(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 103535010 B
(45)授权公告日 2016.10.26

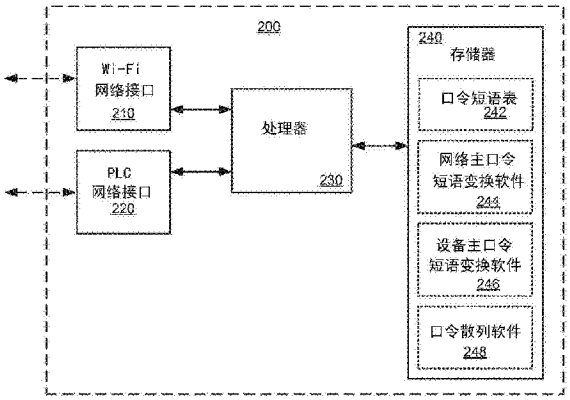
(21)申请号 201280022195.9
(22)申请日 2012.03.14
(65)同一申请的已公布的文献号
申请公布号 CN 103535010 A
(43)申请公布日 2014.01.22
(30)优先权数据
61/452,317 2011.03.14 US
13/420,420 2012.03.14 US
(85)PCT国际申请进入国家阶段日
2013.11.06
(86)PCT国际申请的申请数据
PCT/US2012/029117 2012.03.14
(87)PCT国际申请的公布数据
WO2012/125758 EN 2012.09.20
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 R·E·纽曼 S·B·施鲁姆
L·W·央格三世
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 李小芳
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/04(2006.01)
H04W 12/06(2006.01)
(56)对比文件
CN 1905446 A,2007.01.31,
US 2005071645 A1,2005.03.31,
CN 101292437 A,2008.10.22,
US 2010281249 A1,2010.11.04,
US 6947736 B2,2005.09.20,
审查员 冷静
权利要求书2页 说明书12页 附图8页

(54)发明名称

混合联网主口令短语

(57)摘要

提供了一种为包括配置成在一种或多种通信介质上通信的多个网络接口的混合网络提供基于口令短语的安全性建立的方法和装置。该方法包括在该多个网络接口中的一网络接口处从用户接收口令短语。接收到的口令短语随后被用于为一个或多个网络接口认证该设备。可执行该认证而不管这些网络接口所使用的通信介质为何。



CN 103535010 B

1.一种具有分别根据第一通信协议和第二通信协议进行操作的第一子网络和第二子网络的混合网络，其中所述第一和第二通信协议是不同的并且选自于HomePlug协议和无线局域网(WLAN)协议，所述混合网络包括第一设备，所述第一设备包括：

所述第一通信协议的第一网络接口；

第一处理器；以及

第一存储器，其耦合至所述第一处理器并且其中存储有第一计算机可执行指令，所述第一计算机可执行指令在由所述第一处理器执行时使所述第一设备：

从用户接收主口令短语；

通过响应于所述第一通信协议选择性地截断、添加、或替换所述主口令短语的字符以生成第一口令来将所述主口令短语变换成顺应所述第一通信协议的所述第一口令；

使用所述第一口令向所述第一子网络认证所述第一设备；

对所述第一口令进行散列，以导出顺应所述第一通信协议的第一密钥；以及

使用所述第一密钥将所述第一设备加入所述第一子网络。

2.如权利要求1所述的混合网络，其特征在于，还包括第二设备，所述第二设备包括：

所述第二通信协议的第二网络接口；

第二处理器；以及

第二存储器，其耦合至所述第二处理器并且其中存储有第二计算机可执行指令，所述第二计算机可执行指令在由所述第二处理器执行时使所述第二设备：

从所述用户接收所述主口令短语；

通过响应于所述第二通信协议选择性地截断、添加、或替换所述主口令短语的字符以生成第二口令来将所述主口令短语变换成顺应所述第二通信协议的所述第二口令；

使用所述第二口令向所述第二子网络认证所述第二设备；

对所述第二口令进行散列，以导出顺应所述第二通信协议的第二密钥；以及

使用所述第二密钥将所述第二设备加入所述第二子网络。

3.如权利要求1所述的混合网络，其特征在于，所述第一存储器中存储有附加计算机可执行指令，所述附加计算机可执行指令在由所述第一处理器执行时使所述第一设备：

将所述主口令短语从所述第一设备传送给具有所述第一通信协议或所述第二通信协议的网络接口的第三设备。

4.一种向混合网络添加数个设备的方法，所述混合网络具有分别根据第一通信协议和第二通信协议进行操作的第一子网络和第二子网络，其中所述第一和第二通信协议是不同的并且选自于HomePlug协议和无线局域网(WLAN)协议，所述方法包括：

将主口令短语输入到第一设备中，其中所述第一设备包括所述第一通信协议的第一网络接口；

在所述第一设备中使用第一变换操作来变换所述主口令短语以生成顺应所述第一通信协议的第一口令，其中所述第一变换操作包括响应于所述第一通信协议选择性地截断、添加、或替换所述主口令短语的字符以生成所述第一口令；

使用所述第一口令向所述第一子网络认证所述第一设备；

对所述第一口令进行散列，以导出顺应所述第一通信协议的第一密钥；以及

使用所述第一密钥将所述第一设备加入所述第一子网络。

5.如权利要求4所述的方法，其特征在于，进一步包括：

在经加密消息中将所述主口令短语从所述第一设备发送给第三设备。

6.如权利要求4所述的方法，其特征在于，进一步包括：

将主口令短语输入到第二设备中，其中所述第二设备包括所述第二通信协议的第二网络接口；

在所述第二设备中使用第二变换操作来变换所述主口令短语以生成顺应所述第二通信协议的第二口令，其中所述第二变换操作包括响应于所述第二通信协议选择性地截断、添加、或替换所述主口令短语的字符以生成所述第二口令；

使用所述第二口令向所述第二子网络认证所述第二设备；

对所述第二口令进行散列，以导出顺应所述第二通信协议的第二密钥；以及

使用所述第二密钥将所述第二设备加入所述第二子网络。

7.如权利要求6所述的方法，其特征在于，进一步包括：

将所述主口令短语从所述第一设备传送给具有所述第一和第二通信协议的网络接口的第三设备，其中所述第三设备用于使用所述第二变换操作来变换所述主口令短语，以在所述第三设备中生成所述第二口令。

8.如权利要求7所述的方法，其特征在于，所述第三设备用于：

对所述第二口令进行散列以导出所述第二密钥；以及

使用所述第二密钥将所述第三设备加入所述混合网络。

9.如权利要求4所述的方法，其特征在于，进一步包括：

在作为所述混合网络的现有成员的第三设备中选择先前被用于将所述第三设备加入所述混合网络的第三口令；以及

在所述第三设备中使用逆变换操作从所述第三口令导出所述主口令短语。

10.如权利要求4所述的方法，其特征在于，进一步包括：

在具有所述第一通信协议的网络接口的第三设备中代表不执行所述变换操作的第四设备导出所述主口令短语。

混合联网主口令短语

技术领域

[0001] 本发明各实施例一般涉及网络技术，尤其涉及混合联网解决方案。

[0002] 相关技术背景

[0003] 服务提供商和消费者越来越希望将高质量数字编码内容(例如，数据、语音、和视频)分发给固定设备和移动设备两者，并且通过这些设备来实现和控制丰富的内容相关服务集合。然而，目前不存在能实现此类内容相关服务同时还允许以用户友好的方式来创建和/或修改具有根据不同网络技术进行操作的多个设备的混合网络的整合网络解决方案。

[0004] 可无线地和/或在硬连线连接上操作的现有混合网络通常纳入基于各种不同的联网标准的多种网络技术(例如，Wi-Fi、HomePlug AV、和以太网)。通常情况下，这些不同网络技术的配置、操作、和通信协议是由不同群体创建的，并且因此可能有所不同。更具体地，不仅与Wi-Fi、HomePlug AV、和以太网系统相关联的网络连接建立规程(例如，用于创建新网络、将设备添加到现有网络、发现所连接设备、桥接到其他设备/网络、等等)是彼此不同的，而且在不使用桥接设备和/或复杂的连接建立操作的情况下，根据这些标准中的一种标准进行操作的设备通常难以连接到根据这些标准中的另一标准进行操作的设备(并由此难以与之通信)。从用户立场而言，期望具有用于建立和/或修改采用众多不同联网技术的混合网络的单个简化机制。还期望混合网络作为以对用户完全透明的方式整合不同网络技术的单个无缝网络来起作用。

[0005] 通常情况下，联网技术包括用于防止未获授权设备与获授权设备形成网络、加入现有网络、以及解码在该网络上发送的数据的安全机制。Wi-Fi和HomePlug AV是支持这些类型的安全机制的网络通信技术或协议的示例。

[0006] 用于防止未获授权设备形成或加入网络的一种技术是要求各设备证明它们拥有对于加入方设备以及向网络认证该加入方设备的设备两者已知的机密的安全密钥(例如，“预共享密钥”)或口令。此类安全密钥可与单个设备相关联(例如，设备密钥)或者可与网络相关联并且为该网络中的所有设备所已知的(例如，网络密钥)。

[0007] 用于加密用户数据以保护该数据免于被未获授权设备解码的安全密钥可在认证过程期间生成。确保加入方设备和认证方设备拥有相同安全密钥的常用技术是要求用户在加入方设备和认证方设备两者上输入相同的口令，并且响应于此，加入方设备和认证方设备可生成相同的(例如，预共享的)安全密钥。

