(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 107431916 B
(45)授权公告日 2020.11.13

(21)申请号 201680012708.6
(22)申请日 2016.02.22
(65)同一申请的已公布的文献号
申请公布号 CN 107431916 A
(43)申请公布日 2017.12.01
(30)优先权数据
62/128,724 2015.03.05 US
14/808,862 2015.07.24 US
(85)PCT国际申请进入国家阶段日
2017.08.29
(86)PCT国际申请的申请数据
PCT/US2016/018860 2016.02.22
(87)PCT国际申请的公布数据
WO2016/140823 EN 2016.09.09
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 S•B•李 A•帕拉尼恭德尔 A•E•埃斯科特 G•B•霍恩
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张立达 王英
(51)Int.Cl.
H04W 8/04(2009.01)
H04W 8/18(2009.01)
H04W 12/02(2009.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04L 29/12(2006.01)

(56)对比文件
CN 101998377 A,2011.03.30
CN 101959183 A,2011.01.26
CN 101969638 A,2011.02.09
CN 101720086 A,2010.06.02
CN 101511082 A,2009.08.19

审查员 陈晓霞

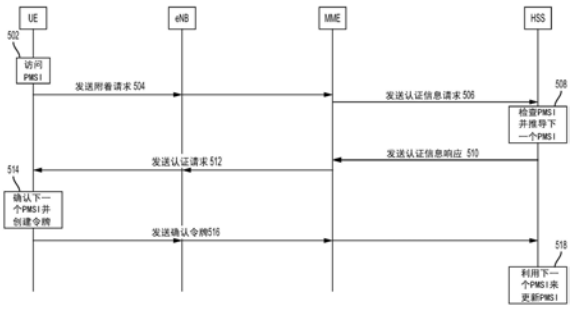
权利要求书6页 说明书19页 附图8页

(54)发明名称

一种用于网络接入技术的方法、用户设备、服务器以及非暂时性计算机可读介质

(57)摘要

公开了用于通过替代地提供私密性移动用户身份来保护用户设备的国际移动用户身份的系统和方法。在向服务网络的附着尝试中,UE提供PMSI而不是IMSI,保护IMSI免受泄露。PMSI是在归属网络服务器与UE之间确定的,使得服务网络中的中间节点单元不知晓PMSI与IMSI之间的关系。在接收到附着请求中的PMSI时,服务器生成要在后续附着请求中使用的下一个PMSI并且将该下一个PMSI发送给UE以进行确认。UE确认该下一个PMSI以便在UE与服务器之间进行同步,并且向服务器发送确认令牌。随后,UE和服务器均更新当前和下一个PMSI值的本地副本。



CN 107431916 B

1.一种用于由用户设备UE进行的网络接入的方法,包括:

利用初始附着消息,从所述UE向服务网络发送私密性移动用户身份PMSI,以作为针对国际移动用户身份IMSI的直接替代来标识所述UE;

从与所述服务网络通信的服务器接收认证请求,所述认证请求包括下一个PMSI和跟踪索引;

由所述UE从所述PMSI和跟踪索引来推导基于UE的下一个PMSI;

响应于所述基于UE的下一个PMSI和所述下一个PMSI匹配,由所述UE生成接收确认;以及

从所述UE向所述服务器发送对所述下一个PMSI的所述接收确认。

2.根据权利要求1所述的方法,还包括:

由所述UE基于初始PMSI来确定用于网络接入的所述PMSI。

3.根据权利要求2所述的方法,还包括:

在所述UE向所述服务器进行用户注册的期间,接收所述初始PMSI。

4.根据权利要求2所述的方法,还包括:

在经由空中通信向所述服务器进行用户注册之后,供应所述初始PMSI。

5.根据权利要求4所述的方法,其中,多个值包括随机数或伪随机数,所述方法还包括:

由所述UE从包括在所述UE处生成的所述随机数或所述伪随机数的数中生成建议的PMSI;

由所述UE使用服务器公钥来加密所生成的PMSI,其中,所述服务器保存相应的服务器私钥;

在所述加密之后,从所述UE向所述服务器发送所生成的PMSI;以及

在所述UE处,从所述服务器接收要使用所生成的PMSI作为所述初始PMSI的确认。

6.根据权利要求1所述的方法,还包括:

在所述生成之前,将所述基于UE的下一个PMSI与作为所述认证请求的一部分而接收的所述下一个PMSI进行比较,以确定是否存在匹配。

7.根据权利要求1所述的方法,还包括:

在所述UE处存储所确认的下一个PMSI以用于下一个附着消息中。

8.根据权利要求1所述的方法,其中,所述接收所述认证请求还包括:

使用匿名密钥来解密所述认证请求中的所述下一个PMSI,其中,所述匿名密钥是根据在所述UE与所述服务器之间共享的秘密密钥来推导出的。

9.根据权利要求1所述的方法,其中,所述下一个PMSI包括与所述PMSI和PMSI生成秘钥的串联的所述跟踪索引的散列。

10.一种用户设备UE,包括:

存储器,其被配置为存储私密性移动用户身份PMSI;

收发机,其被配置为:

利用初始附着消息,向服务网络发送所述PMSI,以作为针对国际移动用户身份IMSI的直接替代来标识所述UE;以及

从与所述服务网络通信的服务器接收认证请求,所述认证请求包括下一个PMSI和跟踪索引;以及

处理器,其被配置为:

从所述PMSI和所述跟踪索引来推导基于UE的下一个PMSI;以及

响应于所述基于UE的下一个PMSI和所述下一个PMSI匹配,生成接收确认,

其中,所述收发机还被配置为向所述服务器发送所述接收确认。

11.根据权利要求10所述的用户设备,其中,所述处理器还被配置为:

基于存储在所述存储器中的初始PMSI来确定用于网络接入的所述PMSI。

12.根据权利要求11所述的用户设备,其中,所述用户设备在所述UE向所述服务器进行用户注册的期间接收所述初始PMSI。

13.根据权利要求11所述的用户设备,其中,所述用户设备被配置为在经由空中通信向所述服务器进行用户注册之后供应所述初始PMSI。

14.根据权利要求13所述的用户设备,其中:

多个值包括在所述UE处生成的随机数或伪随机数;

所述处理器还被配置为从包括在所述UE处生成的所述随机数或所述伪随机数的数中生成建议的初始PMSI,并使用服务器公钥来加密所生成的PMSI,其中,所述服务网络上的所述服务器保存相应的服务器私钥;以及

所述收发机还被配置为:在加密后,向所述服务器发送所生成的PMSI,以及从所述服务器接收要使用所生成的PMSI作为所述初始PMSI的确认。

15.根据权利要求10所述的用户设备,其中,所述处理器还被配置为:

将所述基于UE的下一个PMSI与作为所述认证请求的一部分而接收的所述下一个PMSI进行比较,以确定是否存在匹配。

16.根据权利要求15所述的用户设备,其中,所述存储器还被配置为存储所述下一个PMSI以用于下一个附着消息中。

17.根据权利要求10所述的用户设备,其中,所述处理器还被配置为使用匿名密钥来解密所述认证请求中的所述下一个PMSI,其中,所述匿名密钥是根据在所述UE与所述服务器之间共享的秘密密钥来推导出的。

18.一种用于与网络上的服务器建立网络接入的方法,包括:

经由中间服务网络中的一个或多个网络单元,通过初始附着消息来从用户设备UE接收私密性移动用户身份PMSI,以作为针对国际移动用户身份IMSI的直接替代来标识所述UE;

由所述服务器基于所述PMSI来确定下一个PMSI;

从所述服务器向所述服务网络发送包括所述下一个PMSI和跟踪索引的认证信息,以作为认证的一部分;以及

经由所述服务网络从所述UE接收包括对所述下一个PMSI的确认的、具有确认令牌的接收确认,所述确认令牌是响应于由所述UE从所述PMSI和所述跟踪索引推导出的基于UE的下一个PMSI与所述下一个PMSI匹配而生成的。

19.根据权利要求18所述的方法,还包括:

由所述服务器基于初始PMSI来确定用于网络接入的所述PMSI。

20.根据权利要求19所述的方法,还包括:

在所述服务器处,在所述UE向所述服务器进行用户注册的期间接收所述初始PMSI。

21.根据权利要求19所述的方法,还包括:

从所述UE接收建议的初始PMSI；

由所述服务器使用服务器私钥来解密在所述UE处通过相应的服务器公钥来加密的所述建议的初始PMSI；

由所述服务器存储所述建议的初始PMSI以作为与所述UE相关联的所述初始PMSI；以及

向所述UE发送对将所述建议的初始PMSI作为所述初始PMSI的确认。

22.根据权利要求18所述的方法，还包括：

根据在所述服务器与所述UE之间共享的秘密密钥来推导匿名密钥；

使用所推导的匿名密钥来加密所述认证信息中的所述下一个PMSI；以及

在所述服务器处存储所述下一个PMSI来替代所述PMSI，以用于响应来自所述UE的后续初始附着消息。

23.根据权利要求18所述的方法，其中，所述确定还包括：

检测所述下一个PMSI与关联于不同的UE的另一个现有PMSI之间的冲突；以及

对所述跟踪索引进行递增，并且基于所述下一个PMSI和所递增的跟踪索引来确定新的下一个PMSI。

24.根据权利要求18所述的方法，还包括：

从与所述服务器所位于的归属网络分开的所述服务网络上的移动性管理实体MME接收针对所述UE的所述IMSI的请求；以及

响应于所述请求，发送在所述初始附着消息中所使用的、所述UE的所述PMSI而不是所述UE的所述IMSI。

25.根据权利要求18所述的方法，还包括：

针对对利用所述初始附着消息包括的所述PMSI的匹配，搜索一个或多个数据库；以及

响应于没有定位到匹配，发送针对所述UE的通知来修改在所述UE处保存的PMSI索引以便在所述UE处生成经更新的PMSI。

26.一种服务器，包括：

数据库，其被配置为存储用户设备UE的多个私密性移动用户身份PMSI；

收发机，其被配置为：经由中间服务网络中的一个或多个网络单元，通过初始附着消息来从UE接收私密性移动用户身份PMSI，以作为针对国际移动用户身份IMSI的直接替代来标识所述UE；以及

处理器，其被配置为基于所述PMSI来确定用于所述UE的下一个PMSI；

其中，所述收发机还被配置为：向所述服务网络发送包括所述下一个PMSI和跟踪索引的认证信息以作为认证的一部分，并且经由所述服务网络从所述UE接收包括对所述下一个PMSI的确认的、具有确认令牌的接收确认，所述确认令牌是响应于从所述PMSI和所述跟踪索引推导出的基于UE的下一个PMSI与所述下一个PMSI匹配而生成的。

27.根据权利要求26所述的服务器，其中，所述处理器还被配置为基于初始PMSI来确定用于网络接入的所述PMSI。

28.根据权利要求27所述的服务器，其中，所述收发机还被配置为在所述UE向所述服务器进行用户注册的期间接收所述初始PMSI。

29.根据权利要求27所述的服务器，其中：

所述收发机还被配置为从所述UE接收建议的初始PMSI；

所述处理器还被配置为使用服务器私钥来解密在所述UE处通过相应的服务器公钥来加密的所述建议的初始PMSI,并且存储所述建议的初始PMSI以作为与所述UE相关联的所述初始PMSI;以及

所述收发机还被配置为向所述UE发送对将所述建议的初始PMSI作为所述初始PMSI的确认。

30.根据权利要求26所述的服务器,其中:

所述处理器还被配置为根据在所述服务器与所述UE之间共享的秘密密钥来推导匿名密钥,以及使用所推导的匿名密钥来加密所述认证信息中的所述下一个PMSI;以及

所述数据库还被配置为存储所述下一个PMSI,以替代所述PMSI,以用于响应来自所述UE的后续初始附着消息。

31.根据权利要求26所述的服务器,其中,作为所述确定的一部分,所述处理器还被配置为:

在所述数据库中检测所述下一个PMSI与关联于不同的UE的另一个现有PMSI之间的冲突;以及

对所述跟踪索引进行递增,并且基于所述下一个PMSI和所递增的跟踪索引来确定新的下一个PMSI。

32.根据权利要求26所述的服务器,其中,所述收发机还被配置为:

从与所述服务器所位于的归属网络分开的所述服务网络上的移动性管理实体MME接收针对所述UE的所述IMSI的请求;以及

响应于所述请求,发送在所述初始附着消息中所使用的、所述UE的PMSI而不是所述UE的所述IMSI。

33.根据权利要求26所述的服务器,其中:

所述处理器还被配置为:针对对利用所述初始附着消息包括的所述PMSI的匹配,搜索所述数据库;以及

所述收发机还被配置为:响应于没有定位到匹配,发送针对所述UE的通知来修改在所述UE处保存的PMSI索引以便在所述UE处生成经更新的PMSI。

34.一种具有记录在其上的程序代码的非暂时性计算机可读介质,所述程序代码由计算机执行,所述程序代码包括:

用于使用户设备UE利用初始附着消息,向服务网络发送私密性移动用户身份PMSI,以作为针对国际移动用户身份IMSI的直接替代来标识所述UE的代码;

用于使所述UE从与所述服务网络通信的服务器接收认证请求的代码,所述认证请求包括下一个PMSI和跟踪索引;

用于使所述UE从所述PMSI和所述跟踪索引来推导基于UE的下一个PMSI的代码;

用于使所述UE将所述基于UE的下一个PMSI与作为所述认证请求的一部分而接收的所述下一个PMSI进行比较以确定是否存在所述UE和所述服务器之间的PMSI同步的匹配的代码;

用于响应于确定所述匹配使所述UE生成响应于所述基于UE的下一个PMSI与所述下一个PMSI匹配的接收确认的代码;以及

用于使所述UE向所述服务器发送对所述下一个PMSI的所述接收确认的代码。

35.根据权利要求34所述的非暂时性计算机可读介质,还包括:

用于使所述UE基于初始PMSI来确定用于网络接入的所述PMSI的代码。

36.根据权利要求35所述的非暂时性计算机可读介质,还包括:

用于使所述UE在所述UE向所述服务器进行用户注册的期间,接收所述初始PMSI的代码。

37.根据权利要求35所述的非暂时性计算机可读介质,还包括:

用于使所述UE在经由空中通信向所述服务器进行用户注册之后,供应所述初始PMSI的代码。

38.根据权利要求37所述的非暂时性计算机可读介质,还包括:

用于使所述UE生成建议的PMSI的代码;

用于使所述UE使用服务器公钥来加密所生成的PMSI的代码,其中,所述服务器保存相应的服务器私钥;

