂窝认证算法，执行与所述蜂窝终端的蜂窝认证。

82.如权利要求81所述的装置，其中所述至少一个存储器和所述计算机程序代码配置成与所述至少一个处理器一起使所述装置执行如权利要求32至66中任一项所述的方法。

83.一种系统，包括如权利要求68至73中任一项所述的装置、以及如权利要求77至82中任一项所述的装置。

84.一种计算机程序，包括：

当所述计算机程序在处理器上被运行时，

用于从蜂窝终端接收蜂窝网络认证能力消息的代码；

用于基于由所述网络认证能力消息指示的能力，选择蜂窝认证算法的代码；以及

用于使用所选择的蜂窝认证算法，执行与所述蜂窝终端的蜂窝认证的代码。

85.如权利要求84所述的计算机程序，还包括用于使得执行如权利要求32至66中任一项所述的方法的代码。

86.一种计算机可读非暂时性存储介质，包括如权利要求85所述的计算机程序。

蜂窝网络认证控制

技术领域

[0001] 本申请一般涉及蜂窝网络认证控制。

背景技术

[0002] 本部分示出了有用的背景信息，而并未承认本文描述的任何技术是当前发展水平的代表。

[0003] 蜂窝电信网络或蜂窝网络在现代社会中是普遍存在的。作为必要条件，需要对它们进行保护以避免电话帐单欺骗并且保护通信以防止非法拦截私人呼叫和消息。为此，现代蜂窝网络的电信运营商利用通常依赖于数字信号处理的大量不同技术来保护他们的用户。

[0004] 为了使蜂窝终端能够开始通信，终端需要在网络附着过程中附着到网络。在网络注册过程中，蜂窝终端通常使用用户身份模块(SIM)来交换信号以认证其自身(或更准确地，其签约)。在网络附着或注册过程中，蜂窝终端从网络和SIM获得接入信息诸如会话密钥，蜂窝终端可随后在蜂窝网络中利用该会话密钥进行通信。接入信息通常会变化以防止可能的非法拦截者重新使用该接入信息。

[0005] 加密是也用在其他类型的数字蜂窝系统中的基本工具。GSM已经实现了加密以实际防止非法拦截。计算机技术的发展随后已经使旧的加密技术更加脆弱，但也帮助增强了蜂窝系统中使用的安全技术。例如，宽带CDMA(W-CDMA)被设计用于通过使得网络也能够向蜂窝终端认证自身来实现更强的安全性。在W-CDMA中，用户身份由运行通用用户身份模块(USIM)的通用集成电路卡(UICC)提供。USIM基于存储在UICC上的共享秘密、从网络接收的挑战和重放攻击防止代码、以及比在GSM中使用的密码算法增强的密码算法，来产生例如会话密钥。在W-CDMA中也比GSM增强了认证信令，例如以防止某些中间人攻击。

[0006] 在开发用于保护蜂窝系统中的通信的安全方法的同时，对开发蜂窝终端的安全结构的需求也在不断增长。目前，大多数蜂窝终端包含被称为SIM槽的身份模块槽，在该身份模块槽中，用户可以放置和替换身份模块卡(例如UICC)。还存在着朝向基于软件的身份模块的发展，所述基于软件的身份模块在物理上不可替换，并且另外能够实现签约从一个运营商到另一个运营商的空中改变。嵌入式形状因素防止身份模块从蜂窝终端被盗。具有嵌入式安全模块的终端常常是无人照管的机器。这样的软件身份模块例如对于内置车辆通信系统可能非常有用，使得它们的紧急报告能力和可能的防盗控制系统不会由于移除SIM而被容易地停用。

[0007] 尽管对于安全性是必要的，但是认证信令不幸地延迟了网络附着过程的完成。此外，发明人现在已经认识到，在蜂窝终端设备、网络配置和加密认证协议的一些特定组合中，蜂窝终端可能进入永久性故障回路中，使得其用户根本不能建立电信连接。

发明内容

[0008] 本发明的示例的各个方面在权利要求书中阐述。

[0009] 根据本发明的第一示例方面，提供了一种蜂窝终端中的方法，包括：

[0010] 检测任何能力报告触发，以及响应于这样的确定：

[0011] 产生蜂窝网络认证能力消息，其指示可用于所述终端的蜂窝网络认证能力；以及

[0012] 向所述蜂窝网络传送所述蜂窝网络认证能力消息。

[0013] 以下事件可以是能力报告触发：蜂窝终端将要发送下述中的一个或多个：附着请求消息；跟踪区域更新请求；以及路由区域更新请求。

[0014] 所述方法可包括从蜂窝网络接收对认证能力的能力请求消息。能力请求消息的接收可形成能力报告触发。

[0015] 蜂窝终端可包括安全实体。安全实体可包括安全元件。安全元件可包括用户身份模块应用。蜂窝终端可包括用户设备。用户设备可配置成通过无线电接口与基站进行通信。安全实体可配置成计算用于蜂窝认证的认证密钥管理。