[0008] 遗憾的是，口令和安全密钥的细节(例如，可接受长度、格式、和/或有效字符集)在不同网络技术之间通常是有所不同的。例如，虽然HomePlug网络协议可能规定其口令包括第一可允许字符集(例如，可打印的ASCII字符)的第一范围(例如，N到M个实例之间)，但Wi-Fi网络协议可能规定其口令包括第二可允许字符集(例如，全部ASCII字符)的第二范围(例如，X到Y个实例之间)，其中$N \neq X$，$M \neq Y$，并且第一字符集和第二字符集并不相同。另外，HomePlug口令所允许的最小字符数目可能大于Wi-Fi口令所允许的最小字符数目，并且HomePlug口令中所允许的一些字符(例如，字符“[”和“]”)可能在Wi-Fi口令中是不被允许的。因此，当前的混合网络通常要求用户为寻求形成和/或加入混合网络的每种类型的网络

技术设备输入不同的口令和/或密钥，这不仅是累赘的而且还可能要求用户确定每个设备采用哪种类型的网络技术，或者更糟地，要求用户在同一设备上针对不同技术输入不同口令。

[0009] 因此，需要允许用户使用根据不同网络技术进行操作的设备来形成和/或扩展混合网络的简单且统一的认证机制。

[0010] 概述

[0011] 根据本发明各实施例，公开了一种简单且统一的认证机制，其允许用户通过使用单个主口令短语，用根据不同网络技术进行操作的设备来安全地形成和/或扩展混合网络。因此，本发明各实施例通过为具有根据各种不同网络技术或通信协议进行操作的网络接口的设备统一了基于口令的认证和建立操作，而有利地改善了创建和/或修改混合网络时的用户体验。例如，本发明各实施例并非要求用户向使用不同网络技术来通信的诸设备输入数个不同的因技术而异的口令，而是允许单个主口令短语以无缝且高效的方式来认证根据不同网络技术进行操作的各种设备并将其连接至混合网络。另外，本发明各实施例可结合例如Wi-Fi和HomePlug通信协议所支持的各种“简单连接”建立操作来实现。

[0012] 更具体地，根据本发明各实施例的用于使用单个主口令短语将数个设备加入混合网络以促成根据第一和第二通信协议进行数据通信的示例性方法可如下实现。首先，用户将主口令短语输入到具有第一通信协议的第一网络接口的第一设备中，并且将该主口令短语输入到具有第二通信协议的第二网络接口的第二设备中。接下来，在第一设备中使用第一变换操作来变换该主口令短语，以生成顺应第一通信协议的第一口令。在第二设备中使用第二变换操作来变换该主口令短语，以生成顺应第二通信协议的第二口令。此后，第一口令可被用于在第一设备中导出顺应第一通信协议的第一密钥，并且第二口令可被用于在第二设备中导出顺应第二通信协议的第二密钥。这些密钥随后可被用于向混合网络的相应子网络认证第一和第二设备。

[0013] 对于其他实施例，认证过程可涉及根据每个口令旨在用于的通信协议或网络技术进一步将该特定口令变换成合适的密钥。导出的密钥随后可被用于执行作为加入该网络的操作的一部分的认证和密钥分发。

[0014] 以此方式，用户可以能够有利地对整个混合网络使用单个口令短语，由此不仅减轻了要知晓网络中的每个设备采用哪种(些)协议的需要，而且还减轻了要为每种类型的网络接口输入单独口令的需要。此外，如果在另一设备上的第一网络接口中通过经由第一网络技术的安全连接获得了该主口令短语，则该主口令短语可用于认证该另一设备上的第二网络接口，由此消除了要将主口令短语输入到该另一设备中的需要。

[0015] 对于其他实施例，第一和第二设备可根据相同的通信协议进行操作，和/或可包括根据不同通信协议进行操作的多个网络接口。

[0016] 附图简述

[0017] 本发明各实施例作为示例而非限制在附图中解说，并且在附图中相同的参考标号指示相似的元素，并且其中：

[0018] 图1是其中可实现本发明各实施例的混合网络的框图；

[0019] 图2是图1的混合网络的诸设备中的一个示例性设备的框图；

[0020] 图3是描绘根据一些实施例的用于从单个网络主口令短语(NMPP)创建多个因技术

而异的不同网络口令和密钥的示例性操作的解说性流程图；

[0021] 图4是描绘根据一些实施例的用于从单个设备主口令短语(DMPP)创建多个因技术而异的不同设备口令和密钥的示例性操作的解说性流程图；

[0022] 图5是解说根据示例性实施例的在接口设备之间的用于形成网络的消息交换的序列图；

[0023] 图6是解说根据另一示例性实施例的在接口设备之间的用于形成网络的消息交换的序列图；

[0024] 图7是解说根据又一示例性实施例的在接口设备之间的用于将设备加入网络的消息交换的序列图；以及

[0025] 图8是解说根据再一示例性实施例的在接口设备之间的用于将设备加入网络的消息交换的序列图。

[0026] 详细描述

[0027] 公开了用于为混合网络建立安全机制的方法和装置，其允许单个主口令短语创建、认证、和/或添加设备到混合网络，而不管每个设备采用何种网络技术或通信协议来与其他设备通信。在以下描述中，阐述了诸如具体组件、电路、和过程的示例等众多具体细节，以提供对本公开的透彻理解。另外，在以下描述中并且出于解释目的，阐述了具体的命名以提供对本发明各实施例的透彻理解。然而，对于本领域技术人员将明显的是，可以不需要这些具体细节就能实践本发明各实施例。在其他实例中，以框图形式示出公知的电路和设备以避免混淆本公开。如本文所使用的，术语“耦合”意味着直接连接到、或通过一个或多个居间组件或电路来连接。本文所描述的各种总线上所提供的任何信号可以与其他信号进行时间复用并且在一条或多条共用总线上提供。术语“总线”包括有线和无线通信技术两者，而且并不取决于连接到通信介质的设备的数目。另外，各电路元件或软件块之间的互连可被示为总线或单信号线。每条总线可替换地是单信号线，而每条单信号线可替换地是总线，并且单线或总线可表示用于各组件之间的通信的大量物理或逻辑机制中的任一个或多个。本发明各实施例不应被解释为限于本文描述的具体示例，而是在其范围内包括由所附权利要求所限定的所有实施例。

[0028] 如本文所使用的，Wi-Fi设备可经由无线局域网(WLAN)与其他Wi-Fi设备通信。术语Wi-Fi和WLAN可包括由IEEE802.11标准族、蓝牙、HiperLAN(与IEEE802.11标准相当的无线标准集，主要在欧洲使用)、以及具有相对短的无线电传播距离的其他技术来管控的通信。因此，术语“Wi-Fi设备”和“WLAN设备”在本公开中是可互换的，并且都是指具有允许由IEEE802.11标准族、蓝牙、HiperLAN以及具有相对短的无线电传播距离的其他技术来管控的通信的网络接口的设备。

[0029] 此外，术语HomePlug AV(HPAV)是指针对诸如家中TV分发、游戏和因特网接入等应用、以及针对智能电表和针对电气系统和电器之间的家中通信，由HomePlug电力线联盟所开发的标准集合以及由IEEE1901标准组所开发的标准集合(例如，如HomePlug标准族和IEEE1901标准族中所描述的)。HPAV标准在本文也可被称为电力线通信(PLC)标准，其允许现有家用电气布线被用于促成各种家中设备之间的通信和/或用于促成连接到因特网。因此，术语“HomePlug AV设备”、“HPAV设备”和“PLC设备”在本公开中是可互换的，并且都是指具有允许由PLC标准和/或各种HomePlug标准(例如，HomePlug1.0、HomePlug AV、HomePlug

AV2、等等)来管控的通信的网络接口的设备。

[0030] 本发明各实施例还支持同轴电缆多媒体联盟(MoCA)联网标准和其他联网标准。例如,MoCA是提倡使用同轴电缆来连接家中的消费者电子设备和联网设备并允许在顺从性设备之间进行数据通信以及音频和视频流传递两者的标准的贸易集团。因此,如本文中所使用的,术语"MoCA设备"是指根据MoCA标准来通信的设备。

[0031] 出于本文的讨论目的,术语"按钮"可指任何钮、开关、触摸、滑动、或其他合适的用户接口,其在被激活时使得相关联的设备开始进行网络连接建立操作。此外,如本文所使用的,术语"加入设备"是指当前可能不是网络成员但(例如,响应于对该设备的按钮的激活)已进入"加入状态"的设备,"加入状态"允许该设备开始进行简单连接建立操作以加入该网络。术语"添加设备"是指当前是网络成员且(例如,响应于对该设备的按钮的激活)已进入"添加状态"的设备,"添加状态"允许该设备促成将另一设备(例如,加入设备)添加到该网络。

[0032] 此外,如本文所使用的,术语"口令短语"和"口令"是指字符或符号(例如,ASCII字符)的序列,其可用于建立设备和/或网络之间的安全链路,并且因此出于本文的讨论目的是可互换的。术语"密钥"是指字符或符号(例如,ASCII字符)的序列或比特序列,其可由一个或多个设备用于形成新网络、加入现有网络、和/或认证与网络相关联的一个或多个设备。对于本文描述的一些实施例,可使用相对简单的变换操作(例如,字符截断、字符填补、字符替换操作、和/或字符编码操作)从主口令短语导出网络口令和设备口令,并且可使用相对复杂的变换操作(例如,散列技术)分别从网络口令和设备口令导出网络密钥和设备密钥。