用于使所述UE在所述加密之后向所述服务器发送所生成的PMSI的代码;以及

用于使所述UE从所述服务器接收要使用所生成的PMSI作为所述初始PMSI的确认的代码。

39.根据权利要求34所述的非暂时性计算机可读介质,还包括:

用于使所述UE在所述UE处存储所确认的下一个PMSI以用于下一个附着消息中的代码。

40.根据权利要求34所述的非暂时性计算机可读介质,还包括:

用于使所述UE使用匿名密钥来解密所述认证请求中的所述下一个PMSI的代码,其中,所述匿名密钥是根据在所述UE与所述服务器之间共享的秘密密钥来推导出的。

41.一种具有记录在其上的程序代码的非暂时性计算机可读介质,所述程序代码由计算机执行,所述程序代码包括:

用于使服务器经由中间服务网络中的一个或多个网络单元通过初始附着消息来从用户设备UE接收私密性移动用户身份PMSI,以作为针对国际移动用户身份IMSI的直接替代来标识所述UE的代码;

用于使所述服务器基于所述PMSI来确定下一个PMSI的代码;

用于使所述服务器向所述服务网络发送包括所述下一个PMSI和跟踪索引的认证信息以作为认证的一部分的代码;以及

用于使所述服务器经由所述服务网络从所述UE接收包括对所述下一个PMSI的确认的、具有确认令牌的接收确认的代码,所述确认令牌是响应于由所述UE从所述PMSI和所述跟踪索引推导出的基于UE的下一个PMSI与所述下一个PMSI匹配而生成的。

42.根据权利要求41所述的非暂时性计算机可读介质,还包括:

用于使所述服务器基于初始PMSI来确定用于网络接入的所述PMSI的代码。

43.根据权利要求42所述的非暂时性计算机可读介质,还包括:

用于使所述服务器在所述UE向所述服务器进行用户注册的期间接收所述初始PMSI的代码。

44.根据权利要求42所述的非暂时性计算机可读介质,还包括:

用于使所述服务器从所述UE接收建议的初始PMSI的代码;

用于使所述服务器使用服务器私钥来解密在所述UE处通过相应的服务器公钥来加密

的所述建议的初始PMSI的代码;以及

用于使所述服务器向所述UE发送对将所述建议的初始PMSI作为所述初始PMSI的确认的代码。

45.根据权利要求41所述的非暂时性计算机可读介质,还包括:

用于使所述服务器根据在所述服务器与所述UE之间共享的秘密密钥来推导匿名密钥的代码;

用于使所述服务器使用所推导的匿名密钥来加密所述认证信息中的所述下一个PMSI的代码;以及

用于使所述服务器在所述服务器处存储所述下一个PMSI,以替代所述PMSI,以用于响应来自所述UE的后续初始附着消息的代码。

46.根据权利要求41所述的非暂时性计算机可读介质,其中,用于使所述服务器确定所述下一个PMSI的代码还包括:

用于使所述服务器检测所述下一个PMSI与关联于不同的UE的另一个现有PMSI之间的冲突的代码;以及

用于使所述服务器对所述跟踪索引进行递增并且基于所述下一个PMSI和经递增的跟踪索引来确定新的下一个PMSI的代码。

47.根据权利要求41所述的非暂时性计算机可读介质,还包括:

用于使所述服务器从与所述服务器所位于的归属网络分开的所述服务网络上的移动性管理实体MME接收针对所述UE的所述IMSI的请求的代码;以及

用于使所述服务器响应于所述请求,发送在所述初始附着消息中所使用的、所述UE的PMSI而不是所述UE的所述IMSI的代码。

48.根据权利要求41所述的非暂时性计算机可读介质,还包括:

用于使所述服务器针对对利用所述初始附着消息包括的所述PMSI的匹配,搜索一个或多个数据库的代码;以及

用于使所述服务器响应于没有定位到匹配,发送针对所述UE的通知来修改在所述UE处保存的PMSI索引以便在所述UE处生成经更新的PMSI的代码。

一种用于网络接入技术的方法、用户设备、服务器以及非暂时性计算机可读介质

[0001] 对相关申请的交叉引用

[0002] 本申请要求享有于2015年7月24日递交的美国非临时专利申请No.14/808,862的权益，该非临时专利申请要求享有于2015年3月5日递交的、名称为“Identity Privacy in Wireless Networks”的美国临时专利申请No.62/128,724的权益，上述二者的全部公开内容以引用方式并入本文。

技术领域

[0003] 本申请涉及无线通信系统，并且更具体地说，涉及在无线通信期间增加用户身份的私密性。

背景技术

[0004] 为了从网络接收服务，未知的用户设备UE需要向网络进行注册或以其它方式为网络所知。这是使用网络附着过程来实现的。作为附着过程的一部分，UE发送其国际移动用户身份IMSI号。IMSI是UE在与其进行通信的或代表其进行通信的所有网络上使用的唯一标识。UE利用附着请求来发送IMSI，该附着请求在移动性管理实体MME处接收。

[0005] 在保护IMSI免受窃听和跟踪的尝试中，可以在对UE进行初始地认证之后使用临时移动用户身份TMSI。TMSI对特定区域是本地的，因此必须在每个区域中重新分配TMSI。此外，TMSI是在UE提供用于初始认证的IMSI之后首次分配的使得TMSI的分配可以与UE的真实身份相关联。有时在初始附着请求中提供全球唯一临时UE身份GUTI而不是IMSI。在UE发送GUTI而不是其IMSI的情况下，MME请求来自可能先前已与UE交互的其它网络单元的标识。如果UE为其它网络单元所知，则那些其它网络单元用IMSI来响应。如果UE是未知的，那么MME要求UE提供其IMSI以进行标识，该IMSI稍后用于具有位置注册的更新过程。

[0006] 在上面方法中的任何一种方法下，IMSI仍然是易受攻击的。IMSI被包括在初始附着请求中或必须稍后被提供以便被认证。因此，可以经由空中业务来被动地监测IMSI并使用IMSI来确定用户身份。附着请求中的IMSI常常是明文，使得IMSI对于监测来说甚至更易受攻击。甚至在UE不发送IMSI的场景中，MME仍然从其它网络单元获得实际的IMSI，并且数个不同网络单元可以存储该实际的IMSI例如，MME、服务网关S-GW和/或PDN网关P-GW。这使得IMSI是易受攻击的，并且其依赖于服务网络的可信赖性。

发明内容

[0007] 在本公开内容的一个方面中，一种用于由用户设备UE进行的网络接入的方法包括：利用初始附着消息，从所述UE向网络上的服务器发送私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE；从所述服务器接收认证请求，所述认证请求包括下一个PMSI，所述下一个PMSI是根据所述PMSI来推导出的不同值；以及从所述UE向所述服务器发送对所述下一个PMSI的接收确认。

[0008] 在本公开内容的另外方面中，一种用户设备包括：存储器，其被配置为存储私密性移动用户身份PMSI；收发机，其被配置为利用初始附着消息，向网络上的服务器发送PMSI，以替代国际移动用户身份IMSI来标识所述UE，以及从所述服务器接收认证请求，所述认证请求包括下一个PMSI，所述下一个PMSI是根据所述PMSI来推导出的不同值；以及处理器，其被配置为生成接收确认，其中，所述收发机还被配置为向所述服务器发送所述接收确认。

[0009] 在本公开内容的另外方面中，一种具有记录在其上的程序代码的计算机可读介质包括：用于使用户设备UE利用初始附着消息，向网络上的服务器发送私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE的代码；用于使所述UE从所述服务器接收认证请求的代码，所述认证请求包括下一个PMSI，所述下一个PMSI是根据所述PMSI来推导出的不同值；以及用于使所述UE向所述服务器发送对所述下一个PMSI的接收确认的代码。

[0010] 在本公开内容的另外方面中，一种用于与网络上的服务器建立网络接入的方法包括：经由中间服务网络中的一个或多个网络单元，通过初始附着消息来从用户设备UE接收私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE；由所述服务器基于所述PMSI来确定下一个PMSI；从所述服务器发送包括所述下一个PMSI的认证请求；以及从所述UE接收包括对所述下一个PMSI的确认的接收确认。

[0011] 在本公开内容的另外方面中，一种服务器包括：数据库，其被配置为存储用户设备UE的多个私密性移动用户身份PMSI；收发机，其被配置为经由中间服务网络中的一个或多个网络单元，通过初始附着消息来从UE接收私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE；以及处理器，其被配置为基于所述PMSI来确定用于所述UE的下一个PMSI，其中，所述收发机还被配置为发送包括所述下一个PMSI的认证请求，以及接收包括对所述下一个PMSI的确认的接收确认。

[0012] 在本公开内容的另外方面中，一种具有记录在其上的程序代码的计算机可读介质包括：用于使服务器经由中间服务网络中的一个或多个网络单元，通过初始附着消息来从用户设备UE接收私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE的代码；用于使所述服务器基于所述PMSI来确定下一个PMSI的代码；用于使所述服务器发送包括所述下一个PMSI的认证请求的代码；以及用于使所述服务器从所述UE接收包括对所述下一个PMSI的确认的接收确认的代码。

附图说明

[0013] 图1示出了根据本公开内容的各个方面的无线通信网络。

[0014] 图2是根据本公开内容的实施例的示例性UE的框图。

[0015] 图3是根据本公开内容的实施例的示例性服务器的框图。

[0016] 图4是根据本公开内容的各个方面，示出了示例性发射机系统的框图。

[0017] 图5是根据本公开内容的各个方面，示出了在UE、服务网络和归属网络之间的、用于支持无线网络中的身份私密性的一些信号传递方面的协议图。

[0018] 图6A是根据本公开内容的各个方面，示出了用于UE发起附着过程的示例性方法的流程图。

[0019] 图6B是根据本公开内容的各个方面，示出了用于服务器在附着过程中起作用的示

例性方法的流程图。

[0020] 图7A是根据本公开内容的各个方面，示出了用于关于UE的PMSI初始化的示例性方法的流程图。

[0021] 图7B是根据本公开内容的各个方面，示出了用于关于服务器的PMSI初始化的示例性方法的流程图。

具体实施方式

[0022] 下文结合附图所阐述的详细描述旨在作为对各种配置的说明，而非旨在表示其中可以以其实践本文所描述的概念的唯一配置。出于提供对各种概念的透彻理解的目的，详细描述包括具体的细节。然而，对于本领域技术人员来说将显而易见的是，可以在不具有这些具体细节的情况下实践这些概念。在一些实例中，以框图形式示出公知的结构和组件以便避免混淆这些概念。

[0023] 本文所描述的技术可以用于诸如CDMA、TDMA、FDMA、OFDMA、SC-FDMA和其它网络之类的各种无线通信网络。术语“网络”和“系统”经常可互换地使用。CDMA网络可以实现诸如通用陆地无线接入UTRA、cdma2000等无线技术。UTRA包括宽带CDMAWCDMA以及CDMA的其它变型。cdma2000涵盖IS-2000、IS-95和IS-856标准。TDMA网络可以实现诸如全球移动通信系统GSM之类的无线技术。OFDMA网络可以实现诸如演进的UTRAE-UTRA、超移动宽带UMB、IEEE 802.11Wi-Fi、IEEE802.16WiMAX、IEEE 802.20、闪速OFDMA等无线技术。UTRA和E-UTRA是通用移动电信系统UMTS的一部分。3GPP长期演进LTE和先进的LTELTE-A是UMTS的使用E-UTRA的新版本。在来自名为“第三代合作伙伴计划”3GPP的组织的文档中描述了UTRA、E-UTRA、UMTS、LTE、LTE-A和GSM。在来自名为“第三代合作伙伴计划2”3GPP2的组织的文档中描述了CDMA2000和UMB。本文所描述的技术可以用于上文提到的无线网络和无线技术以及其它无线网络和无线技术，诸如下一代例如，第五代5G网络。本公开内容的实施例是针对于可以在上文记载的网络和/或有待开发的网络中的任意一个或多个网络上使用的任意类型的调制方案。

[0024] 本公开内容的实施例介绍了用于通过替代地提供私密性移动用户身份PMSI来保护用户设备的国际移动用户身份的系统和技术。在一个实施例中，UE向服务网络发起附着请求。取代于提供IMSI或该服务网络上的一些单元可以仍然用来访问该IMSI的关联信息，UE利用附着请求来提供PMSI。随后，在整个过程中使用PMSI，使得在UE与服务器之间不需要IMSI。在一个实施例中，每个PMSI用于每个UE以及用于特定UE的不同迭代二者是与众不同的。这保护IMSI免受窃听和免受服务网络中的任何潜在的恶意单元之害。继续该例子，服务网络的单元向UE的归属网络上的服务器例如，归属用户服务器HSS传递PMSI作为认证信息请求的一部分。HSS定位到PMSI以标识相应的UE并且向网络单元提供认证信息响应。作为该响应的一部分，HSS还推导UE针对后续附着请求将使用的下一个PMSI，检查PMSI冲突，并且向服务网络中的网络单元提供下一个PMSI和PMSI跟踪索引以便传递给UE。

[0025] 可以以加密形式提供下一个PMSI和PMSI跟踪索引。以加密的形式，下一个PMSI和PMSI跟踪索引仍被保护免受服务网络中潜在的恶意网络单元之害和免受窃听。UE接收所加密的下一个PMSI和PMSI跟踪索引，并且能够对其进行解密。UE推导出其自身的下一个PMSI副本以确认UE和HSS是同步的。在确认下一个PMSI在UE与HSS之间是同步的之后，UE向服务

器发送确认令牌token。随后,UE和服务器均更新当前和下一个PMSI值的本地副本。HSS不需要为UE存储PMSI的每次迭代。相反地,HSS可以基于初始PMSI值和期望的PMSI跟踪索引值来得出PMSI的任意迭代。

[0026] 在进一步的实施例中,初始PMSI可以是在UE与HSS之间商定的。在一个实施例中,初始PMSI是在用户注册时商定的,使得将初始PMSI供应给UE的SIM卡并且注册到HSS。在另一个实施例中,UE在用户注册时未被供应有PMSI,而是发起与HSS的空中注册。UE可以生成初始PMSI值,并且在使用HSS的公钥或者UE与HSS之间的其它共享密钥来加密该初始PMSI值之后,向HSS发送所建议的初始PMSI。HSS可以利用相应的私钥来解密来自UE的初始PMSI并且确定该PMSI是否与向HSS注册的任何其它现有PMSI值相冲突。在确认不存在冲突后,HSS可以向UE确认初始PMSI并且存储该初始PMSI以便在UE稍后发起其第一附着请求时使用。