[0016] 用户设备可选自：移动终端；膝上型计算机；车辆；汽车；汽车钥匙；便携式设备；手持电子设备；以及具有蜂窝无线电能力的单功能或多功能设备。安全实体可以是可移除的或者被嵌入或集成在现有处理器架构(例如，基带电路、主处理器、中央处理单元、和/或主控制单元)中。

[0017] 安全实体可配置成形成能力消息的内容。安全实体可配置成接收对能力消息的内容的请求，并响应地产生能力消息的内容。安全实体可配置成接收认证请求、并响应地产生能力消息的内容。

[0018] 蜂窝终端可包括处理器，其配置成控制蜂窝终端的操作。

[0019] 安全实体可以是基于软件的实体。安全实体可包括处理器，其配置成独立于蜂窝终端的处理器进行操作。安全实体可被包含在集成电路中。安全实体可被包含在通用集成电路卡UICC或SoC(片上系统)、TMP(受信任平台模块)、TCM(受信任计算模块)、受信任元件、或者作为基带芯片的一部分的虚拟安全元件中。安全实体可被包含在嵌入式通用集成电路卡eUICC中。

[0020] 蜂窝终端的处理器可配置成在非接入层NAS层中执行认证相关通信。

[0021] 蜂窝终端可配置成接收更新命令、并响应地更新安全实体。蜂窝终端可配置成更新安全实体以支持早先不支持的蜂窝认证算法。

[0022] 能力消息可被包含在由蜂窝终端针对蜂窝网络产生的另一个蜂窝网络认证消息内。可使用认证令牌AUTN中的认证管理字段AMF的一组位来传递能力消息。

[0023] 能力消息可被包含在认证失败消息内。

[0024] 能力消息可被包含在认证响应消息内。

[0025] 蜂窝终端可配置成支持用于蜂窝认证的多个密码算法中的任何一个或多个。

[0026] 密码算法可选自：MILENAGE；128位TUAK；和256位TUAK。TUAK可指代符合3GPP TS 35.231 v.12.0.1的算法集。TUAK可配置成采用AES密码。TUAK可基于Keccak置换。

[0027] 认证能力消息可包括蜂窝终端是否支持MILENAGE、128位TUAK、和256位TUAK中的任何一个或多个的指示。

[0028] 根据本发明的第二示例方面，提供了一种蜂窝网络中的方法，包括：

[0029] 从蜂窝终端接收蜂窝网络认证能力消息；

[0030] 基于由所述网络认证能力消息指示的能力，选择蜂窝认证算法；以及

[0031] 使用所选择的蜂窝认证算法，执行与所述蜂窝终端的蜂窝认证。

[0032] 所述方法可包括维护用户数据库。可基于网络认证消息更新用户数据库。用户数据库可以是归属位置寄存器。

[0033] 蜂窝网络可配置成从非接入层NAS层接收网络认证能力消息。

[0034] 蜂窝网络可配置成检测是否应该更新蜂窝终端的密码能力。蜂窝网络可配置成，如果蜂窝终端不能够使用其应该支持的密码算法进行操作、并且针对该密码算法存在与蜂窝终端兼容的更新，则检测出蜂窝终端的密码能力应该被更新。蜂窝网络可配置成向蜂窝终端发送更新命令，以促使安全实体的更新。蜂窝网络可配置成在更新蜂窝终端的密码能力时更新用户数据库。

[0035] 能力消息可被包含在由蜂窝终端针对蜂窝网络产生的另一个蜂窝网络认证消息内。可使用认证令牌AUTN中的认证管理字段AMF的一组位来传递能力消息。

[0036] 认证令牌可包括128位、192位、256位或320位。认证令牌可由128位、192位、256位或320位组成。在认证令牌多于256位的情况下，可丢弃超出的位。

[0037] 认证令牌可包括序列号SQN。序列号可由48位组成。

[0038] 认证令牌可包括匿名密钥AK。匿名密钥可由48位组成。

[0039] 认证令牌可包括认证管理字段AMF。认证管理字段可由16位组成。认证管理字段可包括7个备用位。备用位可用于指示密码适配信息。密码适配信息可包括不同密码参数的长度。