[0033] 如以上提及的,根据本发明各实施例,可使用单个主口令短语来生成安全凭证(例如,口令和/或安全密钥)以用于认证具有根据一种或多种不同网络技术或通信协议进行操作的网络接口的设备。由于口令和安全密钥的细节(例如,可接受长度、格式、和/或有效字符集)在不同网络技术之间通常是有所不同的,因此用于生成此类口令和安全密钥的具体技术对于不同网络技术是有所不同的。因此,根据本发明各实施例,可对共用的主口令短语执行不同类型的相对简单的变换操作以生成因网络技术而异的不同的口令和安全密钥。对于一些实施例,在给定设备中为了导出此类口令和/或安全密钥而对共用的主口令短语执行的变换操作类型可响应于该给定设备所采用的(诸)网络接口的类型(例如,该设备是具有根据Wi-Fi通信协议、PLC协议、MoCA协议、还是此类协议的组合进行操作的网络接口)来选择。

[0034] 对于一些实施例,在创建和/或修改混合网络时可使用两种类型的主口令短语:"设备主口令短语"和"网络主口令短语"。专用于给定设备的设备主口令短语(DMPP)可用于使该给定设备加入网络并且可由正加入该网络的设备以及认证方设备预共享。对于一些实施例,DMPP可被印刷在附着于该设备的标签上,且还(例如,由该设备的制造商)存储在该设备内的非易失性存储器中。随后,为了使该设备加入混合网络,用户将该标签上所指示的DMPP输入到认证方设备(例如,其可能已经是该网络的成员)中,且此后该加入设备和认证方设备可对该DMPP执行相同的变换操作以生成相同的因网络技术而异的口令,该口令进而可被用于建立(例如,认证)这两个设备之间的安全链路且此后促成使该加入设备加入该网络。

[0035] 为混合网络中的所有设备所已知的网络主口令短语(NMPP)可以是使用各种各样的技术来分发给这些网络设备的。例如,在一个实施例中,用户可生成NMPP并且随后将该NMPP输入到要被加入该网络的每个设备中。在另一个实施例中,给定设备可自动生成NMPP并(例如,在给定设备上提供的合适UI上)向用户显示该NMPP,用户进而将该NMPP输入到寻求加入该网络的其他设备中。在又一实施例中,可在认证操作期间使用其他预共享设备密钥或口令将NMPP从认证方设备传送给加入设备。NMPP随后可由每个设备进行变换以生成相同的因网络技术而异的口令,该口令进而可被用于建立(例如,认证)这两个设备之间的安全链路。

[0036] 图1是其中可实现本发明各实施例的混合网络100的框图。系统100被示为包括Wi-Fi设备110、PLC设备111、以及混合设备112。Wi-Fi设备110包括可根据IEEE802.11标准族进行操作的Wi-Fi接口WL0,PLC设备111包括可根据HPAV标准、PLC标准、和/或IEEE1901标准族进行操作的PLC接口PL1,并且混合设备112包括Wi-Fi接口WL2和PLC接口PL2。尽管出于简化而在图1中仅示出了三个设备110-112,但是将理解,网络100可包括任何数目的具有根据任何合适的网络通信技术或协议进行操作的一个或多个网络接口的设备。此外,尽管出于简化起见而在图1中未示出,但是网络100可包括具有允许进行按MoCA标准来管控的通信的顺应MoCA网络接口的其他设备。

[0037] 每个设备110-112可以是任何合适的设备,包括例如蜂窝电话、PDA、平板计算机、膝上型计算机、无线接入点、调制解调器、路由器、PLC网络适配器、网际协议(IP)电视,或能够使用Wi-Fi协议、HPAV协议、MoCA协议、以太网协议和/或其他协议与其他设备通信的其他合适设备。此外,应注意,此类设备的Wi-Fi接口可在混合网络100的WLAN子网络(出于简化起见而未示出)上彼此通信,此类设备的PLC接口可在混合网络100的PLC子网络(出于简化起见而未示出)上彼此通信,等等。

[0038] 图2示出作为图1的混合设备112的一个实施例的设备200。设备200包括Wi-Fi网络接口210、PLC接口220、处理器230、以及存储器240。Wi-Fi网络接口210包括可被用于使用Wi-Fi(即,WLAN)协议与关联于网络100的其他设备交换数据的接收机/发射机电路(出于简化起见而未示出)。PLC网络接口220包括可被用于使用HPAV协议和/或其他PLC协议与关联于网络100的其他设备交换数据的接收机/发射机电路(出于简化起见而未示出)。

[0039] 存储器240包括口令短语表242,其存储可用来与关联于网络100的其他设备建立安全链路、认证与网络100相关联的其他设备、促成将设备200加入网络100、和/或促成将其他设备加入网络100的各种口令、口令短语、密钥、和/或PIN。例如,表242可存储网络主口令短语(NMPP)、设备主口令短语(DMPP)、HPAV网络成员资格密钥(NMK)、HPAV设备接入密钥(DAK)、Wi-Fi网络口令(WLNP)、Wi-Fi预共享密钥(PSK)、以及专用于任何合适的网络技术的其他合适的口令。

[0040] 存储器240还包括非瞬态计算机可读介质(例如,一个或多个非易失性存储器元件,诸如EPROM、EEPROM、闪存、硬盘驱动器、等等),其存储以下软件模块:

[0041] • 网络主口令短语变换软件(SW)模块244,用于响应于网络主口令短语(NMPP)而生成因网络技术而异的网络口令,其中网络主口令短语(NMPP)可存储在表242中、由用户经由合适的UI来输入、和/或从与混合网络100相关联的另一设备提供;

[0042] • 设备主口令短语变换软件模块246,用于响应于设备主口令短语(DMPP)而生成

因网络技术而异的设备口令,其中设备主口令短语(DMPP)可存储在表242中、由用户经由合适的UI来输入、和/或从与混合网络100相关联的另一设备提供;

[0043] • 口令散列软件模块248,用于响应于因网络技术而异的口令来生成因网络技术而异的密钥。

[0044] 每个软件模块包括指令,这些指令在由处理器230执行时使设备200执行相应的功能。存储器240的非瞬态计算机可读介质由此包括用于执行以下关于图3-4描述的方法的操作的全部或一部分的指令。

[0045] 处理器230耦合到Wi-Fi网络接口210、PLC网络接口220、以及存储器240,且可以是能够执行存储在设备200中(例如,存储器240内)的一个或多个软件程序的脚本或指令的任何合适的处理器。例如,处理器230可执行网络主口令短语变换软件(SW)模块244、设备主口令短语变换软件(SW)模块246、以及口令散列软件模块248。

[0046] 更具体地,处理器230可执行网络主口令短语变换SW模块244以使用根据本发明各实施例的各种变换操作从NMPP生成任何数目的因网络技术而异的不同网络口令。例如,对SW模块244的执行可使得对NMPP执行第一变换操作以生成HPAV网络口令(NPW),可使得对该NMPP执行第二变换操作以生成WLAN网络口令(WLNP),和/或可使得对该NMPP采用其他变换操作以生成用于其他子网络技术的网络口令。

[0047] 类似地,处理器230可执行设备主口令短语变换SW模块246以使用根据本发明各实施例的各种变换操作从DMPP生成任何数目的因网络技术而异的不同设备口令。例如,对SW模块246的执行可使得对DMPP采用第一变换操作以生成HPAV设备口令(DPW),可使得对该DMPP采用第二变换操作以生成WLAN设备口令(WLDP),和/或可使得对该DMPP采用其他变换操作以生成用于其他子网络技术的设备口令。

[0048] 处理器230可执行口令散列SW模块248,以针对每种类型的网络技术,从由口令短语变换SW模块244和/或246生成的相应口令来生成安全密钥。更具体地,对于HPAV网络技术,口令散列SW模块248可从HPAV网络口令(NPW)导出HPAV网络成员资格密钥(NMK),和/或可从HPAV设备口令(DPW)导出HPAV设备接入密钥(DAK)。对于WLAN网络技术,口令散列SW模块248可从WLAN网络口令(WLNP)导出WLAN预共享密钥(PSK),和/或可从WLAN设备PIN(WLDP)导出WLAN设备密钥(WLDK)。

[0049] 注意,图1的Wi-Fi设备110和PLC设备111的实施例除了网络接口的数目和/或类型以外可类似于图2的混合设备200。例如,Wi-Fi设备110的实施例可包括混合设备200的除PLC接口220以外的所有元件,而PLC设备111的实施例可包括混合设备200的除Wi-Fi接口210以外的所有元件。

[0050] 图3是描绘根据一些实施例的用于从单个网络主口令短语(NMPP)创建多个因技术而异的不同网络口令和/或密钥的示例性操作的解说性流程图300。首先,用户将NMPP输入到与混合网络100相关联的一个或多个设备中(302)。注意,NMPP可以是HPAV网络口令(NPW)和Wi-Fi网络口令(WLNP)的超集,如以下更详细地描述的。

[0051] 随后,可在已为其输入了NMPP和/或先前已为其存储了NMPP的设备中执行一种或多种类型的相对简单的变换操作(304)。对于一些实施例,这些相对简单的变换操作可被选择性地执行(例如,根据该设备采用哪种类型的(诸)网络技术接口)以生成一个或多个因技术而异的网络口令(306)。对于一些实施例,这些相对简单的变换操作可选择性地截断NMPP

的字符、填补NMPP(例如,向其添加字符)、替换NMPP的字符、和/或编码NMPP的字符集以生成各种因技术而异的网络口令(306)。例如,可对该NMPP执行第一变换操作以生成HPAV网络口令(NPW)(306A),可对该NMPP执行第二变换操作以生成WLAN网络口令(WLNP)(306B),和/或可对该NMPP执行第三变换操作以生成用于其他网络技术的网络口令(NTPP)(306C)。