[0027] 图1示出了根据本公开内容的各个方面的无线通信网络100。无线通信网络100可以包括多个UE 102以及多个基站104。仅出于简化说明和解释起见,图1中已示出了单个UE 102和单个基站104。基站104可以包括演进型节点BeNodeB。基站还可以被称为基站收发台或接入点。

[0028] 如所示出的,基站104与UE 102通信。UE 102可以经由上行链路和下行链路与基站104通信。下行链路或前向链路指代从基站104到UE 102的通信链路。上行链路反向链路指代从UE 102到基站104的链路。

[0029] UE 102可以散布于整个无线网络100,并且每个UE 102可以是固定的或移动的。UE 102还可以被称为终端、移动站、用户单元等。UE 102可以是蜂窝电话、智能电话、个人数字助理、无线调制解调器、膝上型计算机、平板计算机等。无线通信网络100是本公开内容的各个方面所应用于的网络的一个例子。

[0030] 图1中还示出了移动性管理实体MME106。MME 106可以负责与用户例如,UE 102和会话管理有关的控制平面功能。例如,MME 106可以提供移动性会话管理以及对切换到其它网络、漫游和用户认证的支持。MME 106可以辅助在UE 102的初始附着期间的S-GW的选择、非接入层NAS信令、NAS信令安全、P-GW选择、包括专用承载建立的承载管理功能、信令业务的合法监听和其它功能,仅举几个例子。MME 106和基站104可以在同一个服务网络108例如,演进的分组核心EPC的一部分中。如将认识到的,出于简化对本公开内容的方面的讨论起见,服务网络108包括图1中未示出的许多其它网络单元。

[0031] MME 106与归属网络114中的服务器112通信。在一个实施例中,服务器112是归属用户服务器HSS,除了其它事项之外,其维护归属位置寄存器HLR,HLR负责对保存用户订阅信息的一个或多个数据库进行存储和更新。除了其它事项之外,归属网络114中的服务器112具有UE 102的IMSI用户标识/寻址的副本。服务器112还可以保存用户简档信息,该用户简档信息标识服务订阅状态和/或服务质量QoS信息例如,最大允许的比特率、允许的业务类别等。服务器112还可以包括认证功能,诸如管理根据用户身份密钥来生成的安全信息和该安全信息向HLR和其它网络实体的供应。利用安全信息,可以执行网络-UE认证。出于简化说明和解释的目的,图1中示出了一个服务器112。归属网络114可以包括多个HSS。例如,HSS的数量可以取决于移动用户的数量、设备容量和网络组织。MME 106可以经由网络110来与服务器112通信,如将认识到的,这可以是各种类型的直接或间接连接。

[0032] 如下文参照后续的附图该附图包括示出了在UE、服务网络和归属网络以及相关联

的服务器之间的、用于支持无线网络中的身份私密性的一些信号传递方面的协议图将更详细描述的，UE 102可以将IMSI排除在外，使用私密性移动用户身份PMSI来与服务网络108和归属网络114通信。PMSI可以是与UE 102特定地相关联的唯一号码，并由UE 102和服务器112保存。在本公开内容的实施例中，PMSI可以包括在UE 102和服务器112二者处商定并保持的初始PMSI。用于UE 102的PMSI的特定值可以使用一次，使得在后续每次UE 102发起附着请求时提供新的PMSI值作为该请求的一部分。UE 102和服务器112可以仅存储商定的初始PMSI以及索引。因此，可以基于初始PMSI和用于描述应当执行多少次推导迭代以在UE 102和服务器112二者处得出特定PMSI的特定索引值的共享知识，来后续地推导出任何PMSI值例如，使得UE 102和服务器112关于用于给定会话的特定PMSI保持一致。

[0033] 在一个例子中，UE 102可以将其PMSI而不是IMSI作为其初始附着请求的一部分发送给基站104。随后，基站104将具有UE的PMSI的附着请求转发给MME 106。MME 106将PMSI包括在去往归属网络114的服务器112的认证信息请求中。服务器112能够基于在来自MME 106的初始附着请求/认证信息请求中提供的PMSI来标识UE 102，因此不必向服务网络108提供IMSI。从服务器112回到UE 102的通信也同样基于/包括PMSI而不是IMSI。通信路径中的所有这些阶段使用PMSI而不是IMSI减少了UE 102与基站104之间的空中窃听的风险，并且消除了从服务网络108中的任何网络单元对UE 102的IMSI的可获得性，这是由于将存储PMSI而不是IMSI。

[0034] 图2是根据本公开内容的实施例的示例性UE 102的框图。UE 102可以具有上文所描述的许多种配置中的任何一种。UE 102可以包括处理器202、存储器204、PMSI模块208、收发机210和天线216。这些单元可以例如经由一个或多个总线来彼此直接或间接地通信。

[0035] 处理器202可以包括被配置为执行本文中参照上文针对图1介绍的和下文更详细论述的UE 102所描述的操作的中央处理单元CPU、数字信号处理器DSP、应用特定集成电路ASIC、控制器、现场可编程门阵列FPGA设备、另一种硬件设备、固件设备、或其任意组合。处理器202还可以实现为计算设备的组合，例如DSP和微处理器的组合、多个微处理器、一个或多个微处理器连同DSP内核、或任何其它此种结构。

[0036] 存储器204可以包括高速缓存存储器例如，处理器202的高速缓存存储器、随机存取存储器RAM、磁阻RAMMRAM、只读存储器ROM、可编程只读存储器PROM、可擦除可编程只读存储器EPROM、电可擦除可编程只读存储器EEPROM、闪存、固态存储器设备、硬盘驱动器、其它形式的易失性和非易失性存储器、或不同类型的存储器的组合。在一个实施例中，存储器204包括非暂时性计算机可读介质。存储器204可以存储指令206。指令206可以包括以下指令：当所述指令由处理器202执行时，使处理器202执行本文中结合本公开内容的实施例参照UE 102所描述的操作。指令206还可以被称为代码。术语“指令”和“代码”应被广义地理解为包括任何类型的计算机可读语句。例如，术语“指令”和“代码”可以指代一个或多个程序、例程、子例程、函数、过程等。“指令”和“代码”可以包括单个计算机可读语句或许多个计算机可读语句。

[0037] PMSI模块208可以用于本公开内容的各个方面。例如，PMSI模块208可以涉及对用于特定UE 102的PMSI的初始供应。在一个实施例中，PMSI可以与用于UE 102的IMSI同时被供应给UE 102。例如，在一些实例中，在向HSS例如，图1中的服务器112进行用户注册的期间供应PMSI连同IMSI。可以在制造时在UE 102上的SIM卡中发生这种供应。在另一个实施例

中，可以在UE 102与服务器112之间商定PMSI之前供应IMSI。例如，在已经供应了用于UE 102的IMSI之后，UE 102和服务器112可以通过空中来商定第一初始PMSI。当通过空中商定了PMSI时，UE 102可以生成建议的初始PMSI如下文关于图7A将更详细论述的并且利用服务器112所提供的公钥来加密该建议的初始PMSI。以此方式，可以保护由UE 102发送的该建议的初始PMSI免受窃听和免受服务网络108中潜在受损害的网络单元之害。服务器112保存相应的私钥并且能够解密该建议的初始PMSI。服务器112可以对照一个或多个数据库检查该建议的初始PMSI，以验证不存在与由归属网络114中的服务器112或其它单元保存的、任何其它UE的PMSI的冲突。

[0038] PMSI模块208可以额外地涉及PMSI确认。如上所述，特定的PMSI基于初始PMSI可以仅用于预定数量的附着请求例如，一个、两个、三个或更多个，使得为后续附着请求提供不同的PMSI值。响应于来自UE 102的附着请求，服务器112可以生成“下一个PMSI”将在后续会话中使用的下一个PMSI值，并且将其作为响应于初始附着请求的认证请求的一部分来与UE 102共享该下一个PMSI。UE 102的PMSI模块208可以基于所存储的初始PMSI和递增的索引如下文进一步所论述的来计算其自身的下一个PMSI值，并且将本地计算出的下一个PMSI与从服务器112接收的下一个PMSI进行比较。如果存在匹配，则PMSI模块208可以使UE 102生成用于向服务器112确认该下一个PMSI的响应。如果不存在匹配，则PMSI模块208可以利用从具有下一个PMSI的服务器112接收的索引来更新其本地索引，使得在重新计算之后，这些值匹配。

[0039] 收发机210可以包括调制解调器子系统212和射频RF单元214。收发机210被配置为与其它设备例如，基站104双向地通信。调制解调器子系统212可以被配置为根据调制和编码方案MCS例如，低密度校验LDPC编码方案、turbo编码方案、卷积编码方案等对来自PMSI模块208的数据进行调制和/或编码。RF单元214可以被配置为对来自调制解调器子系统212在向外传输上的经调制/经编码的数据或源自于诸如基站104之类的另一个源的传输的经调制/经编码的数据进行处理例如，执行模数转换或数模转换等。尽管示出为与收发机210集成在一起，但是调制解调器子系统212和RF单元214可以是单独的设备，这些单独的设备在UE 102处耦合在一起以使得UE 102能够与其它设备通信。

[0040] RF单元214可以将经调制和/或经处理的数据例如，数据分组或者，更一般地，可包含一个或多个数据分组或其它信息包括PMSI值的数据消息提供给天线216以便传输到一个或多个其它设备。这可以包括例如根据本公开内容的实施例的向基站104的对数据消息的传输。天线216还可以接收从基站104发送的数据消息并且提供所接收的数据消息以便在收发机210处进行处理和/或解调。尽管图2将天线216示出为单个天线，但是天线216可以包括具有相似或不同设计的多个天线以便支持多个传输链路。

[0041] 图3是示出了根据本公开内容的实施例的示例性服务器112的框图。服务器112可以包括处理器302、存储器304、PMSI模块308、数据库310和收发机312。这些单元可以例如经由一个或多个总线来彼此直接或间接地通信。如上文参照图1所提到的，服务器112可以是提供归属位置寄存器和认证功能仅举两个例子的HSS。

[0042] 处理器302可以包括被配置为执行本文中参照上文在图1中介绍的服务器112所描述的操作的CPU、DSP、ASIC、控制器、FPGA设备、另一种硬件设备、固件设备、或其任意组合。处理器302还可以实现为计算设备的组合，例如DSP和微处理器的组合、多个微处理器、一个

或多个微处理器连同DSP内核、或任何其它此种结构。

[0043] 存储器304可以包括高速缓存存储器例如，处理器302的高速缓存存储器、RAM、MRAM、ROM、PROM、EPROM、EEPROM、闪存、固态存储器设备、一个或多个硬盘驱动器、其它形式的易失性和非易失性存储器、或不同类型的存储器的组合。在一个实施例中，存储器304包括非暂时性计算机可读介质。存储器304可以存储指令306。指令306可以包括以下的指令：当所述指令由处理器302执行时，使处理器302执行本文中结合本公开内容的实施例参照服务器112所描述的操作。指令306还可以被称为代码，其可以被广义地解释为包括任何类型的计算机可读语句，如上文参照图2所论述的。

[0044] PMSI模块308可以用于本公开内容的各个方面。例如，PMSI模块308可以涉及对用于特定UE 102的PMSI的初始供应。在一个实施例中，PMSI可以与用于UE 102的IMSI同时例如在用户注册期间被供应和存储在数据库310中。在另一个实施例中，可以在服务器112与UE 102之间商定PMSI之前供应IMSI。例如，在已经供应了用于UE 102的IMSI之后，服务器112可以通过空中与UE 102商定第一初始PMSI。当通过空中商定了时，服务器112可以从UE 102接收由UE 102生成的建议的初始PMSI如下文关于图7B将更详细论述的。该建议的初始PMSI可能已利用由服务器112向UE 102提供的公钥来加密。因此，服务器112可以使用相应的私钥来解密该建议的初始PMSI。以此方式，可以保护PMSI免受窃听和免受服务网络108中潜在受损害的网络单元之害。服务器112可以对照数据库310中的PMSI值检查该建议的初始PMSI，以验证不存在与由归属网络114中的服务器112或其它单元保存的、任何其它UE的PMSI的冲突。

[0045] PMSI模块308可以额外地涉及与UE 102的初始附着过程。服务器112可以接收利用来自UE的初始附着请求来提供的PMSI，并且对照数据库310中所存储的PMSI值检查该PMSI。响应于来自UE 102的附着请求，服务器112可以生成下一个PMSI，并且将其作为响应于初始附着请求的认证请求的一部分来向UE 102发送该下一个PMSI。响应于从UE 102接收到用于确认下一个PMSI的响应，PMSI模块308更新在数据库310中所存储的PMSI值。例如，当前PMSI值变为先前的PMSI值并且下一个PMSI值变为用于后续交互例如，来自UE 102的后续附着请求的当前PMSI值。

[0046] 出于论述的目的，本文提及了四种PMSI值：1初始PMSI，其是UE 102和服务器112用于推导后续PMSI值的初始商定的PMSI值；2当前PMSI，其是在当前附着请求过程中使用的PMSI值例如，UE 102第一次发送初始附着请求时，当前PMSI可以等于初始PMSI，而在其它实施例中可以对PMSI进行迭代一次或多次，使得即使在初始附着请求期间也保持初始PMSI较安全；3在先的或先前的PMSI，其是在当前PMSI之前的PMSI例如，在先前附着请求中使用的PMSI和/或用于得出当前PMSI的PMSI；以及4下一个PMSI，其是跟在当前PMSI后面的PMSI例如，针对商定应当将怎样的PMSI用于UE 102发起的、与任何给定服务网络108的下一个附着过程，UE 102和服务器112二者推导出的PMSI。

[0047] 数据库310可以包括由服务器112维护的一个或多个数据库，例如上文参照图1所提到的HLR。数据库310可以跟踪诸如用户标识和寻址之类的用户信息包括例如IMSI、PMSI包括初始PMSI、当前PMSI、先前的PMSI和/或下一个PMSI、PMSI跟踪索引和所有用户或用户子集的移动电话号码、简档信息例如，服务订阅状态、以及与每个用户相关联的安全信息例如，安全密钥。

[0048] 收发机312使得服务器112能够进行通信以向外部源发送数据和从外部源接收数据，这些外部源诸如归属网络114中的其它网络单元或服务网络108。收发机312可以实现无线和/或有线通信。如将认识到的，收发机312可以包括例如以太网连接、WiFi连接、或其它类型的调制解调器和/或RF子系统。