[0040] 认证令牌可包括挑战RAND。挑战可由128位组成。

[0041] 蜂窝认证可采用加密密钥CK。加密密钥可由64位、128位或256位组成。

[0042] 蜂窝认证可采用完整性密钥IK。完整性密钥可由64位、128位或256位组成。

[0043] 蜂窝认证可采用响应参数RES。响应参数可由32位、64位、128位或256位组成。

[0044] 能力消息可被包含在认证失败消息内。

[0045] 能力消息可被包含在认证响应消息内。

[0046] 蜂窝网络可配置成支持用于蜂窝认证的多个密码算法中的任何一个或多个。

[0047] 密码算法可选自：MILENAGE；128位TUAK；和256位TUAK。TUAK可指代符合3GPP TS 35.231 v.12.0.1的算法集。TUAK可配置成采用AES密码。TUAK可基于Keccak置换。

[0048] 认证能力消息可包括蜂窝终端是否支持MILENAGE、128位TUAK、和256位TUAK中的任何一个或多个的指示。

[0049] 根据本发明的第三示例方面，提供了一种装置，包括用于执行第一或第二示例方面的方法的模块。

[0050] 根据第四示例方面，提供了一种装置，包括配置成执行第一或第二示例方面的方法的处理器。

[0051] 根据第五示例方面，提供了一种装置，包括：至少一个处理器以及包括计算机程序代码的至少一个存储器；所述至少一个存储器和所述计算机程序代码配置成与所述至少一个处理器一起使所述装置至少执行第一或第二示例方面的方法。

[0052] 根据第六示例方面，提供了一种计算机程序，包括用于执行第一或第二示例方面的方法的代码。

[0053] 根据第七示例方面，提供了一种计算机可读存储介质，包括第六示例方面的计算

机程序。

[0054] 任何前述存储介质可以包括数字数据存储装置，诸如数据盘或磁盘、光学存储装置、磁存储装置、全息存储装置、光磁存储装置、相变存储器、阻变随机存取存储器、磁随机存取存储器、固体电解质存储器、铁电随机存取存储器、有机存储器或聚合物存储器。存储介质可以被形成到除了储存存储器之外没有其他实质功能的设备中，或者其可以被形成为具有其他功能的设备的一部分，包括但不限于计算机的存储器、芯片集、以及电子设备的子组件。

[0055] 前面已经示出了本发明的不同非约束性示例方面和实施例。前文中的实施例仅仅用于解释可以在本发明的实现中利用的所选方面或步骤。可以仅参考本发明的某些示例方面来呈现一些实施例。应当理解的是，相应的实施例也可以应用于其他示例方面。

附图说明

[0056] 为了更完整地理解本发明的示例实施例，现在结合附图参考下面的描述，在附图中：

[0057] 图1示出示例实施例的系统的架构图；

[0058] 图2示出示例实施例的过程的流程图；

[0059] 图3示出根据本发明的示例实施例的过程的流程图；

[0060] 图4示出示例实施例的装置的框图；以及

[0061] 图5示出示例实施例的装置的框图。

具体实施方式

[0062] 通过参考附图的图1至4理解本发明的示例实施例及其潜在优点。在本文档中，相同的附图标记表示相同的部件或步骤。

[0063] 图1是示例实施例的系统的架构图。蜂窝终端100被绘制为具有用户设备110和安全实体诸如安全元件。安全实体可以包含USIM 120。在示例实施例中，USIM是软件实现的安全元件上的应用。在示例实施例中，安全实体是基于软件的实体。在示例实施例中，安全实体包括配置成独立于蜂窝终端的处理器进行操作的处理器。在示例实施例中，安全实体被包含在集成电路中。在示例实施例中，安全实体被包含在通用集成电路卡UICC或片上系统(SoC)、受信任平台模块(TPM)、受信任计算模块(TCM)、受信任元件、或者作为基带芯片或主处理器的一部分的虚拟安全元件中。在示例实施例中，安全实体被包含在嵌入式通用集成电路卡(eUICC)中。

[0064] 系统还包括蜂窝电信网络200，其包括E-UTRAN或eNB 210、移动性管理实体MME 220、归属用户服务器HSS 230(例如，归属位置寄存器HLR、认证中心AuC)、服务网关240、服务网关支持节点SGSN 250、通用陆地无线电接入网UTRAN 260和GSM EDGE无线电接入网GERAN 270。