[0052] 如以上提及的,口令和安全密钥的细节(例如,可接受长度、格式、和/或有效字符集)在不同网络技术之间通常是有所不同的。例如,一种网络技术(例如,HPAV)可允许具有任何可打印的ASCII字符的8到64个实例之间(含8个和64个)的实例的口令,而另一种网络技术(例如,Wi-Fi)可允许仅字母数字字符的4到20个实例之间(含4个和20个)的实例的口令。因此,根据本发明各实施例,若目标网络技术不允许其口令包括非字母数字字符(例如,空格、制表符、标点符号、等等),则可使用一变换操作来变换包括此类非字母数字字符的网络主口令短语(NMPP),该变换操作用预定字母数字字符和/或预定字符序列来替换此类非字母数字字符,以使得从该NMPP生成的因技术而异的口令顺应目标网络技术(例如,以使得所得的因网络技术而异的口令仅包含目标网络技术所允许的字符和/或符号)。相反,如果NMPP不包括任何不被目标网络技术所允许的字符,则在从该NMPP生成网络口令时,用来生成因技术而异的网络口令的变换可以无需替换该NMPP的任何字符。

[0053] 如果NMPP包含比目标网络技术所允许的最小口令字符数目少的字符(例如,NMPP太短),则可按确定性的方式(例如,用目标网络技术所允许的一个或多个字符或符号,诸如“x”)来填补该NMPP。填补字符可包括从NMPP中的字符确定性地导出的字符,包括复制该NMPP中的字符以及使用另一变换操作的简单字符替代,以使得从该NMPP生成的网络口令顺应目标网络技术(例如,以使得所得的因技术而异的口令是具有目标网络技术所允许的最短长度的口令)。

[0054] 如果NMPP包含比目标网络技术所允许的最大口令字符数目多的字符(例如,NMPP太长),则可使用又一变换操作来截断该NMPP,以使得从该NMPP生成的网络口令顺应目标网络技术(例如,以使得所得的因技术而异的口令是具有目标网络技术所允许的最长长度的口令)。对于其他实施例,可将超出目标网络技术所允许的最长长度的数个NMPP字符与原本不会被截断的NMPP字符相组合,以从该NMPP的所有字符导出新口令(例如,具有目标网络技术所允许的最长长度)。因此,对于此类其他实施例,并非截断NMPP的部分,而是可使用合适的字符组合或编码算法来组合该NMPP的一群或多群字符,以产生目标网络技术所允许的相应数目的单个字符或符号。

[0055] 不管为了生成网络口令而对NMPP执行的(诸)变换操作为何,重要的是,所得的因技术而异的网络口令顺应与相应的目标网络技术相关联的口令要求,并且这些网络口令是以确定性的方式生成的,以使得无论是由哪个设备从给定NMPP导出(诸)网络口令,使用这些相对简单的变换操作(例如,字符替换、填补、截断、以及编码)中的一种特定变换操作来变换该NMPP会产生相同的口令。

[0056] 对于替代实施例,针对给定网络技术从相关联的NMPP导出网络口令(例如,在304中使用这些相对简单的变换操作)可由第一设备代表使用该给定网络技术的第二设备来执行,而该第一设备可以使用或可以不使用该给定网络技术。可针对其中第二设备不实现根据本发明各实施例的从NMPP导出网络口令的操作的情形而采用这些替代实施例。在该替代实施例中,网络口令可显示在第一设备的UI上,由此允许用户读取该口令并将其输入到第

二设备上的UI中。

[0057] 一旦已根据本发明各实施例使用这些相对简单的变换操作从NMPP导出了各种因技术而异的网络口令，就可响应于网络技术类型对所导出的网络口令执行一个或多个相对复杂的变换操作(308)以生成一个或多个网络安全密钥(310)。对于一些实施例，这些相对复杂的变换操作可选择性地散列或级联这些网络口令以导出网络安全密钥，网络安全密钥进而可用于认证设备和/或将设备加入混合网络。对于其他实施例，密钥的导出可涉及两个设备之间的消息交换连同合适的变换操作。例如，为了达成更大的安全性，可在两个设备之间功能性地分担临时密钥的导出，并且临时密钥的导出是作为认证消息交换的副产品来执行的。

[0058] 更具体地，HPAV网络口令(NPW)可根据第一散列函数被散列以生成HPAV网络成员资格密钥(NMK)(310A)，WLAN网络口令(WLNP)可根据第二散列函数被散列以生成WLAN预共享机密密钥(PSK)(310B)，并且其他网络口令(NTTP)可根据第三散列函数被散列以生成用于其他网络技术的预共享机密密钥(NTPSK)(310C)。对于一些实施例，第一、第二和第三散列函数可以是不同的，而对于其他实施例，第一、第二和第三散列函数中的一者或多者可以是相同的。

[0059] 此外，对于替代实施例，针对给定网络技术从相关联的网络口令导出网络安全密钥(例如，在308中使用这些相对复杂的变换操作)可由不使用该给定网络技术的设备代表使用该给定网络技术的另一设备来执行。可针对其中该另一设备不具有允许用户输入主口令短语或网络口令的UI的情形而采用这些替代实施例。

[0060] 所得的因技术而异的网络安全密钥随后可被用于认证这些设备之间的安全链路、形成网络、和/或将设备添加到混合网络。

[0061] 图4是描绘根据一些实施例的用于从单个设备主口令短语(DMPP)创建多个因技术而异的不同设备口令和/或密钥的示例性操作的解说性流程图400。首先，用户将DMPP输入到与混合网络100相关联的一个或多个设备中(402)。注意，DMPP可以是HPAV设备口令(DPW)和Wi-Fi设备口令(WLDP)的超集，如以下更详细地描述的。

[0062] 随后，在已为其输入了DMPP和/或先前已为其存储了DMPP的设备中执行一种或多种类型的相对简单的变换操作(404)。对于一些实施例，可响应于设备接口的各种网络技术类型而选择性地执行这些相对简单的变换操作以生成一个或多个因技术而异的设备口令(406)。对于一些实施例，这些相对简单的变换操作可选择性地截断DMPP的字符、填补DMPP(例如，向其添加字符)、替换DMPP的字符、和/或编码DMPP的字符集以生成各种因技术而异的设备口令(406)。例如，可对该DMPP执行第一变换操作以生成HPAV设备口令(DPW)(406A)，可对该DMPP执行第二变换操作以生成WLAN设备口令(WLDP)(406B)，和/或可对该DMPP执行第三变换操作以生成用于其他网络技术的设备口令(NTDP)(406C)。

[0063] 如以上提及的，口令和安全密钥的细节(例如，可接受长度、格式、和/或有效字符集)在不同网络技术之间通常是有所不同的。例如，一种网络技术(例如，HPAV)可允许具有任何可打印的ASCII字符的8到64个实例之间(含8个和64个)的实例的口令，而另一种网络技术(例如，Wi-Fi)可允许具有仅字母数字字符的4到20个实例之间(含4个和20个)的实例的口令。因此，根据本发明各实施例，若目标网络技术不允许其口令包括非字母数字字符(例如，空格、制表符、标点符号、等等)，则可使用一变换操作来变换包括此类非字母数字字

符的设备主口令短语(DMPP),该变换操作用预定字母数字字符和/或预定字符序列来替换此类非字母数字字符,以使得从该DMPP生成的因技术而异的口令顺应目标网络技术(例如,以使得所得的因网络技术而异的口令仅包含目标网络技术所允许的字符和/或符号)。相反,如果DMPP不包括任何不为目标网络技术所允许的字符,则在从该DMPP生成设备口令时,用来生成因技术而异的口令的变换可以无需替换该DMPP的任何字符。

[0064] 如果DMPP包含比目标网络技术所允许的最小口令字符数目少的字符(例如,DMPP太短),则可按确定性的方式(例如,用目标网络技术所允许的一个或多个字符或符号,诸如"x")来填补该DMPP。填补字符可包括从DMPP中的字符确定性地导出的字符,包括复制该DMPP中的字符以及使用另一变换操作的简单字符替代,以使得从该DMPP生成的设备口令顺应目标网络技术(例如,以使得所得的因技术而异的设备口令是具有目标网络技术所允许的最短长度的口令)。

[0065] 如果DMPP包含比目标网络技术所允许的最大口令字符数目多的字符(例如,DMPP太长),则可使用又一变换操作来截断该DMPP,以使得从该DMPP生成的设备口令顺应目标网络技术(例如,以使得所得的因技术而异的设备口令是具有目标网络技术所允许的最长长度的口令)。对于其他实施例,可将超出目标网络技术所允许的最长长度的数个DMPP字符与原本不会被截断的DMPP字符相组合,以从该DMPP的所有字符导出新口令(例如,具有目标网络技术所允许的最长长度)。因此,对于此类其他实施例,并非截断DMPP的部分,而是使用合适的字符组合或编码算法来组合该DMPP的一群或多群字符,以产生目标网络技术所允许的相应数目的单个字符或符号。

[0066] 不管为了生成设备口令而对DMPP执行的(诸)变换操作为何,重要的是所得的因技术而异的设备口令顺应与相应的目标网络技术相关联的口令要求,并且该设备口令是以确定性的方式生成的,以使得无论由哪个设备从给定DMPP导出设备口令,使用这些相对简单的变换操作(例如,字符替换、填补、截断、以及编码)中的一种特定变换操作来变换该DMPP会产生相同的口令。

[0067] 对于替代实施例,针对给定网络技术从相关联的DMPP导出设备口令(例如,在404中使用这些相对简单的变换操作)的操作可由第一设备代表使用该给定网络技术的第二设备来执行,而该第一设备可以使用或可以不使用该给定网络技术。可针对其中第二设备不实现根据本发明的从DMPP导出设备口令的操作的情形而采用这些替代实施例。在该替代实施例中,设备口令被显示在第一设备的UI上,由此允许用户读取该口令并将其输入到第二设备上的UI中。