[0049] 图4是根据本公开内容的某些方面，示出了MIMO系统400中的示例性发射机系统410例如，基站104和接收机系统450例如，UE 102的框图。在发射机系统410处，从数据源412向发射TX数据处理器414提供多个数据流的业务数据。根据本公开内容的方面，该业务数据可以包括各种各样的业务，其包括来自一个或多个MME实体的认证请求。

[0050] 在下行链路传输中，例如，在各自的发射天线上发送每个数据流。TX数据处理器414基于为每个数据流选定的特定编码方案来对该数据流的业务数据进行格式化、编码和交织以提供经编码的数据。

[0051] 可以使用OFDM技术将每个数据流的经编码的数据与导频数据复用在一起。导频数据例如，导频序列通常是已知的数据模式，其以已知方式被处理并且可以在接收机系统处用于估计信道响应或其它信道参数。可以将导频数据格式化成导频符号。可以由处理器430执行的指令来确定导频符号的数量和导频符号在OFDM符号内的放置。

[0052] 随后，基于为每个数据流选定的特定调制方案例如，BPSK、QSPK、M-PSK或M-QAM来对该数据流的复用的导频和编码数据进行调制即，符号映射以提供调制符号。可以由处理器430执行的指令来确定每个数据流的数据速率、编码和调制。还可以由处理器430执行的指令来确定导频符号的数量和导频符号在每个帧中的放置，例如如上文参照图2或图3所描述的。发射机系统410还包括存储器432，例如如上文参照图2或图3所描述的。

[0053] 随后将所有数据流的调制符号提供给TX MIMO处理器420，TX MIMO处理器420可以进一步处理调制符号例如，针对OFDM。随后，TX MIMO处理器420将N_T个调制符号流提供给N_T个发射机TMTR422_a至422_t.在一些实施例中，TX MIMO处理器420向数据流的符号以及向从其发送符号的天线应用波束成形权重。发射机系统410包括具有仅一个天线或具有多个天线的实施例。

[0054] 每个发射机422接收并处理各自的符号流以提供一个或多个模拟信号，并且进一步调节例如，放大、滤波和上变频模拟信号以提供适合于在MIMO信道上传输的调制信号。随后，从N_T个天线424_a至424_t分别发送来自发射机422_a至422_t的N_T个调制符号。本文所描述的技术还应用于具有仅一个发射天线的系统。使用一个天线的传输比多天线场景要简单。例如，在单天线场景中可能不需要TX MIMO处理器420。

[0055] 在接收机系统450处，由N_R个天线452_a至452_r接收所发送的调制信号，并且将从每个天线452接收的信号提供给各自的接收机RCVR454_a至454_r。每个接收机454调节例如，滤波、放大和下变频各自的接收信号，对经调节的信号进行数字化以提供采样，并且进一步处理采样以提供相应的“接收到的”符号流。本文所描述的技术还应用于具有仅一个天线452的接收机系统450的实施例。

[0056] 随后，RX数据处理器460基于特定的接收机处理技术从接收机454_a至454_r接收并处理N_R个接收符号流，以提供N_T个经检测的符号流。随后，RX数据处理器460根据需要对每个经检测的符号流进行解调、解交织和解码，以恢复数据流的业务数据。根据本公开内容的方面，所恢复的业务可以包括例如来自MME的认证信息请求中的信息。由RX数据处理器460进

行的处理可以与在发射机系统410处由TX MIMO处理器420和TX数据处理器414执行的处理互补。

[0057] 由RX数据处理器460所提供的信息允许处理器470生成诸如信道状态信息CSI和其它信息之类的报告以提供给TX数据处理器438。处理器470制定formulate包括CSI和/或导频请求的反向链路消息以发送给发射机系统。

[0058] 处理器470可以实现成例如上文关于图2或图3中描述的处理器所描述的。除了反向链路消息之外，接收机系统450可以发送其它各种类型的信息，包括附着请求、确认令牌和用于建立通信会话的其它信息以及在通信会话期间的数据。消息可以由TX数据处理器438进行处理、由TX MIMO处理器480进行调制、由发射机454_a至454_r进行调节，并且被发送回发射机系统410。如所示出的，TX数据处理器438还可以从数据源436接收多个数据流的业务数据。

[0059] 在发射机系统410处，来自接收机系统450的调制信号由天线424进行接收、由接收机422进行调节、由解调器440进行解调，并且由RX数据处理器442进行处理，以提取由接收机系统450所发送的反向链路消息。因此，可以在发射机系统410与接收机系统450之间发送和接收数据。如将认识到的，发射机系统410还可以用于将其从接收机系统450接收的信息发送给其服务网络内的其它网络单元以及从服务网络中的一个或多个其它网络单元接收信息。图4中示出的实施例仅是示例性的，本公开内容的实施例适用于未在图4中示出的其它发射机/接收机系统。

[0060] 图5是根据本公开内容的各个方面，示出了在UE、服务网络和归属网络以及服务器之间的、用于支持无线网络中的身份私密性的一些信号传递方面的协议图。为了简化论述，在描述图5的协议图中的动作时将引用图1中示出的单元例如，UE 102、基站104其作为eNB、MME 106以及服务器112其作为HSS。进一步出于简化起见，论述将聚焦于协议流的对本公开内容的实施例的方面进行描述的那些方面而不是附着过程的所有方面例如，论述将聚焦于除了具有一些重叠的3GPP标准例如在TS 23.401 5.3.2.1中找到的，或其它附着过程以外的方面或不同于具有一些重叠的3GPP标准的方面。

[0061] 在动作502，UE 102访问在UE 102中所存储的当前PMSI。在UE 102第一次尝试附着到服务网络108的情况下，当前PMSI可以对应于初始PMSI例如，其中PMSI是与UE 102的IMSI同时被供应的，或者其中PMSI是在稍后但在附着请求之前商定的。在在先的附着过程已发生的实施例中或者由于在服务器112处的PMSI冲突而成为必要的实施例中，存储在UE 102中的当前PMSI是在在先的附着过程期间UE与服务器112之间商定的下一个PMSI。UE 102可以存储一个或多个PMSI值，包括初始PMSI、当前PMSI、先前的PMSI和/或下一个PMSI。在一些实例中，当前PMSI存储成与先前的PMSI值不同的值。

[0062] 在一些实施例中，UE 102根据先前的PMSI和PMSI跟踪索引来推导当前PMSI。例如，对于初始PMSI，PMSI跟踪索引可以初始化为0，并且每次UE 102和服务器112成功地完成附着过程时，可以在UE 102和服务器112处将PMSI跟踪索引递增固定值例如，1。因此，UE 102和服务器112中的每一个可以存储[初始PMSI，PMSI跟踪索引]，其可以用于得出当前在使用中的PMSI的任何迭代。每一个还可以存储[当前PMSI，PMSI跟踪索引]并且依赖于PMSI跟踪索引来确定是否需要替代地引用初始PMSI例如，当索引值在UE 102与服务器112之间不匹配时。

[0063] 在动作504,UE 102例如通过向基站104发送初始附着请求,来向服务网络108发送初始附着请求,该初始附着请求随后前进至MME 106。初始附着请求包括当前PMSI而不是IMSI或服务网络108内的一个或多个单元可以用于与UE 102的IMSI进行关联的任何其它值。

[0064] 在MME 106在动作504期间接收到初始附着请求之后,在动作506,MME 106取得初始附着请求中的信息并且向服务器112发送认证信息请求。该认证信息请求可以包括当前PMSI和序列号,该序列号指代UE 102正在接入的服务网络108。

[0065] 在动作508,在服务器112在动作506期间已接收到认证信息请求之后,服务器112检查认证信息请求中所包括的PMSI并且除了别的事情之外对照一个或多个数据库检查PMSI。作为动作508的一部分,服务器112对PMSI进行解密当PMSI已被加密时。例如,服务器112可以使用与用于对PMSI进行加密的公钥相关联的私钥来对PMSI进行解密。服务器112将PMSI与例如在上文图3中描述的数据库310中所存储的值进行比较。当服务器112发现PMSI值之间的匹配时,服务器112还可以检查与从UE 102接收的当前PMSI相对应的IMSI。

[0066] 当存在PMSI值的匹配时,作为动作508的一部分,服务器112例如,PMSI模块308可以推导下一个PMSI以便包括在去往MME 106的认证响应中。在一个实施例中,如以下来推导下一个PMSI。将PMSI跟踪索引递增一固定量例如,1并且将其串联到数据库310中所存储的当前PMSI值如在来自MME 106的认证信息请求中所标识的。该值作为输入连同K_{PMSI}值被包括到另一个推导函数中。K_{PMSI}是PMSI生成密钥。例如,K_{PMSI}可以是通过使用密钥推导函数KDF来创建的,该KDF具有原始密钥K例如,EPS主密钥和PMSI推导上下文CTX作为输入例如,K_{PMSI}＝KDF(K,CTX)。CTX可以是上下文,例如,诸如“PMSI生成”之类的字符串—通过在密钥生成中使用上下文,可以使用相同的密钥K来生成不同的密钥,诸如通过并入不同的上下文来得到有差异的密钥生成结果。

[0067] 与索引串联的K_{PMSI}值和PMSI在函数中一起被散列化例如,(结果＝HMAC(K_{PMSI},PMSI|索引),其中|是串联运算符。可以对函数的结果进行截断,使得将HMAC函数的输出带密钥的散列消息认证码限制到固定数量的数字例如,9-10个数位。随后可以将该截断的结果与移动网络码MNC和移动国家码MCC串联并且所得值变为下一个PMSI。作为截断的结果,在一个实施例中该值可以是15个数位长,但是将认识到,在不脱离本公开内容的范围的情况下,其它长度更长和更短是可能的。在一个实施例中,可以如下描述整个运算:

[0068] 下一个PMSI＝MCC|MNC|截断(HMAC(K_{PMSI},PMSI|索引)).公式1

[0069] 一般而言,服务器112可以存储PMSI例如,初始和/或当前PMSI与PMSI跟踪索引。PMSI跟踪索引使得服务器112能够通过对初始PMSI重复地散列化x次来根据初始PMSI计算当前PMSI,其中x等于PMSI跟踪索引值。PMSI跟踪索引对于计账以及对于冲突避免也是有用的。例如,服务器112可以对照其它已知的PMSI值来检查所生成的下一个PMSI,以验证不存在与任何其它UE的PMSI的冲突。在存在冲突的情况下,服务器112可以将索引递增例如,递增1并且利用新的PMSI-串联-索引值来重复公式1。

[0070] 在动作510,服务器112取得所生成的信息并且将其并入到要发送给MME 106的认证信息响应中。可以为了认证信息响应中增加的安全性而对下一个PMSI进行加密,例如,使得MME 106不能够区分在UE 102与服务器112之间的下一个PMSI。例如,可以利用根据K_{PMSI}和随机数RAND推导出的匿名密钥例如,匿名密钥＝函数(K_{PMSI},RAND)来对下一个PMSI进行

加密。

[0071] 匿名密钥是通过将K_{PMSI}和随机数RAND放置到密钥推导函数中作为输入而推导出的。密钥推导函数可以是符合3GPP标准或未来等同/相似的标准的任何推导函数，例如f5*。在一个实施例中，密钥推导函数可以是HMAC函数。因此，在一个实施例中，匿名密钥可以是由HMAC(K_{PMSI},RAND)推导出的。在替代的实施例中，匿名密钥可以是密钥加密密钥KEK，其中启用了初始服务网络108认证。

[0072] 作为动作510的一部分，服务器112可以向MME 106发送认证信息响应。认证信息响应可以包括除了其它事项以外认证向量和加密形式的下一个PMSI/PMSI跟踪索引如由以上描述了其推导的匿名函数所加密的。在一个实施例中，认证向量自身可以包括认证令牌、期望的响应、随机数和本地主密钥K_{ASME}。因此，除了传统上认证向量可以包括的那些以外，本公开内容的实施例还包括用于与UE 102同步的下一个PMSI和PMSI跟踪索引。MME 106可以存储认证向量，但是在一些实施例中，其不存储经加密的PMSI/PMSI跟踪索引。

[0073] 在动作512，MME 106通过向UE 102发送认证请求来参与与UE 102的相互认证。认证请求带有从动作510的认证信息响应获得的信息。例如，MME 106可以保持期望的响应作为认证的一部分，并且传递认证令牌、随机数、eUTRAN密钥集标识符eKSI以及经加密的下一个PMSI和PMSI跟踪索引。

[0074] 在动作514，UE 102除了与MME 106的传统相互认证过程以外确认下一个PMSI并且生成用于返回给服务器112的确认令牌。关于这一点，UE 102从在动作512中接收的认证请求中解密出经加密的下一个PMSI和PMSI跟踪索引值。UE 102能够解密下一个PMSI和PMSI跟踪索引值，这是因为UE 102具有服务器112而不是MME 106也具有的共享秘密密钥CTXPMSI推导密钥。

[0075] UE 102自身推导出下一个PMSI，以便与由服务器112所生成的下一个PMSI进行比较以确认它们是否是同步的。UE 102可以通过利用下一个PMSI跟踪索引对当前PMSI进行散列化来推导下一个PMSI。或者，UE 102可以通过对初始PMSI重复地散列化x次来推导下一个PMSI，其中x等于PMSI跟踪索引值如UE 102本地地保存的或如从服务器112解密出的。随后UE 102将本地推导出的下一个PMSI与从服务器112接收的下一个PMSI进行比较。如果值匹配，则UE 102可以继续生成确认令牌。

[0076] 如果这两个下一个PMSI值不匹配例如，当UE 102使用其自身版本的PMSI跟踪索引时，则UE 102和服务器112不是同步的。这可能例如在来自UE 102的消息或去往UE 102的消息在途中被丢弃的情形中发生。在该场景中，UE 102可以更新其PMSI跟踪索引以对应于从服务器112接收和解密的PMSI跟踪索引。随后UE 102可以重新推导下一个PMSI并将其与从服务器112接收和解密的下一个PMSI再次进行比较。

[0077] 在下一个PMSI被确认的情况下该下一个PMSI将用作针对后续附着过程的当前PMSI值，UE 102可以继续生成确认令牌。可以通过串联经加密的序列号用于同步和MAC-A值来生成确认令牌。加密方面包括对在UE 102与服务器112之间共享的序列号进行加密。加密可以是通过另一个匿名密钥来执行的，在一个实施例中，该另一个匿名密钥不同于上文在动作510所描述的匿名密钥例如，这里匿名密钥是使用符合3GPP标准或其它标准的不同函数来推导的。例如，用于加密序列号的匿名密钥自身可以是由采用上文所描述的K_{PMSI}和随机数作为输入的各种密钥推导函数中的任何一种来生成的。