[0065] 图2示出示例实施例的过程的流程图。在步骤21中，蜂窝终端经由eNB 210向MME 220发送非接入层(NAS)附着请求或网络注册请求。MME 220从HSS 230请求22认证数据(例如，认证五元组)，并且响应地接收23具有所请求的认证数据的认证数据响应。MME 220然后向终端100发送24NAS认证请求，如果终端100能够解码NAS认证请求并产生NAS认证响应，则

终端100利用NAS认证响应进行答复25。为此，终端100必须支持由MME使用的认证算法，并且拥有为HSS 230和终端100已知的共享秘密(shared secret)。如果终端100未能解码NAS认证请求，则终端100利用NAS认证失败进行答复25'。

[0066] 在成功解码NAS认证请求以及响应性的NAS认证响应之后，MME向终端100发送26NAS安全模式完成消息，并且终端100利用相应的NAS安全模式完成消息进行答复27。在另一个示例实施例中，NAS安全模式完成和NAS安全模式完成答复中的任一个或两者被省略或者由一个或多个其他信号或消息替代。

[0067] 图2的各种消息以及它们的处理可以用各种不同的方式实现。

[0068] 在示例实施例中，图2的过程开始于向蜂窝网络200要求认证过程触发的另一个请求(诸如跟踪区域更新请求或路由区域请求)，而不是网络注册请求。

[0069] 在示例实施例中，认证请求消息24包括从一组多个密码算法中选择的密码算法的指示。在示例实施例中，密码算法选自:MILENAGE;128位TUAK;以及256位TUAK。TUAK可指代符合3GPP TS 35.231 v.12.0.1的算法集。TUAK可配置成采用AES密码。TUAK可以基于Keccak置换。

[0070] 图3示出根据本发明的示例实施例的过程的流程图。所述过程包括：

[0071] 检测310任何能力报告触发并响应于这样的确定：

[0072] 产生320指示可用于终端的蜂窝网络认证能力的蜂窝网络认证能力消息;以及

[0073] 向蜂窝网络传送330蜂窝网络认证能力消息。

[0074] 在示例实施例中，以下事件是能力报告触发:蜂窝终端将要发送下述中的一个或多个:附着请求消息;跟踪区域更新请求;以及路由区域更新请求。

[0075] 在示例实施例中，所述过程包括从蜂窝网络接收对认证能力的能力请求消息。能力请求消息的接收可以形成能力报告触发。

[0076] 在示例实施例中，安全实体配置成形成能力消息的内容。在示例实施例中，安全实体配置成接收对能力消息的内容的请求，并且响应地产生能力消息的内容。在示例实施例中，安全实体配置成接收认证请求并且相应地产生能力消息的内容。

[0077] 在示例实施例中，蜂窝终端的处理器配置成在非接入层NAS层中执行认证相关通信。

[0078] 在示例实施例中，蜂窝终端配置成接收更新命令并响应地更新安全实体。在示例实施例中，蜂窝终端配置成更新安全实体，以支持早先不支持的蜂窝认证算法。

[0079] 在示例实施例中，能力消息被包含在由蜂窝终端针对蜂窝网络产生的另一个蜂窝网络认证消息内。在示例实施例中，使用认证令牌AUTN中的认证管理字段AMF的一组位来传递能力消息。

[0080] 在示例实施例中，能力消息被包含在认证失败消息内。

[0081] 在示例实施例中，能力消息被包含在认证响应消息内。

[0082] 在示例实施例中，所选的密码算法采用加密密钥CK。加密密钥可由64位、128位或256位组成。

[0083] 在示例实施例中，所选的密码算法采用完整性密钥IK。完整性密钥可由64位、128位或256位组成。

[0084] 在示例实施例中，所选的密码算法采用响应参数RES。响应参数可由32位、64位、

128位或256位组成。

[0085] 在示例实施例中，认证请求消息24是扩展认证请求消息。在示例实施例中，扩展认证请求包括配置成使遗留终端忽略扩展认证请求消息的消息类型指示。

[0086] 在示例实施例中，扩展认证请求包括配置成容纳256位认证令牌AUTN的字段。

[0087] 在示例实施例中，认证请求消息24是更新的认证请求。在示例实施例中，更新的认证请求包括标识符，用于指示哪个密码算法正用于认证。在示例实施例中，标识符是除了正常认证请求中的那些之外的新字段。在示例实施例中，正常认证请求符合3GPP TS 24.301或3GPP TS 24.008。在示例实施例中，标识符被包含在认证管理字段AMF的一个或多个位中。