[0068] 一旦已根据本发明各实施例使用这些相对简单的变换操作从DMPP导出了各种因技术而异的设备口令,就可响应于网络技术类型对这些设备口令执行一个或多个相对复杂的变换操作(408)以生成一个或多个设备安全密钥(410)。对于一些实施例,这些相对复杂的变换操作可选择性地散列或级联这些设备口令以导出设备安全密钥,设备安全密钥进而可用于认证设备和/或将设备加入混合网络。例如,对于PLC子网络,加入设备的DAK可由该网络的成员设备用来加密用于传送给该加入设备的网络成员资格密钥(NMK),该加入设备进而可使用该DAK来解密该NMK并在此后使用该NMK来加入该网络。

[0069] 更具体地,HPAV设备口令(DPW)可根据第一散列函数被散列以生成HPAV设备接入密钥(DAK)(410A),WLAN设备口令(WLDP)可根据第二散列函数被散列以生成WLAN设备密钥

(WLDK)(410C),并且其他设备口令(NTDP)可根据第三散列函数被散列以生成用于其他网络技术的设备密钥(NTDK)(410D)。对于一些实施例,第一、第二和第三散列函数可以是不同的,而对于其他实施例,第一、第二和第三散列函数中的一者或多者可以是相同的。

[0070] 此外,对于替代实施例,针对给定网络技术从相关联的设备口令导出设备安全密钥(例如,在408中使用这些相对复杂的变换操作)的操作可由不使用该给定网络技术的设备代表使用该给定网络技术的另一设备来执行。可针对其中该另一设备不具有允许用户输入主口令短语或设备口令的UI的情形而采用这些替代实施例。

[0071] 另外,可响应于网络技术类型使用一个或多个复杂变换和/或安全消息交换操作来变换所得的因技术而异的设备密钥(412)以生成临时设备密钥(414)。例如,HPAV DAK可被变换(例如,散列)以导出HPAV临时设备接入密钥(TDAK)(414A),而WLAN设备密钥可被变换(例如,散列)以导出WLAN临时设备密钥(WTDK)(414B)。更具体地,对于一些实施例,密钥导出可涉及两个设备之间的消息交换连同合适的变换操作。例如,为了达成更大的安全性,可在两个设备之间功能性地分担对临时密钥的导出,并且临时密钥的导出是作为认证消息交换(例如,根据如802.11RSNA数据机密性协议中描述的"4路握手")的副产品来执行的。

[0072] 在以下关于图5-8描述本发明各实施例的具体示例之前,应注意,当用户创建主口令短语(例如,NMPP或DMPP)并将该主口令短语输入到具有UI的设备中时,这些设备可能具有用于执行从该主口令短语导出因技术而异的口令的变换操作的预定协定和/或标准。例如,如果用户使用膝上型电脑创建网络,则用户可通过使用DAK技术来加入不具有UI的所选设备。更具体地,对于该示例,用户可将所选设备的DAK输入到膝上型电脑中,从而该膝上型电脑和所选设备具有可用来建立它们之间的安全链路的共用机密密钥。随后,膝上型电脑可加密主口令短语并在该安全链路上与所选设备共享经加密的主口令短语。随后,所选设备可使用其DAK来解密该经加密的主口令短语,并在此后对主口令短语执行变换操作以生成用于将该所选设备加入网络的口令和密钥。

[0073] 另外,对于其中用户希望将Wi-Fi设备加入已经具有HPAV口令和密钥的现有HPAV网络(例如,由此修改该HPAV网络以创建混合网络)的情形,诸PLC设备中的所选PLC设备可对HPAV网络口令(NPW)执行逆变换操作以导出合适的NMPP,该NMPP随后可被变换(例如,使用另一变换操作)以创建生成顺应WLAN口令要求的WLAN口令(WLNP)。对于此类实施例,所选PLC设备可向用户显示经逆变换的NMPP,并且还可向用户显示结果所得的WLAN口令(例如,以使得用户可将结果所得的WLAN口令输入到Wi-Fi设备中并由此促成其向网络的认证)。

[0074] 以下关于图5-8来描述根据本发明各实施例的使用主口令短语的各种示例性建立操作,其中在水平方向上描绘距离而在垂直方向上描绘时间(其中时间在向下方向上增长)。

[0075] 图5是解说与形成混合网络500相关联的消息交换的序列图,混合网络500被形成为包括两个各自具有PLC网络接口的PLC设备PL2和PL3、具有Wi-Fi网络接口的Wi-Fi设备WL2、以及具有PLC和Wi-Fi网络接口两者的混合PLC/Wi-Fi设备PL1/WL1。注意,在形成网络500之后,PLC设备接口PL1-PL3可经由PLC子网络501来彼此通信,并且Wi-Fi设备WL1-WL2可经由Wi-Fi子网络(出于简化起见而未示出)来彼此通信。在形成网络500之后,若混合PLC/Wi-Fi设备PL1/WL1能够在PLC子网络与Wi-Fi子网络之间转发帧,则网络500中的所有设备都可以彼此通信。对于图5的示例,PLC设备PL2和PL3首先使用由用户输入的网络主口令短

语(NMPP)经由相互认证来形成网络，接着使用输入到PLC设备PL3中的设备主口令来认证混合设备PL1/WL1。在认证操作期间，混合设备PL1/WL1从PLC设备PL3设备获得NMPP，并在此后使用该NMPP来认证Wi-Fi设备WL2。

[0076] 更具体地，用户首先将NMPP输入到PLC设备PL2和PL3中，PLC设备PL2和PL3进而对该NMPP进行变换以导出NMK。一旦PLC设备PL2和PL3两者都已从NMPP导出了NMK，设备PL2和PL3就可形成PLC子网络并授权对彼此的认证。在设备PL2和PL3已形成PLC子网络之后，用户将混合设备PL1/WL1的设备主口令短语(DMPP)输入到设备PL3中。响应于此，设备PL3从该DMPP导出混合设备PL1/WL1的接口PL1的DAK(例如，使用合适的散列技术)。随后，为混合设备PL1/WL1的接口PL1导出的DAK可被用于授权和认证混合设备PL1/WL1的PLC接口PL1。

[0077] 例如，设备PL3可使用混合设备PL1/WL1的接口PL1的DAK来加密NMK并将其传送给混合设备PL1/WL1。随后，混合设备PL1/WL1的接口PL1使用其预存的DAK来解密该NMK，并在此后使用解密出的NMK来加入PLC子网络501。

[0078] 一旦混合设备PL1/WL1的接口PL1加入了PLC子网络，设备PL3就在现在建立好的PLC子网络501上将NMPP传递给混合设备PL1/WL1，并且混合设备PL1/WL1的接口PL1的上软件层(USL)将该NMPP传递给混合设备PL1/WL1的WLAN接口WL1。随后，混合设备PL1/WL1的接口WL1可使用该NMPP来导出WLAN PSK。注意，将NMPP从PLC设备PL3传递给混合设备PL1/WL1的操作所起到的用意就像用户已直接将NMPP输入到混合设备PL1/WL1的Wi-Fi接口WL1中的用意一样，但有利地不需要用户手动将NMPP输入到混合设备PL1/WL1中。对于其他实施例，可在这两个设备之间建立安全链路之后在经加密消息中将NMPP传递给混合设备PL1/WL1(或另一设备)。

[0079] 接下来，用户将该NMPP输入到Wi-Fi设备WL2中，Wi-Fi设备WL2进而从该NMPP导出WLAN PSK。由于相同的NMPP已被提供或输入到Wi-Fi设备WL1和WL2两者中，因此它们皆导出相同的PSK，并且因此可使用该PSK例如根据稳健安全网络关联(RSNA)认证技术来建立WLAN子网络。

[0080] 图6是解说与形成混合网络600相关联的消息交换的序列图，混合网络600被形成为包括具有PLC网络接口的PLC设备PL2、两个各自具有Wi-Fi网络接口的Wi-Fi设备WL2和WL3、以及具有PLC和Wi-Fi网络接口两者的混合PLC/Wi-Fi设备PL1/WL1。注意，在形成网络600之后，PLC设备接口PL1-PL2可经由PLC子网络601来彼此通信，并且Wi-Fi设备WL1-WL3可经由Wi-Fi子网络(出于简化起见而未示出)来彼此通信。在形成网络600之后，若混合PLC/Wi-Fi设备PL1/WL1能够在PLC子网络与Wi-Fi子网络之间转发帧，则网络600中的所有设备都可以彼此通信。对于图6的示例，网络主口令短语(NMPP)与“简单连接”按钮建立操作的组合被用来向混合网络认证诸设备，藉此Wi-Fi设备WL2和WL3使用该NMPP来彼此认证，简单连接建立操作被用来将Wi-Fi设备WL3连接至混合设备PL1/WL1的Wi-Fi接口WL1并在此后将该NMPP传递给混合设备PL1/WL1。随后，混合设备PL1/WL1使用根据本发明各实施例从该NMPP导出的共用NMK来与PLC设备PL2形成PLC子网络。

[0081] 更具体地，用户首先将NMPP输入到Wi-Fi设备WL2和WL3中，Wi-Fi设备WL2和WL3进而对该NMPP进行变换以导出WLAN网络口令并在此后导出PSK。一旦Wi-Fi设备WL2和WL3两者已从该NMPP导出了相同的PSK，设备WL2和WL3就可使用RSNA技术来彼此认证并藉此形成WLAN子网络。随后，用户激活Wi-Fi设备WL3上和混合设备PL1/WL1上的按钮，这使得Wi-Fi设