[0078] 串联到经加密的序列号的MAC-A值是根据消息认证函数例如,f1*来生成的,消息认证函数采用另一个匿名密钥例如,不同于上文所描述的其它匿名密钥中的任何一种、与随机数串联的序列号、和认证管理字段AMF值作为输入。用作消息认证函数中的输入的匿名密钥可以是通过采用K_{PMSI}和随机数作为输入的另一个密钥推导函数来生成的。出于简化讨论起见,描述了这些函数和特定的输入。如将认识到的,在不脱离本公开内容的范围的情况下,可以使用其它的函数和对这些函数的其它输入。

[0079] 在动作516,UE 102将在动作514生成的确认令牌发送回给MME 106和服务器112作为PMSI确认消息。PMSI确认消息可以包括上文关于动作514所生成和描述的认证令牌,以及随机数例如,上文在密钥推导函数中使用的相同随机数。在一个实施例中,可以利用附着过程的其它方面例如,加密的选项响应消息从UE 102向MME 106捎带piggybackPMSI确认消息,这里没有详细描述。在MME 106处,可以利用发送给服务器112的另一个消息例如,更新位置请求从MME 106向服务器112捎带PMSI确认消息。

[0080] 在动作518,在接收到确认令牌时,服务器112用当前PMSI值来更新先前的PMSI,并用下一个PMSI值其已通过UE 102进行确认,并因此是同步的来更新当前PMSI。这是有用的,使得在附着过程中使用的PMSI值可以仍然在建立的会话期间在服务器112、服务网络108和UE 102之间使用,例如在向其它MME的切换期间,使得UE 102的位置可以向服务器112适当地更新而无需披露UE 102的IMSI。尽管根据本公开内容,任何对IMSI的使用由对PMSI的使用来替换,但该附着过程随后可以继续包括传统上执行的其它方面。

[0081] 在UE 102的成功认证之后,例如参照图5所描述的,依据一些管辖区域的法律,可能要求服务器112向诸如图1中示出的服务网络108之类的请求服务网络披露UE 102的IMSI。根据本公开内容的方面,在这些情况下服务器112可以仍然供应PMSI来替代IMSI以防范一个或多个恶意网络单元例如恶意的MME 106的可能性。

[0082] 这种请求可能如下所呈现尽管在图5中未示出。MME 106可以向服务器112发送对UE 102的IMSI请求。根据本公开内容的实施例,由于MME106在附着过程或切换期间没有接收到UE 102的IMSI而是接收到PMSI,因此MME 106包括所接收的与UE 102相关联的PMSI连同K_{IMSI}加密密钥。K_{IMSI}加密密钥可以生成为来自函数例如,具有K_{ASME}访问安全管理实体和IMSI取回密钥作为输入的HMAC函数的结果。K_{ASME}是MME 106基本密钥,其对于MME 106和服务器112都是已知的。

[0083] 响应于IMSI请求,服务器112提供IMSI响应。在一个实施例中,在MME 106不具有用来得出IMSI的其它能力的情况下,服务器112发送PMSI。这是可能的,例如,由于服务器112仍然保持着UE 102的PMSI与IMSI其是IMSI请求的主题之间的关联,并且因此出于所有意图,PMSI提供所请求的验证,这是因为服务器112将能够如使用IMSI一样使用PMSI来访问相同的信息。在另一个实施例中,服务器112利用PMSI以及加密版本的IMSI来进行响应。例如,服务器112可以取得PMSI和IMSI并且使用K_{IMSI}来对它们进行加密。因此,可以仅由有效地拥有K_{ASME}的MME 106来正确地解密IMSI。

[0084] 现在转到图6A,根据本公开内容的各个方面,流程图示出了用于UE使用PMSI来发起附着过程的示例性方法600。可以在与服务网络108例如,仅示出服务网络108的两个网络单元,基站104和MME 106相通信的UE102中实现方法600。出于简化论述起见,将参照特定的UE 102来描述方法600,但是将认识到的,本文所描述的方面可以适用于多个UE 102。应当

理解，可以在方法600的步骤之前、期间和之后提供额外的步骤，并且对于方法600的其它实施例来说，可以替换或消除所描述的步骤中的一些步骤。

[0085] 在步骤602，UE 102访问当前PMSI，该当前PMSI将用于在步骤604处的初始附着请求。如上文参照图5所论述的，如果对于UE 102而言是第一次附着尝试，则当前PMSI可以是在UE 102处例如，在存储器204中所存储的初始PMSI。在在先的附着过程已发生的其它实施例中，当前PMSI是在在先的附着过程期间在服务器112与UE 102之间确认的下一个PMSI。

[0086] 在步骤604，一旦取得当前PMSI，UE 102就向当前服务网络例如，如图1中所示出的108发送初始附着请求。初始附着请求包括所取得的当前PMSI而不是IMSI或可以用于重构UE 102的IMSI的其它值以及其它信息。初始附着请求可以由基站104接收，基站104将该请求转发给MME 106。在MME 106接收到初始附着请求之后，MME 106取得初始附着请求中的信息并且向服务器112发送具有PMSI而不是IMSI的认证信息请求。

[0087] 在步骤606，UE 102从服务网络108中的MME 106例如，经由基站104接收认证请求例如如上文在图5的动作512处所描述的。认证请求可以包括来自服务器112的经加密的下一个PMSI和PMSI跟踪索引，MME 106可能无法访问该经加密的下一个PMSI和PMSI跟踪索引，因为其不具有适当的密钥来进行解密。

[0088] 在步骤608，UE 102对从MME 106接收的作为认证请求的一部分的下一个PMSI和PMSI跟踪索引值进行解密。UE 102能够对下一个PMSI和PMSI跟踪索引值进行解密，这是因为UE 102具有服务器112在生成用于加密这些值的匿名密钥时所使用的共享秘密密钥，如上文参照图5的动作508和514所描述的。

[0089] 在步骤610，UE 102自身推导下一个PMSI值即，无需依赖于在步骤608处接收的下一个PMSI和PMSI跟踪索引。在一个实施例中，UE 102基于在UE 102处例如，在存储器204中所存储的先前的PMSI值和PMSI跟踪索引值来推导下一个PMSI值。在另一个实施例中，UE 102基于存储在UE 102中的初始PMSI值以及PMSI跟踪索引的当前值来推导下一个PMSI值例如，对PMSI值进行散列化若干次，该次数等于PMSI跟踪索引的当前值。

[0090] 在步骤612，UE 102例如，处理器202与PMSI模块208合作将本地推导出的下一个PMSI值与所接收和解密的下一个PMSI值进行比较。

[0091] 在决定步骤614，如果本地推导出的下一个PMSI值与所接收和解密的下一个PMSI值不匹配，则方法600行进到步骤616，其中在步骤616，UE102将其本地版本的PMSI跟踪索引更新为等于从服务器112接收和解密的PMSI跟踪索引的值。随后方法600从步骤616行进回到步骤610，在步骤610该过程如上文所描述的继续进行。

[0092] 返回到决定步骤614，如果本地推导出的下一个PMSI值与所接收和解密的下一个PMSI值确实匹配，则方法600行进到步骤618。

[0093] 在步骤618，UE 102例如，处理器202与PMSI模块208合作生成要向服务器112发送的确认令牌，例如如上文参照图5的动作514所描述的。

[0094] 在步骤620，UE 102例如经由服务网络108的一个或多个网络单元向服务器112发送所生成的确认令牌。UE 102还例如通过以下方式来更新其本地PMSI值：更新先前的PMSI以反映当前PMSI值在当前附着过程中使用的PMSI，以及更新当前PMSI以反映同步的下一个PMSI值。如将认识到的，UE 102和服务网络108可以继续建立通信会话。

[0095] 图6B是根据本公开内容的各个方面，示出了用于服务器在附着过程中使用PMSI的

示例性方法630的流程图。可以在与服务网络108例如，仅示出服务网络108的一个网络单元例子，MME 106相通信的服务器112中实现方法630。出于简化论述起见，将参照服务器112来描述方法630，但是将认识到的，本文所描述的方面可以适用于多个服务器112。应当理解，可以在方法630的步骤之前、期间和之后提供额外的步骤，并且对于方法630的其它实施例来说可以替换或消除所描述的步骤中的一些步骤。

[0096] 在步骤632，服务器112从服务网络108例如，MME 106接收认证信息请求，该认证信息请求包括由UE 102提供给MME 106的当前PMSI而不是UE 102的IMSI。如上文参照动作506所描述的，MME 106基于该MME 106从UE 102接收的初始附着请求来发送认证信息请求。

[0097] 在步骤634，服务器112例如，处理器302与PMSI模块308和数据库310合作对照已在服务器112处保存或可由服务器112从别处访问的PMSI值检查所接收的PMSI，以标识与所接收的PMSI相对应的特定UE 102，例如如上文关于图5的动作508所描述的。

[0098] 在步骤636，在发现匹配之后，服务器112对位于数据库310中或可由服务器112从别处访问的、与所接收的PMSI相关联的PMSI跟踪索引进行递增。PMSI跟踪索引由服务器112保存并保持与UE的PMSI记录相关联。PMSI跟踪索引使得服务器112能够基于在UE 102与服务器112之间商定的初始PMSI来计算UE 102的PMSI的任何迭代，如上文所描述的。这种用于得出PMSI值的任何迭代的能力还使得服务器112能够实现各种计账和计费目的。服务器112还使用PMSI跟踪索引来解决以下情形：其中，在由服务器112推导的可能的下一个PMSI值与已在服务器112处保存的用于另一个UE 102的另一个PMSI值之间发生冲突。在一个实施例中，举例而言，可以将PMSI跟踪索引递增值1。

[0099] 在步骤638，服务器112例如，处理器302与PMSI模块308合作推导下一个PMSI。服务器112可以基于在步骤632处在认证信息请求中接收的当前PMSI以及来自步骤636的递增的PMSI跟踪索引来推导下一个PMSI，例如如上文参照图5中的动作508所描述的。类似地，服务器可以基于初始PMSI和PMSI跟踪索引值来推导下一个PMSI。

[0100] 在决定步骤640，服务器112对照其它已知的PMSI值检查在步骤638处推导的下一个PMSI，以验证不存在与任何其它UE的PMSI的冲突。如果存在冲突，则方法630行进回到步骤636，其中在步骤636再次递增PMSI跟踪索引，并且随后在步骤638利用新的PMSI跟踪索引值来推导下一个PMSI。

[0101] 返回到决定步骤640，如果不存在冲突，则方法630行进到步骤642。在步骤642，服务器112对下一个PMSI和递增的PMSI跟踪值进行加密，例如如上文参照图5中的动作508所描述的。如图5中所论述的，可以将经加密的下一个PMSI和PMSI跟踪索引值与认证信息响应连同认证向量包括在一起。

[0102] 在步骤644，服务器112向MME 106发送包括经加密的下一个PMSI和PMSI跟踪索引值的认证信息响应。随后，MME 106可以参与与UE 102的相互认证。作为该相互认证的一部分，MME 106可以发送经加密的下一个PMSI和PMSI跟踪索引值而无需在MME 106处已解密该信息。

[0103] 在UE 102确认下一个PMSI值之后，例如根据图6A的步骤608-616中的一个或多个步骤，方法600行进到步骤646。在步骤646，一旦UE 102确认了下一个PMSI值或者以其它方式完成了同步例如，通过发送新建议的下一个PMSI值、请求新的下一个PMSI值、或调整其本地PMSI跟踪索引以反映所接收和解密的PMSI跟踪索引的值，服务器112经由MME 106从UE

102接收认证令牌。作为响应，服务器112随后更新其PMSI信息例如，服务器112更新先前的PMSI以反映当前PMSI值在当前附着过程中使用的PMSI并且更新当前PMSI以反映同步的下一个PMSI值。如将认识到的，UE 102和服务网络108可以继续建立通信会话。

[0104] 现在转到图7A，根据本公开内容的各个方面，流程图示出了用于关于UE的PMSI初始化的示例性方法700。可以在与基站104和MME 106相通信的UE 102中实现方法700。出于简化讨论起见，将参照单个UE 102来描述方法700，但是将认识到的，本文所描述的方面可以适用于多个UE 102。应当理解，可以在方法700的步骤之前、期间和之后提供额外的步骤，并且对于方法700的其它实施例来说可以替换或消除所描述的步骤中的一些步骤。

[0105] 在步骤702，UE 102开始初始化过程。这可以发生在供应provisioningUE102的时候例如，利用根据本公开内容的方面的IMSI和PMSI值对UE 102的SIM卡进行编程或者稍后的时间。

[0106] 在决定步骤704，UE 102确定其是否已具有在供应的时候被初始化的PMSI。这可以例如在处理器202、存储器204和PMSI模块208之间的合作下完成。如果PMSI已被初始化，则方法700行进到步骤716，其中在步骤716，存储初始PMSI并且PMSI初始化方法700结束。如果PMSI尚未被初始化，则方法700行进到步骤706。

[0107] 在步骤706，处理器202和PMSI模块208一起合作并生成建议的初始PMSI。该建议的初始PMSI可以基于各种因素。在一个实施例中，该建议的初始PMSI可以基于UE 102的IMSI，例如基于结合随机数或伪随机数的一个或多个散列函数和/或迭代。在另一个实施例中，PMSI未基于UE 102的IMSI，而是基于随机数或伪随机数仅举几个例子，使得任何窃听者将无法根据PMSI来推导IMSI。

[0108] 在步骤708，处理器202和PMSI模块208一起合作并对在步骤706处生成的该建议的初始PMSI进行加密。在一个实施例中，PMSI是使用服务器112在先前一些时间与UE 102共享的公钥来加密的。服务器112具有用于在接收时对PMSI进行解密的相应私钥。

[0109] 在步骤710，UE 102例如经由基站104和/或MME 106，经由收发机210向服务器112发送经加密的PMSI。

[0110] 在步骤712，UE 102经由收发机210从服务器112接收用于确认对建议的初始PMSI的接收的响应。

[0111] 在决定步骤714，处理器202和PMSI模块208一起合作并确定从服务器112接收的响应是否指示服务器112接受了建议的初始PMSI。如果该响应指示服务器112接受了建议的初始PMSI，则方法700行进到步骤716，其中在步骤716，存储初始PMSI并且方法700结束。如果该响应指示服务器112没有接受建议的初始PMSI，则方法700返回到步骤706以生成与刚被拒绝的该建议的初始PMSI不同的、新的建议的初始PMSI。例如当存在该PMSI与例如，在服务器112的数据库310中已存储的、另一个关联的UE的任何其它PMSI之间的冲突时，该建议的初始PMSI可能被拒绝。