[0088] 在示例实施例中，认证请求消息24包括协议鉴别符。在示例实施例中，认证请求消息包括安全报头类型。在示例实施例中，认证请求消息包括非接入层密钥集标识符。在示例实施例中，认证请求消息包括备用的半个八位字节。在示例实施例中，认证请求消息包括挑战RAND(例如，演进分组系统EPS挑战)。在示例实施例中，认证请求消息包括认证令牌AUTN。在示例实施例中，认证令牌包括认证管理字段AMF。认证管理字段可以包括指示将被使用的TUAK的位长度的参数。

[0089] 在示例实施例中，更新的认证请求的消息类型与正常认证请求消息的消息类型匹配。在示例实施例中，更新的认证请求包括256位认证令牌字段。更新的认证请求可以仅当正在使用256位认证令牌时包括256位认证令牌字段。否则，更新的认证请求可以包括128位认证令牌字段。

[0090] 在示例实施例中，认证令牌包括128位、192位、256位或320位。在示例实施例中，认证令牌由128位、192位、256位或320位组成。在认证令牌多于256位的情况下，可以丢弃超出的位。

[0091] 在示例实施例中，认证令牌包括序列号SQN。在示例实施例中，序列号由48位组成。

[0092] 在示例实施例中，认证令牌包括匿名密钥AK。在示例实施例中，匿名密钥由48位组成。

[0093] 在示例实施例中，认证令牌包括认证管理字段AMF。在示例实施例中，认证管理字段由16位组成。在示例实施例中，认证管理字段包括7个备用位。在示例实施例中，备用位用于指示密码适配信息。在示例实施例中，密码适配信息包括不同密码参数的长度。

[0094] 在示例实施例中，认证令牌包括挑战RAND。在示例实施例中，挑战由128位组成。

[0095] 在示例实施例中，根据所选的密码算法、并且基于为蜂窝终端和蜂窝终端的网络运营商已知的共享秘密，来将认证请求消息24解码成经解码的认证请求。

[0096] 在示例实施例中，所述过程包括基于经解码的认证请求、共享秘密、和所选的密码算法，产生并加密认证响应消息25。

[0097] 在示例实施例中，认证响应消息25包括消息类型指示。在示例实施例中，消息类型指示将认证响应消息标识为扩展认证响应消息。在示例实施例中，消息类型指示与正常认证响应消息的消息类型指示匹配。在示例实施例中，正常认证响应消息的消息类型指示符合3GPP TS 24.301。

[0098] 在示例实施例中，扩展认证响应消息包括可变长度认证响应参数RES。在示例实施例中，认证响应参数所具有的长度选自下述中的一个或多个：32位、64位、128位或256位。

[0099] 在示例实施例中，与正常认证响应消息相比，认证响应消息25被提供有新的信息元素。在示例实施例中，新的信息元素配置成容纳128位或256位认证响应参数。

[0100] 在示例实施例中，认证响应消息25包括扩展认证响应参数字段，其配置成容纳128位或256位认证响应参数。

[0101] 在示例实施例中，认证响应消息25包括密码算法指示。

[0102] 图4示出根据示例实施例的装置400的示例框图。装置400包括存储器420，其包括易失性存储器430和非易失性存储器440，该非易失性存储器440配置成存储包括计算机程序代码450的计算机程序或软件。装置400还包括：至少一个处理器410，用于使用计算机程序代码450控制装置400的操作；以及输入/输出系统460，用于与其他实体或装置通信。因此，输入/输出系统460包括提供朝向其他实体和/或装置的通信接口的一个或多个通信单元或模块。在示例实施例中，处理器410配置成在易失性存储器430中运行程序代码450。在示例实施例中，装置400配置成充当MME 220。

[0103] 处理器410包括例如下述中的任何一个或多个：主控制单元(MCU)；微处理器；数字信号处理器(DSP)；专用集成电路(ASIC)；现场可编程门阵列；以及微控制器。

[0104] 图5示出根据示例实施例的装置500的示例框图。装置500包括存储器520，其包括易失性存储器530和非易失性存储器540，该非易失性存储器540配置成存储包括计算机程序代码550的计算机程序或软件。装置500还包括至少一个处理器510，用于使用计算机程序代码550控制装置500的操作。装置500还包括输入/输出系统560，用于与其他实体或装置通信。因此，输入/输出系统560包括提供朝向其他实体和/或装置的通信接口的一个或多个通信单元或模块。装置500还包括安全元件(SE)570，其包含一个或多个网络接入应用，诸如SIM(多个SIM)或USIM(多个USIM)。在示例实施例中，SE 570是由实现为软件的安全元件托管的应用。在另一个示例实施例中，安全元件570包括通用集成电路卡UICC。在示例实施例中，处理器510配置成在易失性存储器530中运行程序代码550。在示例实施例中，装置500配置成充当蜂窝终端100。