备WL3进入添加状态并且使得混合设备PL1/WL1的Wi-Fi接口进入加入状态。Wi-Fi设备WL3和WL1完成Wi-Fi按钮按压简单连接协议以将混合设备PL1/WL1的Wi-Fi接口WL1加入Wi-Fi子网络，并且此后Wi-Fi设备WL3的USL将该NMPP传送给混合设备PL1/WL1的Wi-Fi接口WL1。混合设备PL1/WL1将该NMPP从其Wi-Fi接口WL1传递到其PLC接口PL1，PLC接口PL1随后变换该NMPP以导出HPAV NMK。用户随后将该NMPP输入到PLC设备PL2中，PLC设备PL2响应于此使用根据本发明各实施例的变换操作来导出HPAV NMK。由于现在PLC设备PL2和混合设备PL1/WL1的PLC接口PL1两者具有相同的NMK，因此它们能够彼此认证并形成PLC子网络601。

[0082] 图7是解说与向混合网络700添加两个各自具有PLC网络接口的PLC设备PL2和PL3相关联的消息交换的序列图。注意，如本文中所使用的，向网络“添加”设备也可以指向新网络添加设备（例如，由此“形成”新网络）。对于图7的示例，Wi-Fi设备WL2-WL3和混合设备PL1/WL1的Wi-Fi接口WL1已经是WLAN子网络的成员。注意，在形成网络700之后，PLC设备接口PL1-PL3可经由PLC子网络701彼此通信。在形成网络700之后，若混合PLC/Wi-Fi设备PL1/WL1能够在PLC子网络与Wi-Fi子网络之间转发帧，则网络700中的所有设备都可以彼此通信。通过使用Wi-Fi设备WL3作为认证方设备，用设备主口令短语(DMPP)向网络认证PLC设备PL2。混合设备PL1/WL1中继被认证PL2设备与认证方WL3设备之间的认证消息。注意，对于图7的示例性图示，Wi-Fi设备WL3将第一HPAV的基于DAK协议(DBP)的消息(DBP-M1)传递给混合设备PL1/WL1，混合设备PL1/WL1进而将DBP-M1和DAK2发送给PLC设备PL2和PL3。因此，如本文中所使用的，DBP-Mn是指基于DAK的协议消息Mn，其中n是整数。

[0083] 图8是解说根据又一示例性实施例的在接口设备之间的用于向网络添加设备的消息交换的序列图(800)。该实施例的情形类似于图7中所示的情形；使用Wi-Fi设备WL3作为认证方设备在混合设备PL1/WL1的辅助下用设备主口令短语向网络认证PLC设备PL2。然而，该认证机制的细节不同于以上关于图7所描述的认证机制。更具体地，对于图8的示例，临时密钥被导出并且设备PL1/WL1用作设备WL3在PLC子网络上的代理以便于执行认证协议。

[0084] 在前述说明书中，已参照具体示例描述了本发明各实施例。然而将明显的是，可对其作出各种修改和改变而不背离如所附权利要求中所阐述的本公开更宽泛的精神和范围。相应地，本说明书和附图被认为是解说性而非限制性的。

[0085] 本发明各实施例可被作为计算机程序产品或软件来提供，其可包括上面存储有指令的非瞬态机器可读介质。机器可读介质可被用于将计算机系统(或其他电子设备)编程为实现本发明各实施例。机器可读介质可包括但不限于：软盘、光盘、CD-ROM和磁光盘、ROM、RAM、EPROM、EEPROM、磁或光卡，闪存、或者其他类型的适于存储电子指令的介质/机器可读介质。

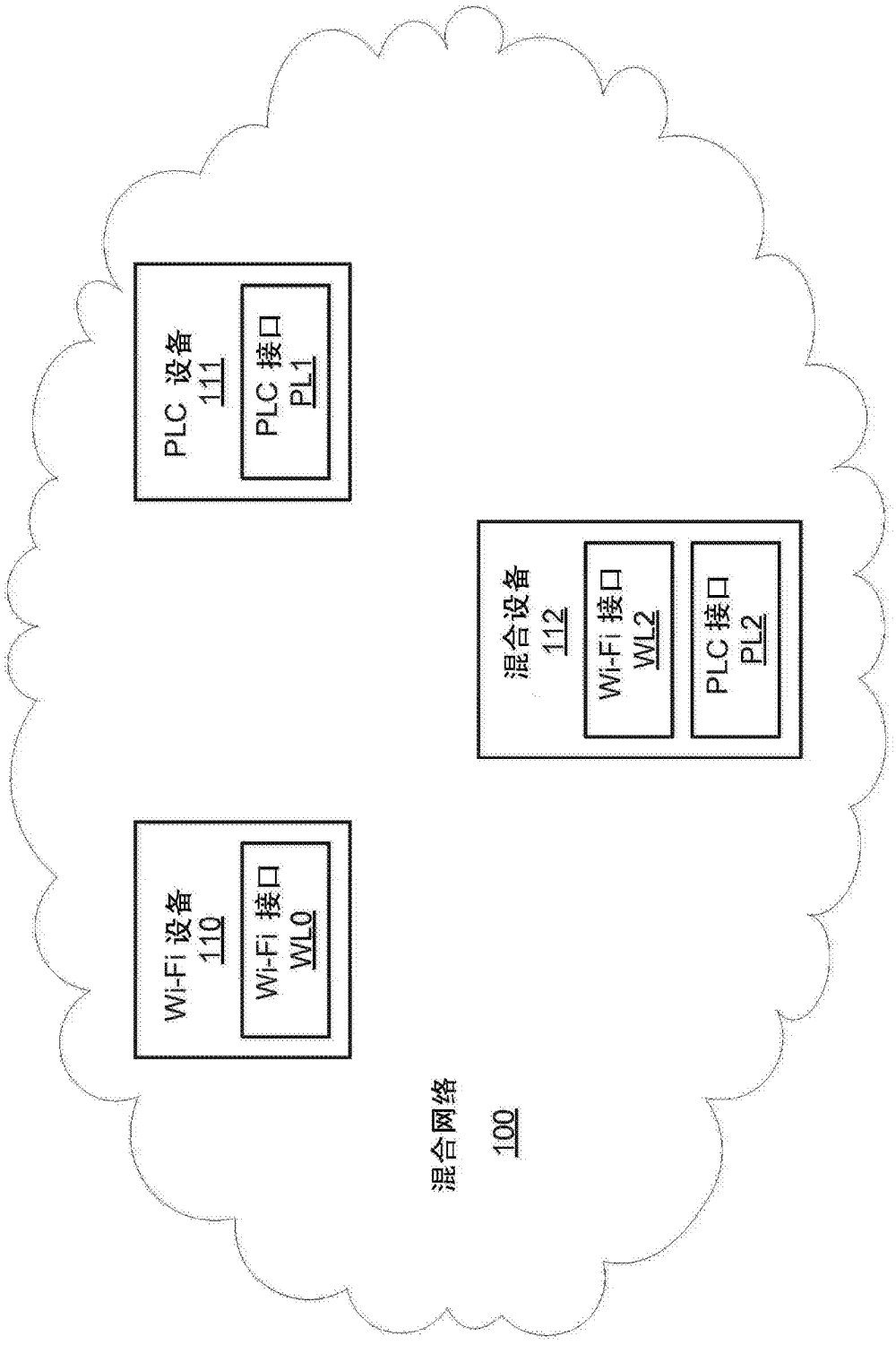

PLC 设备
111
PLC 接口
PL1
混合设备
112
Wi-Fi 接口
WL2
PLC 接口
PL2
Wi-Fi 设备
110
Wi-Fi 接口
WL0
混合网络
100