[0112] 方法700可以重复进行直到得出UE 102和服务器112均同意的PMSI为止。在替代的实施例中，如果在决定步骤714处UE 102确定服务器112没有接受建议的初始PMSI，则UE 102还可以查看来自服务器112的响应与步骤712处相同或不同的响应，以标识服务器112是否针对UE 102发送其自身建议的初始PMSI。在该实施例中，UE 102可以检查来自服务器112的该建议的初始PMSI以确定其对于UE 102是否是可接受的。不出任何问题的话，UE 102可

以接受来自服务器112的该建议的初始PMSI并且向服务器112通知该接受。一旦商定了初始PMSI，就在UE 102处存储该初始PMSI以供后续使用，并且方法700在步骤716处结束。

[0113] 图7B是根据本公开内容的各个方面，示出了用于关于服务器的使用PMSI的附着过程的示例性方法720的流程图。出于简化讨论起见，将关于单个服务器112和单个UE 102来描述方法720，但是将认识到的，本文所描述的方面可以适用于任意数量的服务器112和/或UE 102。应当理解，可以在方法720的步骤之前、期间和之后提供额外的步骤，并且对于方法720的其它实施例来说可以替换或消除所描述的步骤中的一些步骤。

[0114] 在步骤722，服务器112例如经由收发机312从UE 102接收经加密的、建议的初始PMSI。

[0115] 在步骤724，例如通过处理器302、存储器304和PMSI模块308相合作，服务器112解密所接收的PMSI。在一个实施例中，所接收的PMSI是利用UE 102处的公钥其与在服务器112处保持的私钥或用于服务器112的私钥相对应来加密的。

[0116] 在步骤726，服务器112将所接收的经解密的PMSI与数据库310处或服务器112处的任何其它数据库中，或在保存用于多个UE的信息并可由服务器112访问的别处已存在的用于其它UE的其它PMSI值进行比较。

[0117] 在步骤728，服务器112确定是否存在在所接收的、建议的初始PMSI与所存储的或以其它方式可由服务器112访问的任何其它PMSI值之间的任何冲突。

[0118] 在决定步骤730，基于在步骤728的确定结果，服务器112决定是否接受该建议的初始PMSI。如果服务器112接受该建议的初始PMSI，则方法720行进到步骤734，其中在步骤734，服务器112向UE 102发送对初始PMSI的接受确认，并且在服务器112处将该初始PMSI存储在数据库310中，使得该初始PMSI与UE 102相关联例如，作为服务器112为UE 102保持的记录的一部分。

[0119] 如果在决定步骤730，服务器112确定其不接受建议的初始PMSI，则方法720行进到步骤732，其中在步骤732，服务器112从UE 102请求新的PMSI，服务器112向UE 102发送请求并等待响应。在替代的实施例中，服务器112可以替代地自己on its own accord生成建议的初始PMSI响应于决定步骤730，并将该建议的初始PMSI与拒绝一起发送给UE 102。

[0120] 信息和信号可以使用多种不同的技术和技艺中的任何技术和技艺来表示。例如，在贯穿上面的描述中可能提及的数据、指令、命令、信息、信号、比特、符号和码片可以用电压、电流、电磁波、磁场或粒子、光场或粒子或者其任意组合来表示。

[0121] 可以利用被设计为执行本文中所描述功能的通用处理器、DSP、ASIC、FPGA或其它可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件或者其任意组合，来实现或执行结合本文公开内容所描述的各种示例性框和模块。通用处理器可以是微处理器，或者，该处理器也可以是任何常规的处理器、控制器、微控制器或者状态机。处理器还可以实现为计算设备的组合例如，DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合，或者任何其它此种结构。

[0122] 本文所描述的功能可以在硬件、由处理器执行的软件、固件、或其任意组合中实现。如果在由处理器执行的软件中实现，则这些功能可以作为一个或多个指令或代码存储在计算机可读介质上或通过其进行传输。其它例子和实现落在本公开内容和所附权利要求书的保护范围内。例如，由于软件的本质，上文所描述的功能可以使用由处理器执行的软

件、硬件、固件、硬连线、或任意这些部件的组合来实现。用于实现功能的特征还可以物理地位于各种位置，包括被分布为使得在不同的物理位置处实现功能的一部分。此外，如本文所使用的包括在权利要求书中，如在项目列表例如，以诸如“中的至少一个”或“中的一个或多个”之类的短语为结束的项目列表中所使用的“或”指示包含性列表，使得例如列表[A、B或C中的至少一个]意指A或B或C或AB或AC或BC或ABC即，A和B和C。

[0123] 本公开内容的实施例包括一种用户设备UE，所述UE包括：用于利用初始附着消息，向服务网络发送私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE的单元；用于从所述服务网络接收认证请求的单元，所述认证请求包括由与所述服务网络进行通信的服务器确定的下一个PMSI，所述下一个PMSI是根据所述PMSI来推导出的；以及用于经由所述服务网络向所述服务器发送对所述下一个PMSI的接收确认的单元。

[0124] 所述UE还包括：用于根据先前的PMSI来推导所述PMSI的单元，其中，所述先前的PMSI包括初始PMSI。所述UE还包括：用于根据先前的PMSI来推导所述PMSI的单元，其中，所述先前的PMSI包括根据初始PMSI来推导的PMSI值。所述UE还包括：用于由所述UE基于初始PMSI来确定用于网络接入的所述PMSI的单元。所述UE还包括：用于在所述UE向所述服务器进行用户注册的期间，接收所述初始PMSI的单元。所述UE还包括：用于在经由空中通信向所述服务器进行用户注册之后，供应所述初始PMSI的单元。所述UE还包括：用于生成建议的PMSI的单元；用于使用服务器公钥来加密所生成的PMSI的单元，其中，所述服务器保存相应的服务器私钥；以及用于从所述服务器接收要使用所生成的PMSI作为所述初始PMSI的确认的单元。所述UE还包括：用于确定基于UE的下一个PMSI的单元；以及用于将所述基于UE的下一个PMSI与作为所述认证请求的一部分而接收的所述下一个PMSI进行比较，以确定是否存在匹配的单元。所述UE还包括：用于响应于确定存在匹配，生成确认令牌的单元，所述接收确认包括所述确认令牌；以及用于在所述UE处存储所确认的下一个PMSI以用于下一个附着消息中的单元。所述UE还包括：用于使用匿名密钥来解密所述认证请求中的所述下一个PMSI的单元，其中，所述匿名密钥是根据在所述UE与所述服务器之间共享的秘密密钥来推导出的。

[0125] 本公开内容的实施例还包括一种服务器，所述服务器包括：用于经由中间服务网络中的一个或多个网络单元，通过初始附着消息来从用户设备UE接收私密性移动用户身份PMSI，以替代国际移动用户身份IMSI来标识所述UE的单元；用于由所述服务器基于所述PMSI来确定下一个PMSI的单元；用于从所述服务器向所述服务网络发送包括所述下一个PMSI的认证信息的单元，其中，作为认证的一部分，所述下一个PMSI由所述服务网络中继给所述UE；以及用于经由所述服务网络从所述UE接收包括对所述下一个PMSI的确认的接收确认的单元。

[0126] 所述服务器还包括：用于根据先前的PMSI来推导所述下一个PMSI的单元，其中，所述先前的PMSI包括初始PMSI。所述服务器还包括：用于根据先前的PMSI来推导所述下一个PMSI的单元，其中，所述先前的PMSI包括根据初始PMSI来推导的PMSI值。所述服务器还包括：用于由所述服务器基于初始PMSI来确定用于网络接入的所述PMSI的单元。所述服务器还包括：用于在所述服务器处，在所述UE向所述服务器进行用户注册的期间接收所述初始PMSI的单元。所述服务器还包括：用于从所述UE接收建议的初始PMSI的单元；用于由所述服务器使用服务器私钥来解密在所述UE处通过相应的服务器公钥来加密的所述建议的初始

PMSI的单元;以及用于向所述UE发送将所述建议的初始PMSI作为所述初始PMSI的确认的单元。所述服务器还包括:用于根据在所述服务器与所述UE之间共享的秘密密钥来推导匿名密钥的单元;用于使用所推导的匿名密钥来加密所述认证信息中的所述下一个PMSI的单元;用于作为所述确认的一部分,接收对所述下一个PMSI进行确认的确认令牌的单元;以及用于在所述服务器处存储所述下一个PMSI以替代所述PMSI,以用于响应来自所述UE的后续初始附着消息的单元。所述服务器还包括:用于检测所述下一个PMSI与关联于不同的UE的另一个现有PMSI之间的冲突的单元;以及用于对PMSI索引进行递增,并且基于所述下一个PMSI和经递增的PMSI索引来确定新的下一个PMSI的单元。所述服务器还包括:用于从与所述服务器所位于的归属网络分开的所述服务网络上的移动性管理实体MME接收针对所述UE的所述IMSI的请求的单元;以及用于响应于所述请求,发送在所述初始附着消息中所使用的、所述UE的所述PMSI而不是所述UE的所述IMSI的单元。所述服务器还包括:用于针对对利用所述初始附着消息包括的所述PMSI的匹配,搜索一个或多个数据库的单元;以及用于响应于没有定位到匹配,发送针对所述UE的通知来修改在所述UE处保存的PMSI索引以便在所述UE处生成经更新的PMSI的单元。

[0127] 本公开内容的实施例还包括一种用于由用户设备UE进行的网络接入的方法,所述方法包括:由所述UE确定在服务网络处进行附着;以及从所述UE向所述服务网络发送初始附着消息,所述初始附着消息包括临时标识符ID以替代用于所述UE的永久ID,其中,基于所述临时ID来建立与所述服务网络的认证服务器HSS的安全上下文。

[0128] 所述方法还包括:从所述服务网络的所述HSS接收认证请求,所述认证请求包括由所述HSS确定的下一个临时ID,所述下一个临时ID是根据所述初始附着消息中所包括的所述临时ID来推导出的。所述方法还包括:从所述UE经由所述服务网络向所述HSS发送对所述下一个临时ID的接收确认。

[0129] 本公开内容的实施例还包括一种用户设备,所述用户设备包括:存储器,其被配置为存储临时标识符ID;处理器,其被配置为确定在服务网络处进行附着;以及收发机,其被配置为向所述服务网络发送初始附着消息,所述初始附着消息包括临时ID以替代用于所述UE的永久ID,其中,与所述服务网络的认证服务器HSS的安全上下文是基于所述临时ID来建立的。

[0130] 所述UE还包括:其中,所述收发机还被配置为从所述服务网络的所述HSS接收认证请求,所述认证请求包括由所述HSS确定的下一个临时ID,所述下一个临时ID是根据所述初始附着消息中所包括的所述临时ID来推导出的。所述UE还包括:其中,所述处理器还被配置为生成接收确认,并且所述收发机还被配置为经由所述服务网络向所述HSS发送所述接收确认。

[0131] 本公开内容的实施例还包括一种用于与网络上的服务器建立网络接入的方法,所述方法包括:经由服务网络从用户设备UE接收初始附着消息,所述初始附着消息包括临时标识符ID以替代用于所述UE的永久ID;以及基于所述临时ID来建立安全上下文。

[0132] 所述方法还包括:基于所述初始附着消息中所包括的所述临时ID来确定下一个临时ID。所述方法还包括:作为认证的一部分,从所述服务器经由所述服务网络向所述UE发送包括所述下一个临时ID的认证信息。所述方法还包括:经由所述服务网络从所述UE接收包括对所述下一个临时ID的确认的接收确认。

[0133] 本公开内容的实施例还包括一种服务器，所述服务器包括：收发机，其被配置为经由服务网络从用户设备UE接收初始附着消息，所述初始附着消息包括临时标识符ID以替代用于所述UE的永久ID；以及处理器，其被配置为基于所述临时ID来建立安全上下文。

[0134] 所述服务器还包括：其中，所述处理器还被配置为基于所述初始附着消息中所包括的所述临时ID来确定下一个临时ID。所述服务器还包括：其中，所述收发机还被配置为：作为认证的一部分，经由所述服务网络向所述UE发送包括所述下一个临时ID的认证信息。所述服务器还包括：其中，所述收发机还被配置为经由所述服务网络从所述UE接收包括对所述下一个临时ID的确认的接收确认。

[0135] 如本领域技术人员到目前为止将意识到的，并且取决于手边的特定应用，可以在使用本公开内容的设备的材料、装置、配置和方法中或对使用本公开内容的设备的材料、装置、配置和方法进行许多种修改、替换和变更。鉴于这一点，本公开内容的范围不应受限于本文示出和描述的特定实施例，因为这些特定实施例是仅通过其一些例子来举例说明的，而是相反地，该范围应与所附权利要求书及其功能等同物的范围完全相称。