[0105] 处理器510包括例如下述中的任何一个或多个：主控制单元(MCU)；微处理器；数字信号处理器(DSP)；专用集成电路(ASIC)；现场可编程门阵列；以及微控制器。

[0106] 在不以任何方式限制下面出现的权利要求书的范围、解释或应用的情况下，本文公开的示例实施例中的一个或多个的技术效果是，可以允许蜂窝网络使用现有设备通过它们的认证特征发展到更大的程度，或者换句话说，现有设备的寿命可被增加和/或蜂窝网络的安全性可被增强。本文公开的示例实施例中的一个或多个的另一个技术效果在于，可以关于蜂窝认证过程避免或减轻可靠性问题。本文公开的示例实施例中的一个或多个的另一个技术效果在于，可以在现有蜂窝网络中作出很小的变化的情况下传送能力信息。例如，AUTN可由SQN、AK、AMF和MAC组成。序列号SQN(单独的实例)可被存储在用于所有用户的HLR/HSS中。在这样的情况下，向SQN添加位可能对HLR/HSS具有较大或甚至关键的影响。相反，AMF字段可以更好地适合用于承载认证能力信息的字段。AMF也可以比AK字段或MAC字段更好地适合于该功能，其中AK字段或MAC字段的改变可能对整个运营商网络造成严重和/或广泛的影响。

[0107] 本发明的实施例可以在软件、硬件、应用逻辑、或者软件、硬件和应用逻辑的组合中实现。在示例实施例中，应用逻辑、软件或指令集被保持在各种常规计算机可读介质中的

任一个上。在该文档的上下文中，“计算机可读介质”可以是任何非暂时性介质或装置，其可以包含、存储、传送、传播或传输由指令执行系统、装置或设备(诸如计算机)使用或与其结合使用的指令，其中计算机的一个示例在图4或5中被描述和描绘。计算机可读介质可以包括计算机可读存储介质，其可以是能够包含或存储由指令执行系统、装置或设备(诸如计算机)使用或与其结合使用的指令的任何介质或装置。

[0108] 如果需要，本文所讨论的不同功能可以按照不同的顺序执行和/或彼此同时执行。此外，如果需要，前述功能中的一个或多个可以是任选的或者可被组合。

[0109] 尽管在独立权利要求中阐述了本发明的各个方面，但是本发明的其他方面包括来自所述实施例和/或从属权利要求的特征与独立权利要求的特征的其他组合，而不仅仅是在权利要求中明确阐述的组合。

[0110] 在本文中还应注意的是，尽管前文描述了本发明的示例实施例，但是这些描述不应被视为具有限制性意义。相反，在不脱离如所附权利要求中限定的本发明的范围的情况下，可以作出若干变型和改型。

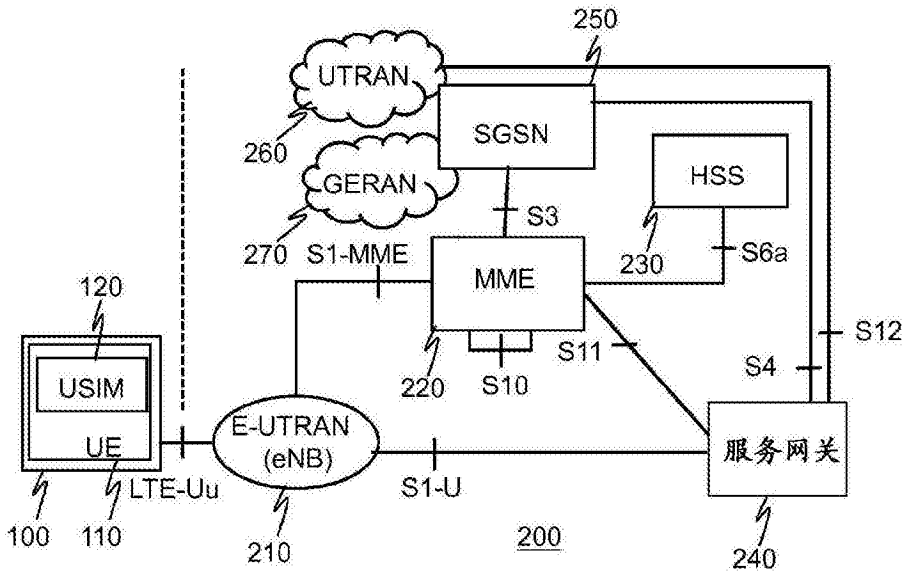

250
UTRAN
260
SGSN
GERAN
270
S1-MME
HSS
S3
230
S6a
MME
120
USIM
UE
220
S10
S11
S12
S4
E-UTRAN
(eNB)
服务网关
LTE-Uu
S1-U
100
110
210
200
240