图1

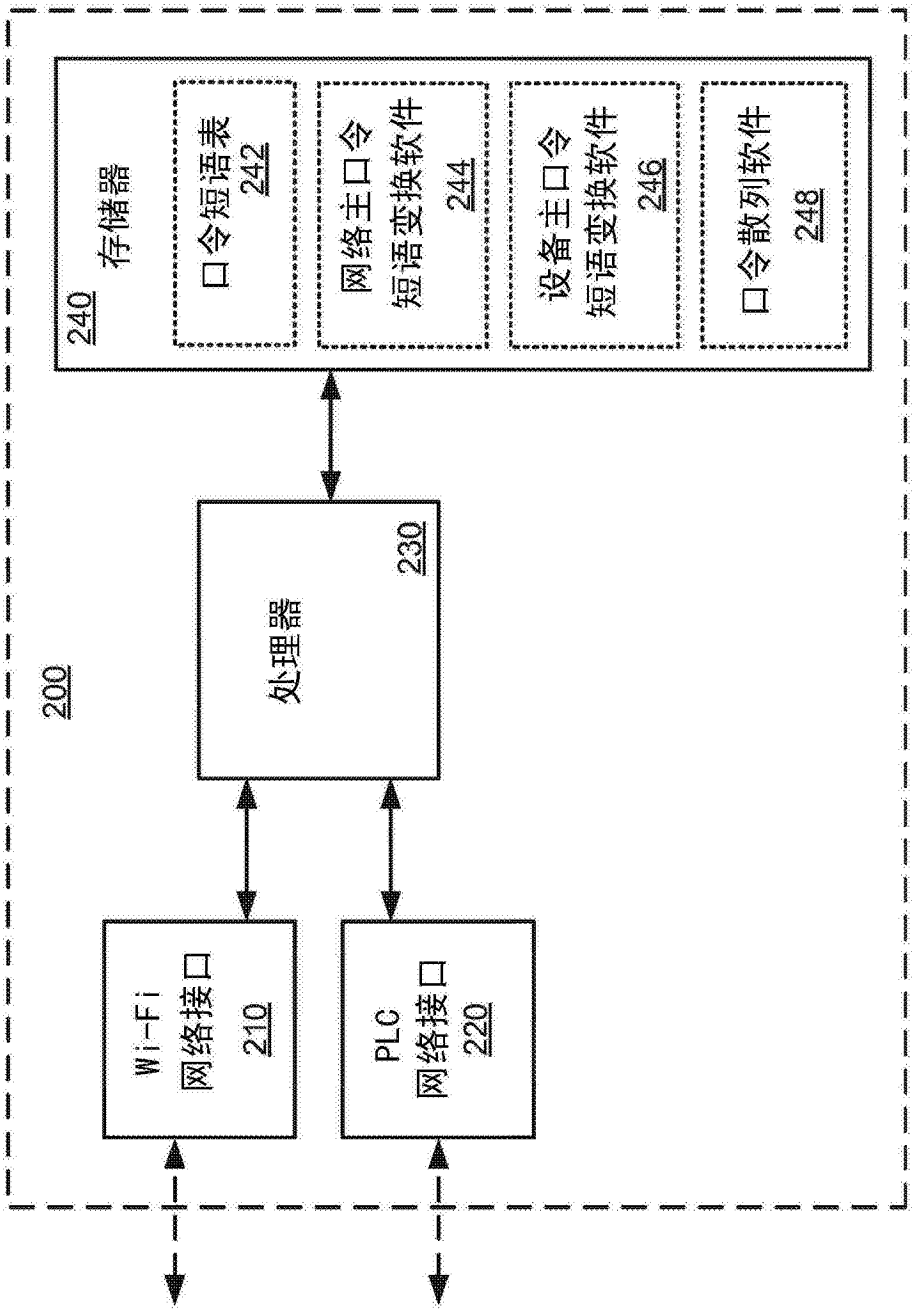

200
240
存储器
口令短语表
242
网络主口令
短语变换软件
244
设备主口令
短语变换软件
246
口令散列软件
248
处理器
230
Wi-Fi
网络接口
210
PLC
网络接口
220

图2

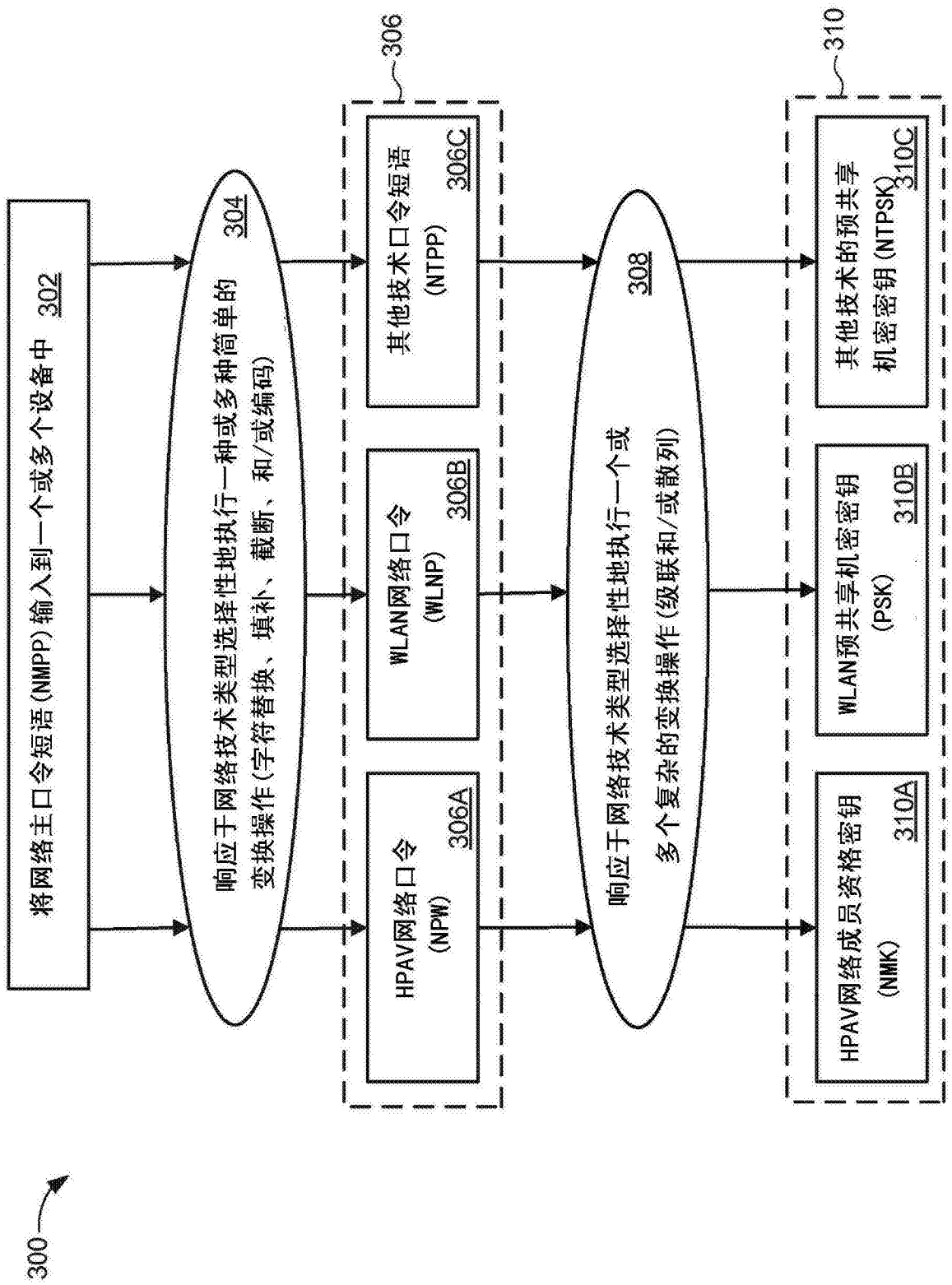

将网络主口令短语(NMPP)输入到一个或多个设备中 302
响应于网络技术类型选择性地执行一种或多种简单的变换操作(字符替换、填补、截断、和/或编码) 304
306
HPAV网络口令(NPW) 306A
WLAN网络口令(WLNP) 306B
其他技术口令短语(NTPP) 306C
响应于网络技术类型选择性地执行一个或多个复杂的变换操作(级联和/或散列) 308
310
HPAV网络成员资格密钥(NMK) 310A
WLAN预共享机密密钥(PSK) 310B
其他技术的预共享机密密钥(NTPSK) 310C
300

图3

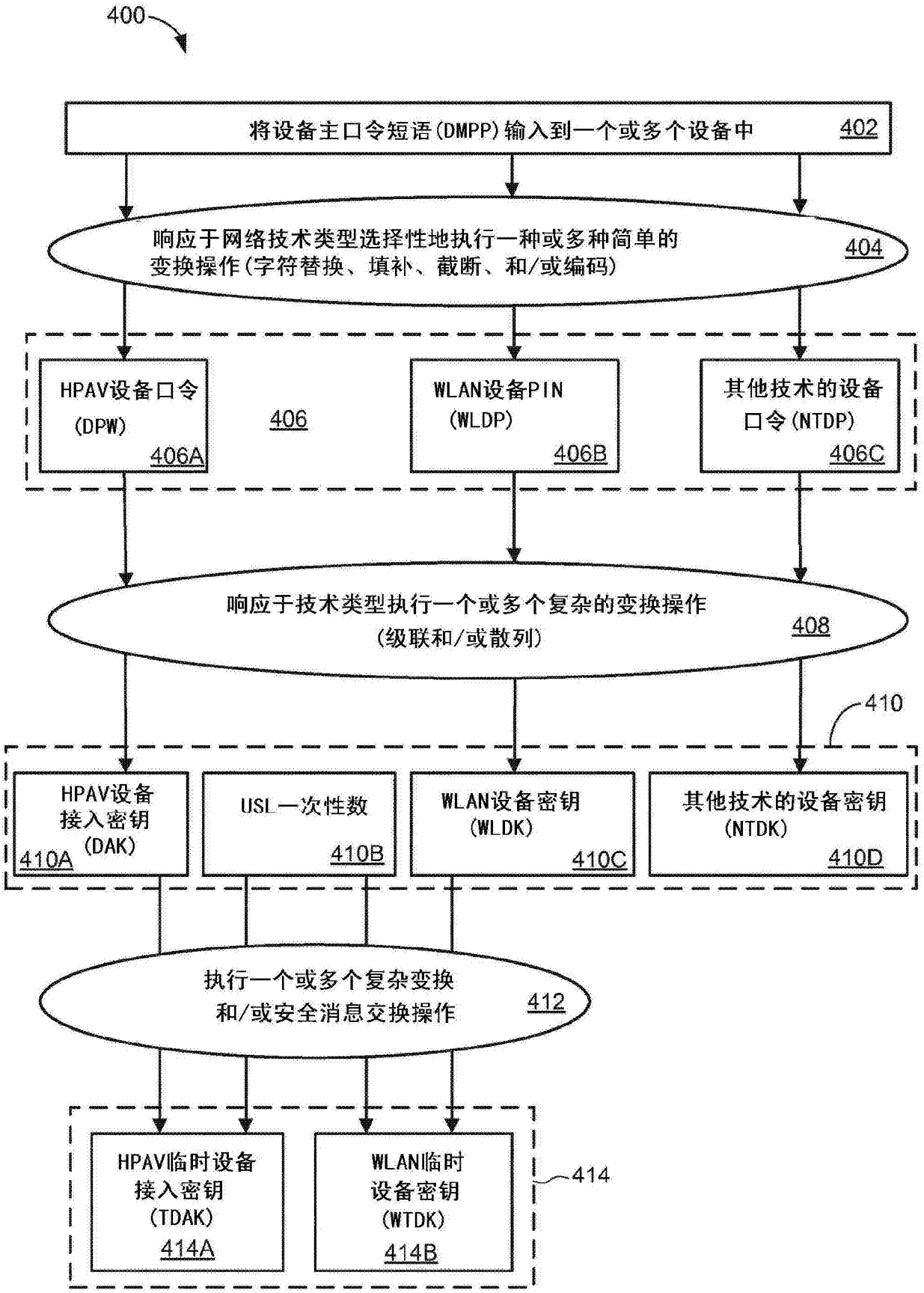

400
将设备主口令短语(DMPP)输入到一个或多个设备中
402
响应于网络技术类型选择性地执行一种或多种简单的变换操作(字符替换、填补、截断、和/或编码)
404
HPAV设备口令(DPW)
406A
406
WLAN设备PIN(WLDP)
406B
其他技术的设备口令(NTDP)
406C
响应于技术类型执行一个或多个复杂的变换操作(级联和/或散列)
408
410
HPAV设备接入密钥(DAK)
410A
USL一次性数
410B
WLAN设备密钥(WLDK)
410C
其他技术的设备密钥(NTDK)
410D
执行一个或多个复杂变换和/或安全消息交换操作
412
HPAV临时设备接入密钥(TDAK)
414A
WLAN临时设备密钥(WTDK)
414B
414