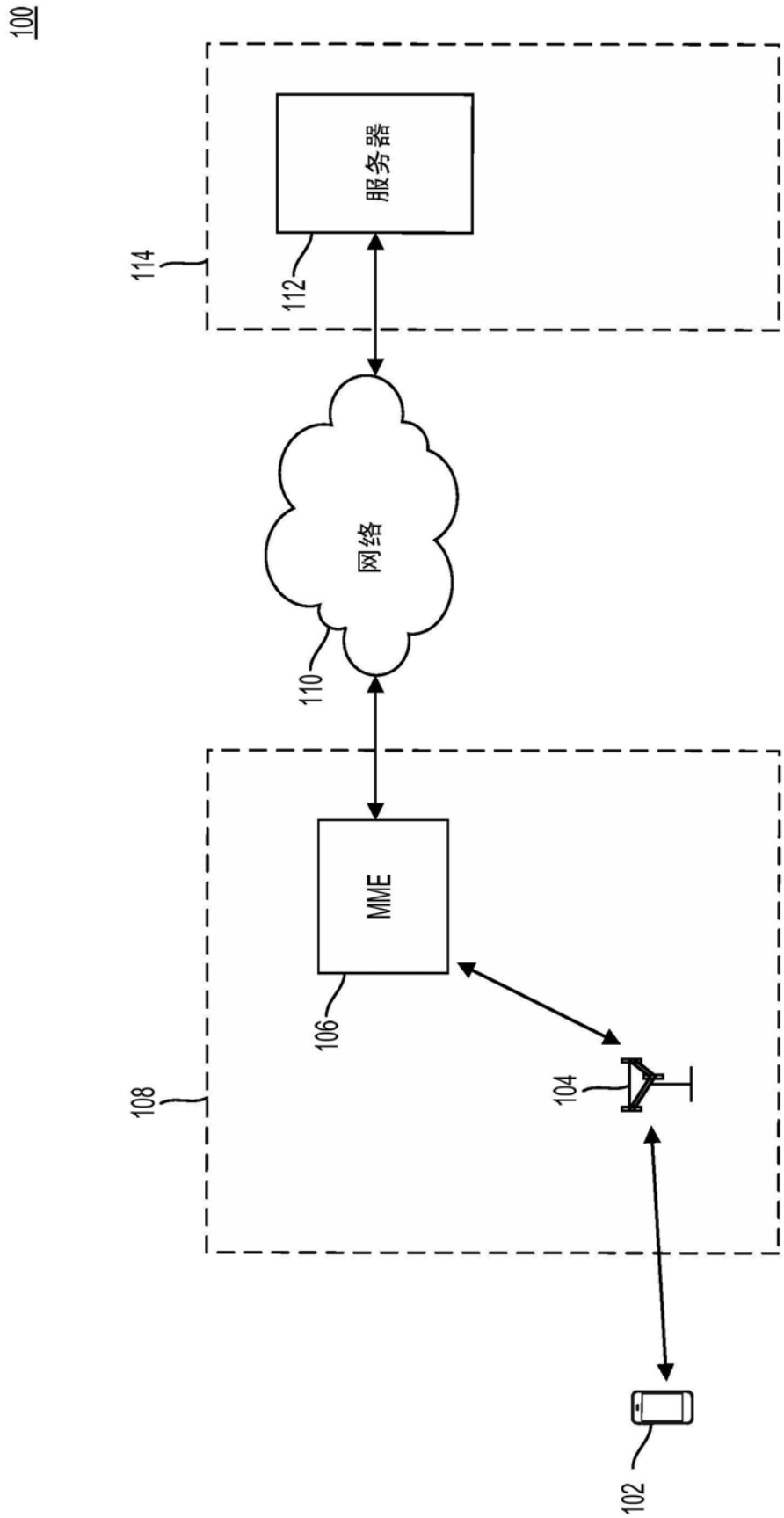


图1

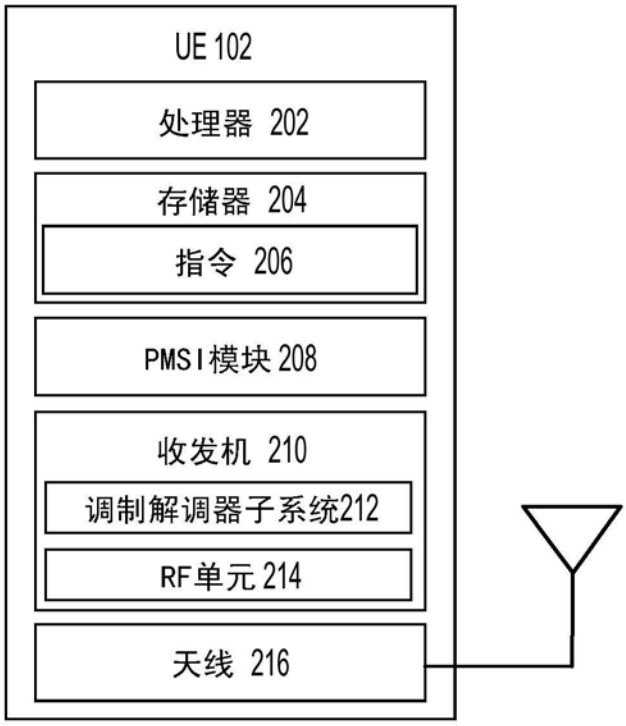

UE 102
处理器 202
存储器 204
指令 206
PMSI模块 208
收发机 210
调制解调器子系统212
RF单元 214
天线 216

图2


服务器 112
处理器 302
存储器 304
指令 306
PMSI模块 308
数据库 310
收发机 312

图3

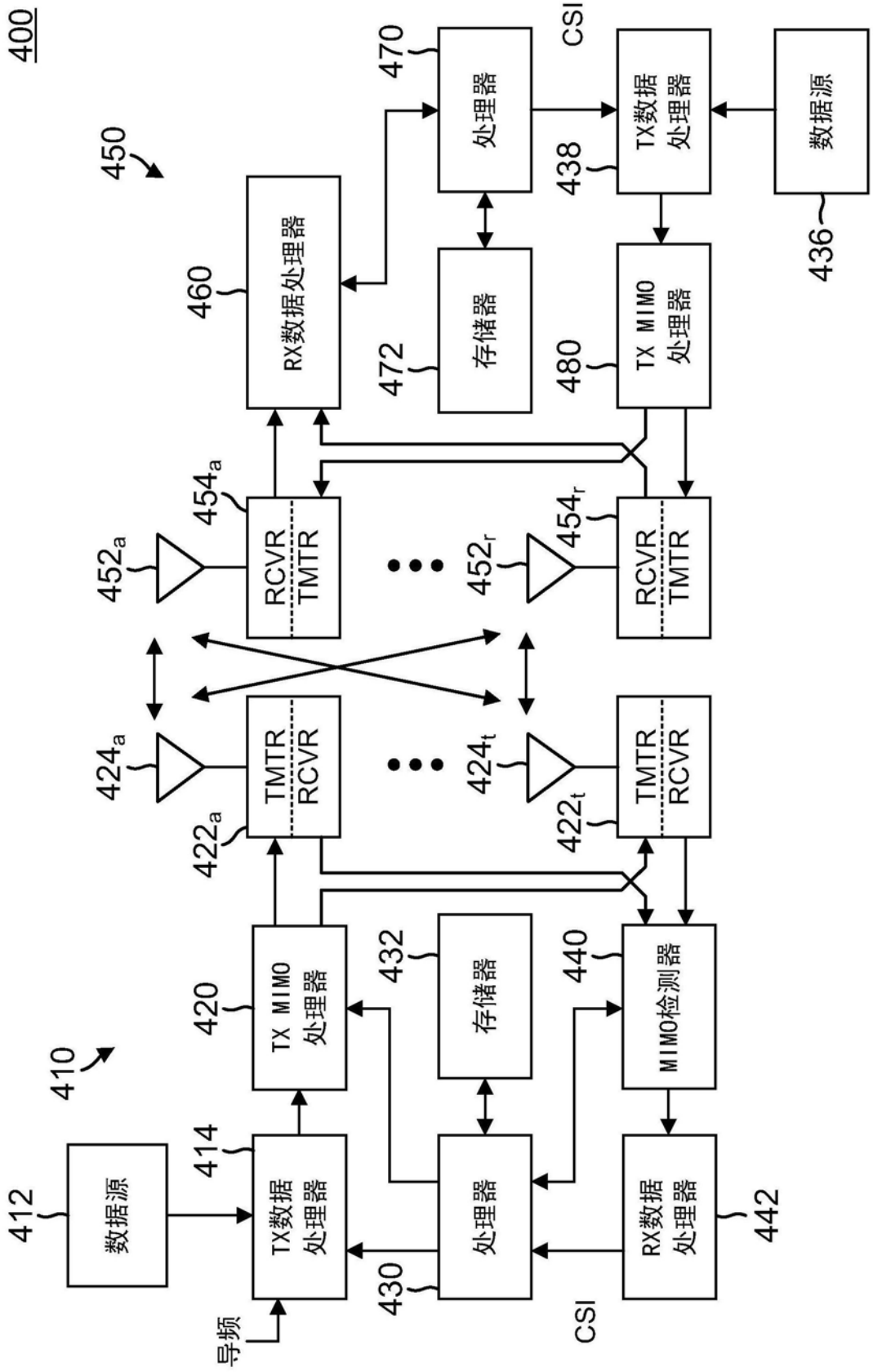

400
450
460
RX数据处理器
470
处理器
CSI
438
TX数据处理器
数据源
436
472
存储器
480
TX MIMO处理器
454a
RCVR
TMTR
452a
452r
454r
424a
TMTR
RCVR
424t
422a
422t
410
420
TX MIMO处理器
432
存储器
440
MIMO检测器
412
数据源
414
TX数据处理器
处理器
RX数据处理器
442
430
导频
CSI

图4

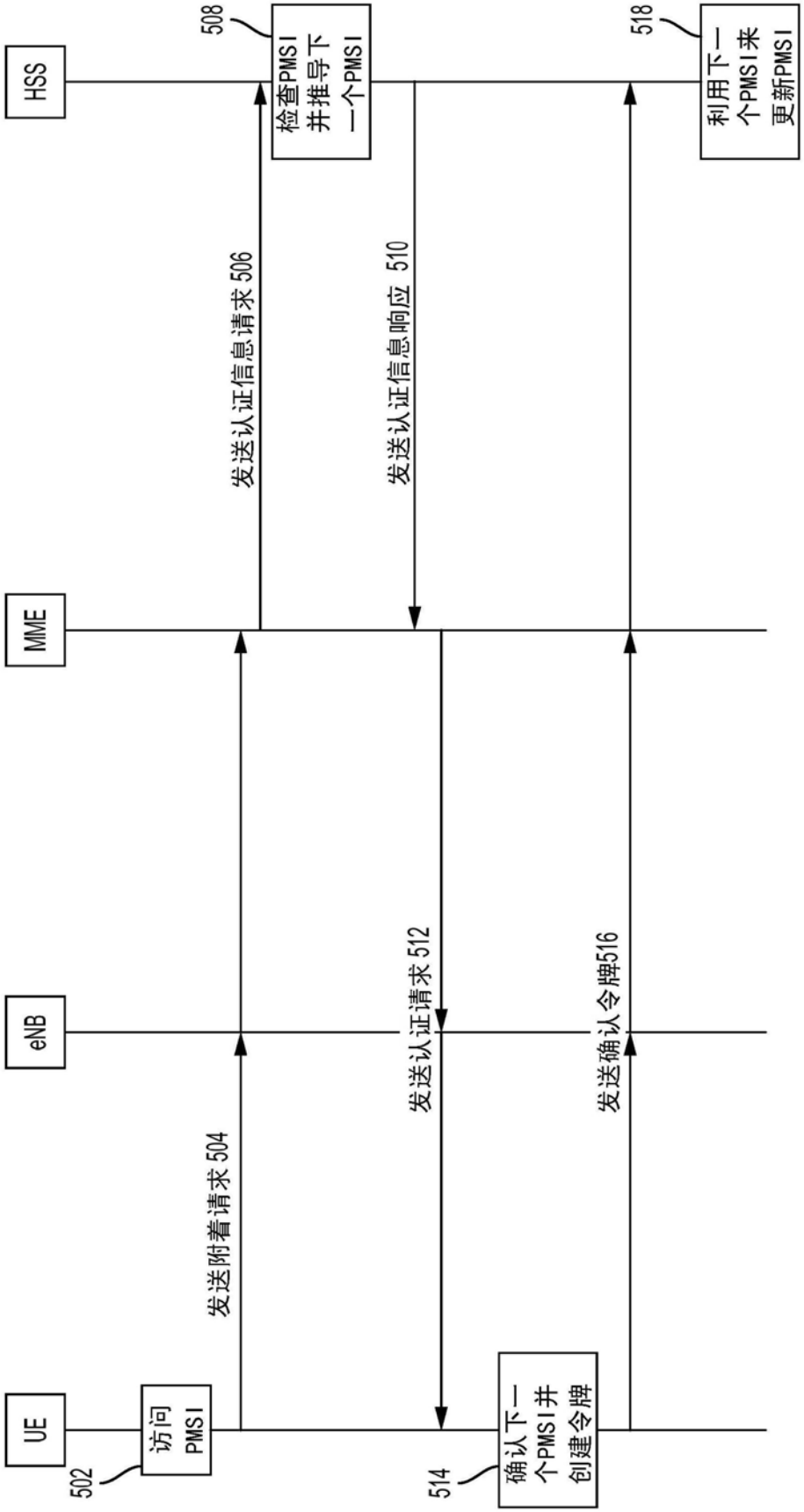

HSS
MME
eNB
UE
508
检查PMSI并推导下一个PMSI
518
利用下一个PMSI来更新PMSI
发送认证信息请求 506
发送认证信息响应 510
发送认证请求 512
发送确认令牌516
发送附着请求 504
访问PMSI
502
确认下一个PMSI并创建令牌
514

图5

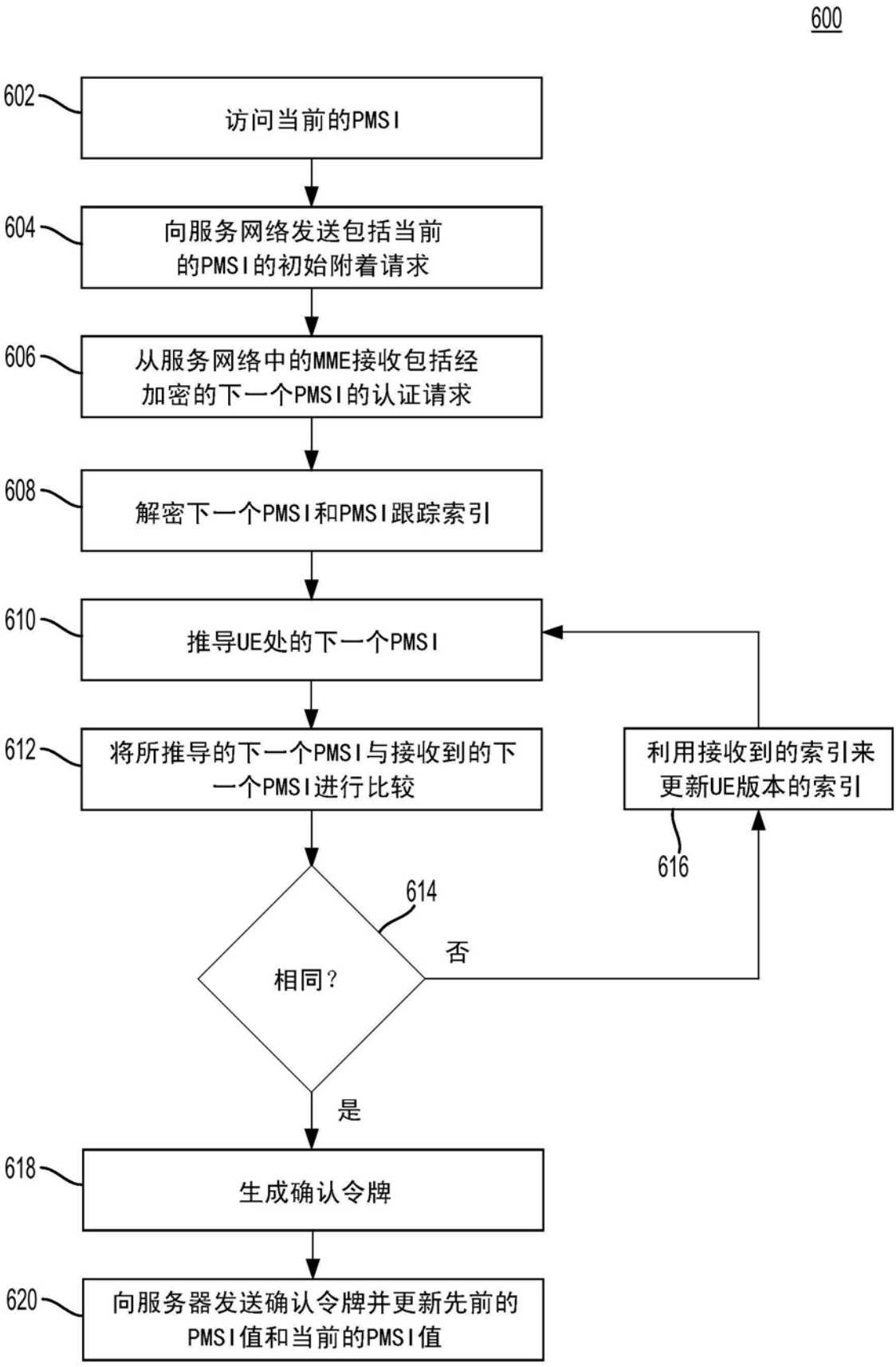

600
602
访问当前的PMSI
604
向服务网络发送包括当前的PMSI的初始附着请求
606
从服务网络中的MME接收包括经加密的下一个PMSI的认证请求
608
解密下一个PMSI和PMSI跟踪索引
610
推导UE处的下一个PMSI
612
将所推导的下一个PMSI与接收到的下一个PMSI进行比较
614
相同?
否
是
616
利用接收到的索引来更新UE版本的索引
618
生成确认令牌
620
向服务器发送确认令牌并更新先前的PMSI值和当前的PMSI值