图1

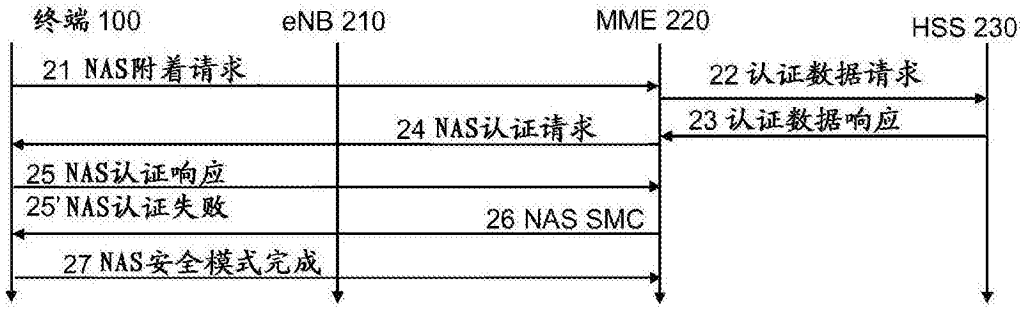

终端 100
eNB 210
MME 220
HSS 230
21 NAS附着请求
22 认证数据请求
23 认证数据响应
24 NAS认证请求
25 NAS认证响应
25' NAS认证失败
26 NAS SMC
27 NAS安全模式完成