图6A

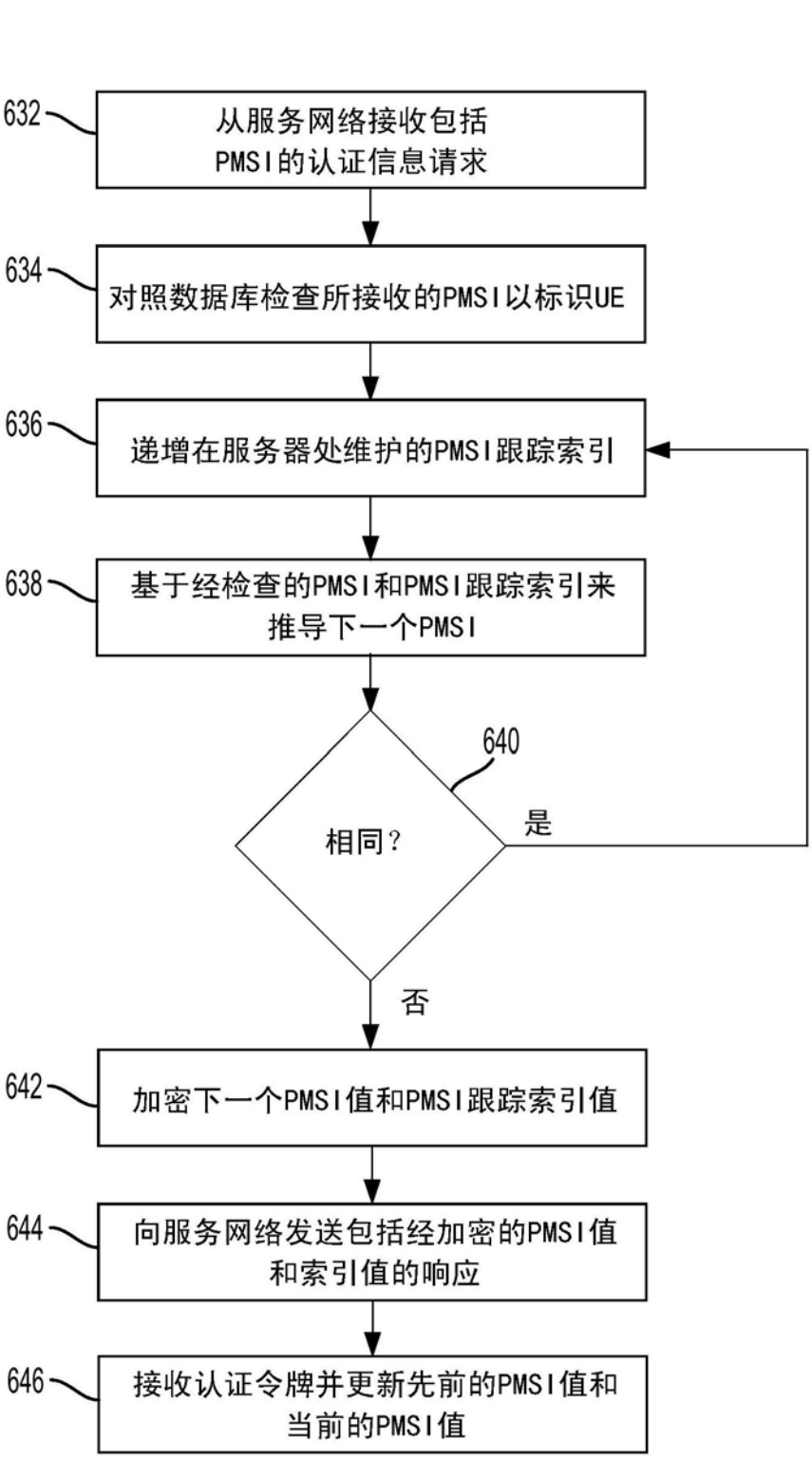

630
632
从服务网络接收包括PMSI的认证信息请求
634
对照数据库检查所接收的PMSI以标识UE
636
递增在服务器处维护的PMSI跟踪索引
638
基于经检查的PMSI和PMSI跟踪索引来推导下一个PMSI
640
相同?
是
否
642
加密下一个PMSI值和PMSI跟踪索引值
644
向服务网络发送包括经加密的PMSI值和索引值的响应
646
接收认证令牌并更新先前的PMSI值和当前的PMSI值

图6B

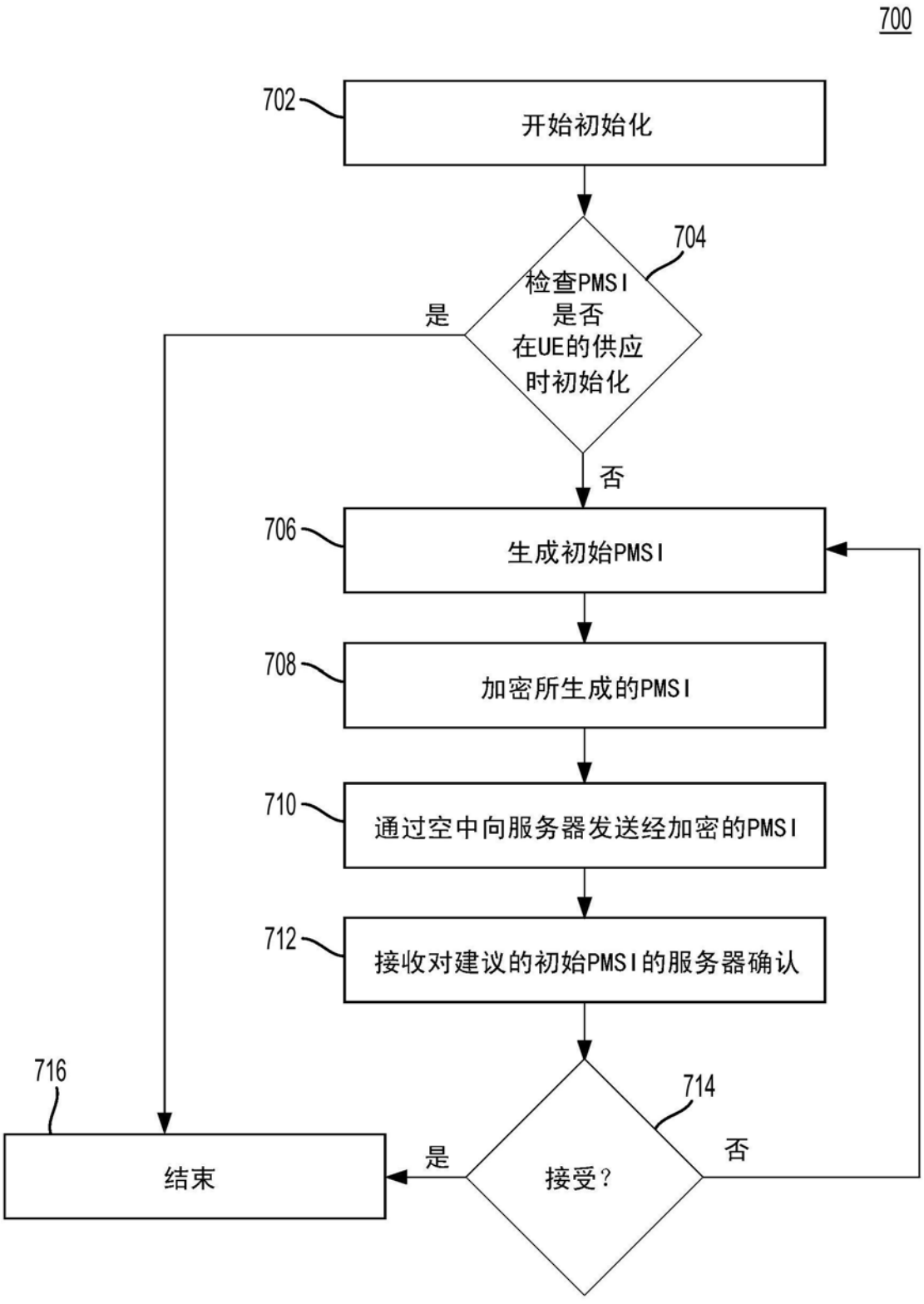

700
702
开始初始化
704
检查PMSI是否在UE的供应时初始化
是
否
706
生成初始PMSI
708
加密所生成的PMSI
710
通过空中向服务器发送经加密的PMSI
712
接收对建议的初始PMSI的服务器确认
714
接受?
是
否
716
结束

图7A

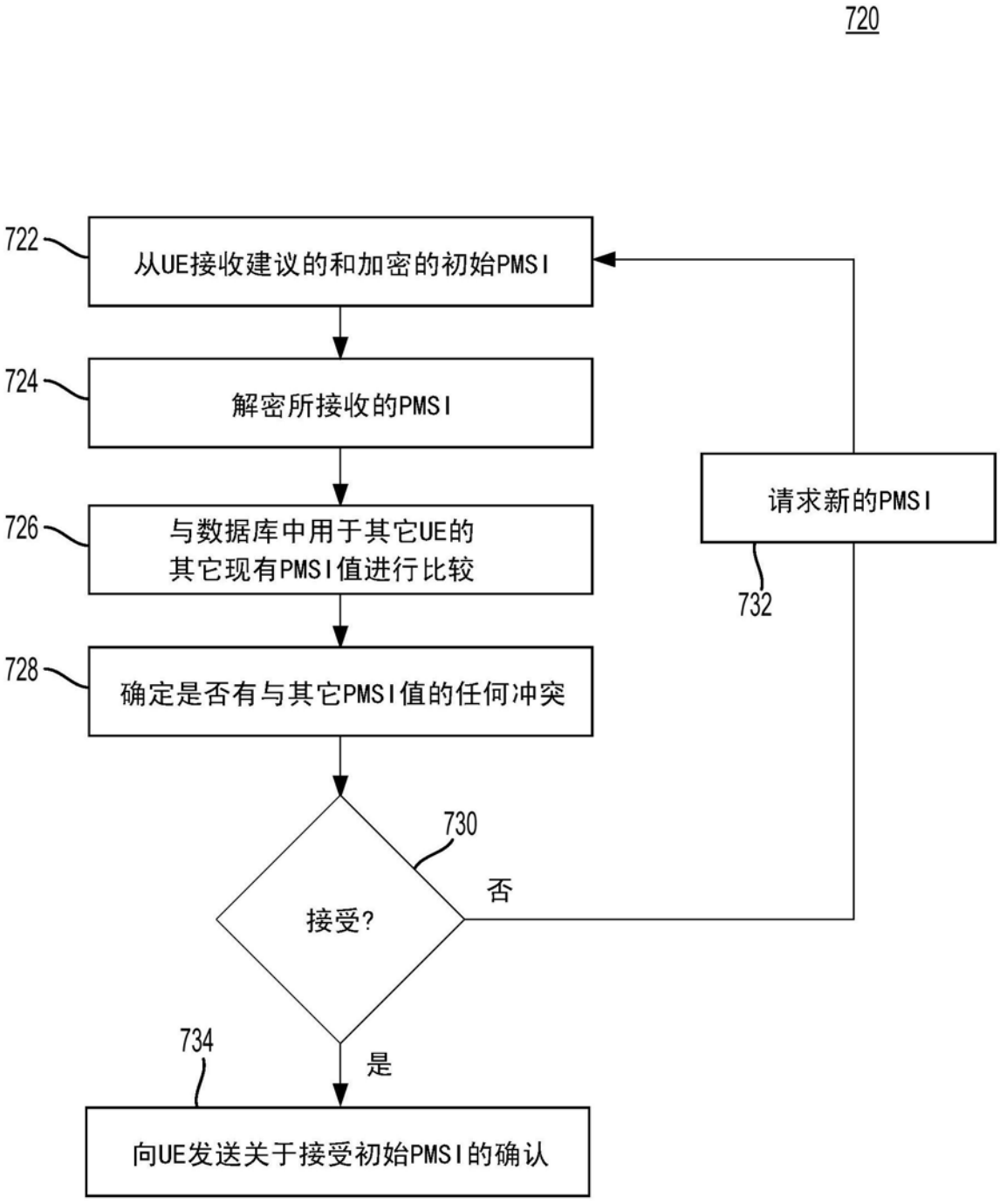

720
722
从UE接收建议的和加密的初始PMSI
724
解密所接收的PMSI
726
与数据库中用于其它UE的
其它现有PMSI值进行比较
728
确定是否有与其它PMSI值的任何冲突
730
接受?
否
是
732
请求新的PMSI
734
向UE发送关于接受初始PMSI的确认

图7B