图2

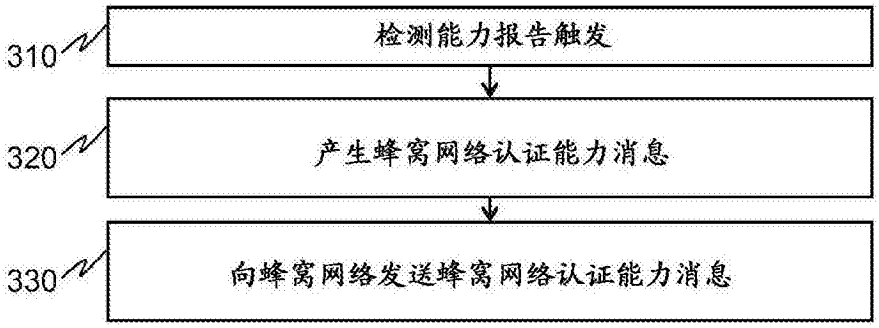

310
检测能力报告触发
320
产生蜂窝网络认证能力消息
330
向蜂窝网络发送蜂窝网络认证能力消息

图3

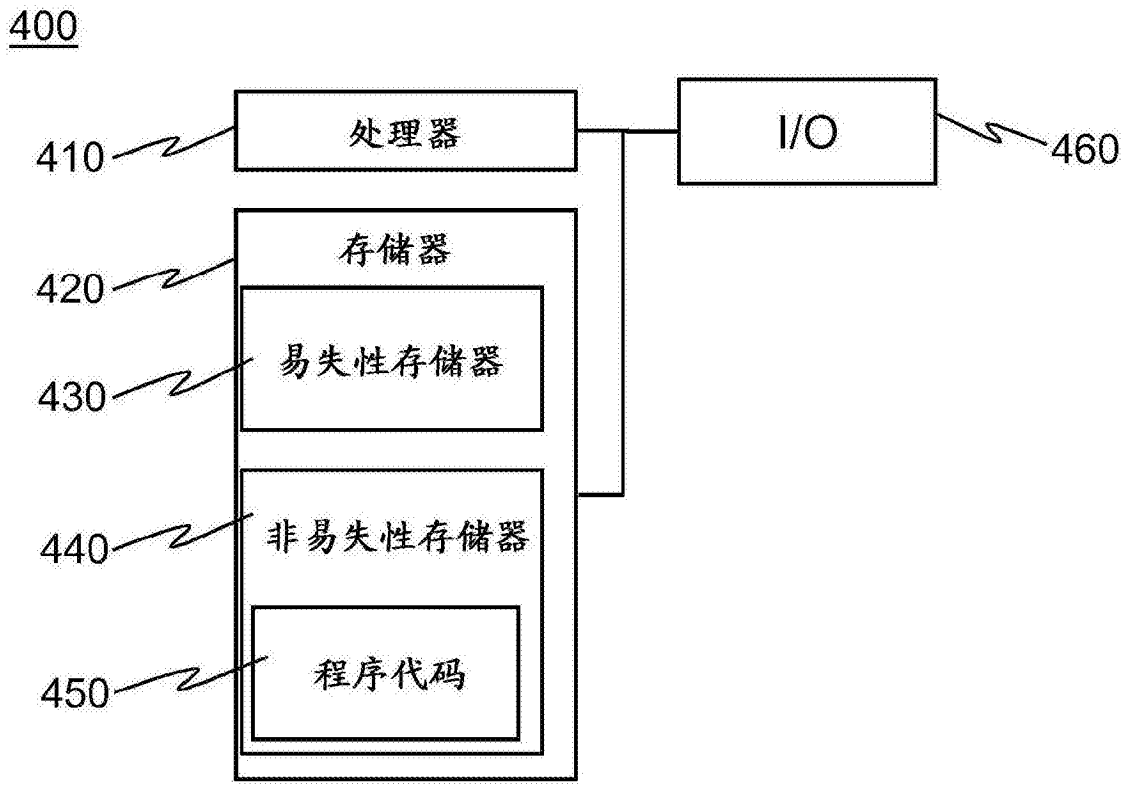

400
处理器
410
I/O
460
存储器
420
易失性存储器
430
非易失性存储器
440
程序代码
450

图4

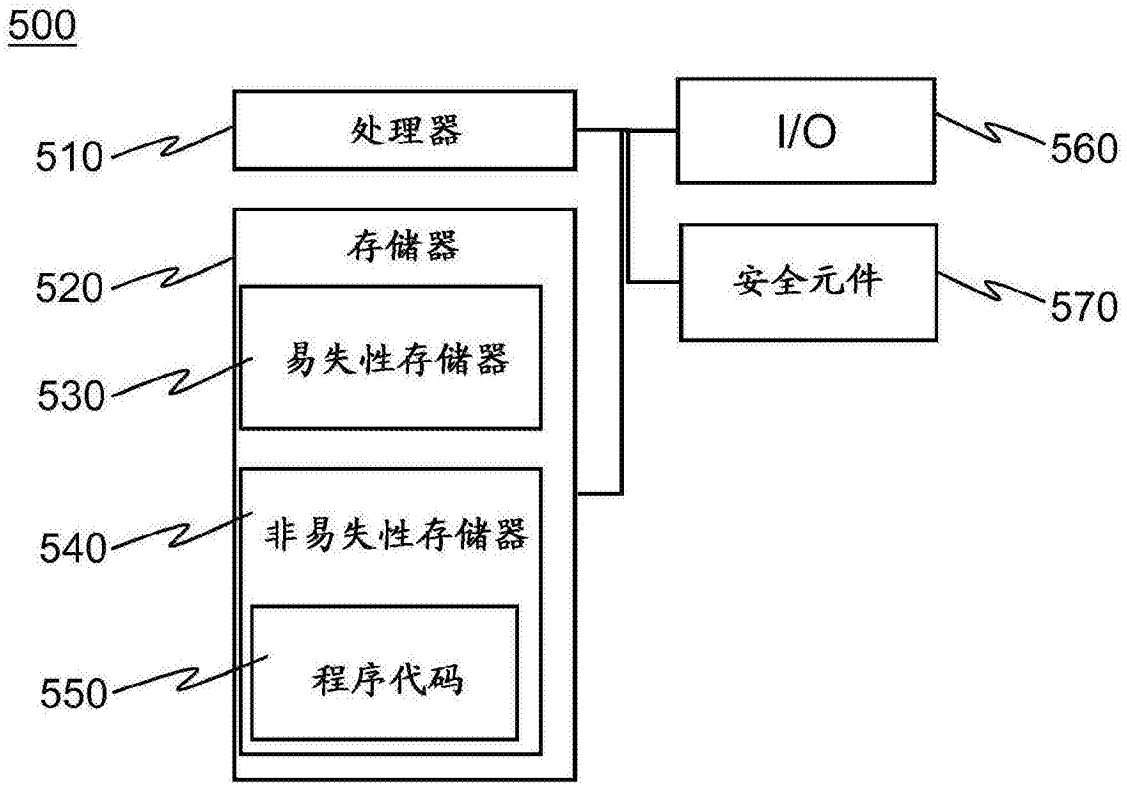

500
处理器
510
I/O
560
存储器
520
安全元件
570
易失性存储器
530
非易失性存储器
540
程序代码
550

图5