图4

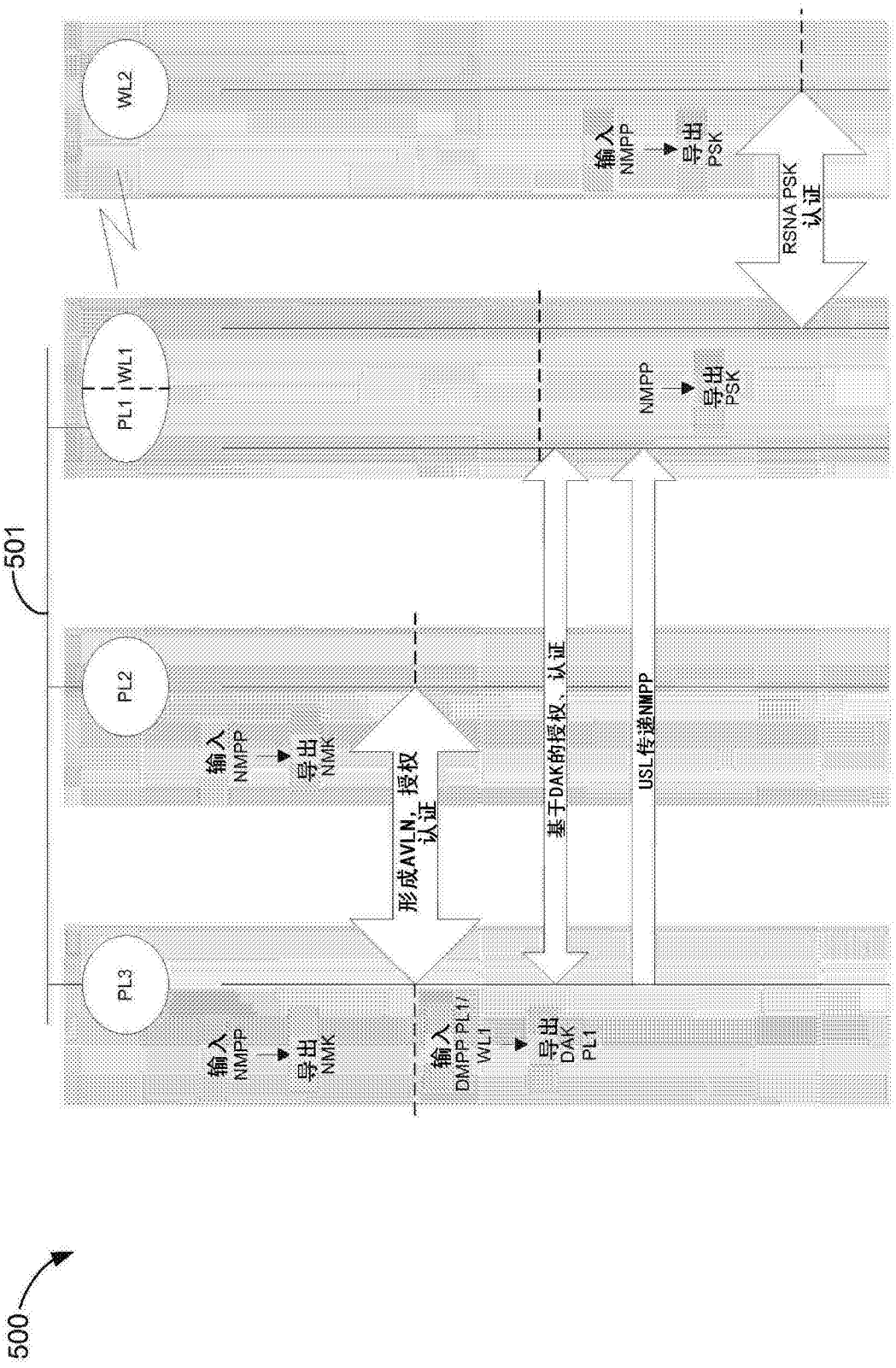

WL2
输入 NMPP
导出 PSK
RSNA PSK 认证
PL1 WL1
NMPP
导出 PSK
501
PL2
输入 NMPP
导出 NMK
形成AVLN，授权认证
基于DAK的授权、认证
USL传递NMPP
PL3
输入 NMPP
导出 NMK
输入 DMPP PL1/WL1
导出 DAK PL1
500

图5

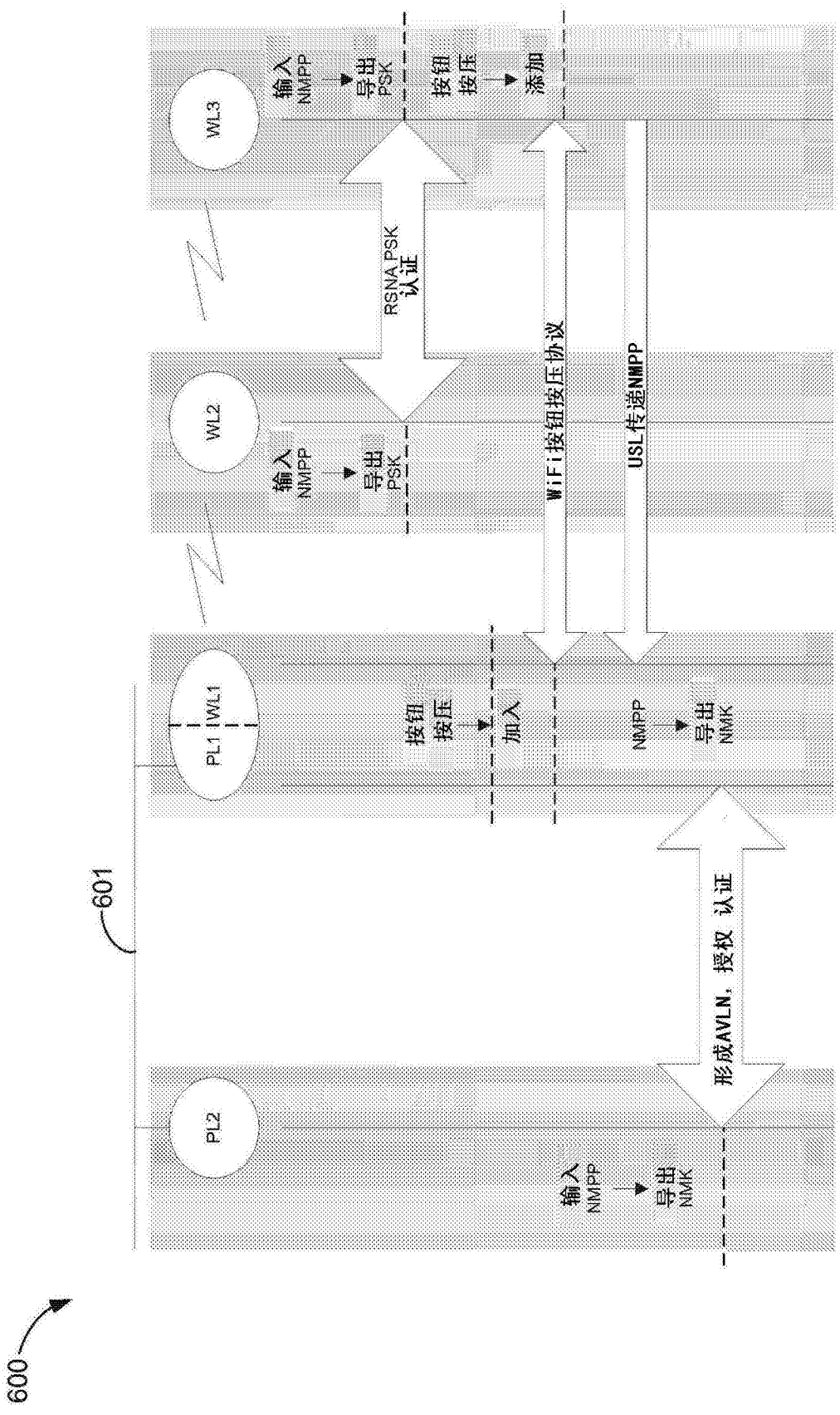

600
601
WL3
WL2
PL1
WL1
PL2
输入 NMPP
导出 PSK
按钮 按压
添加
RSNA PSK 认证
WiFi按钮按压协议
USL传递NMPP
加入
NMPP
导出 NMK
形成AVLN，授权 认证

图6

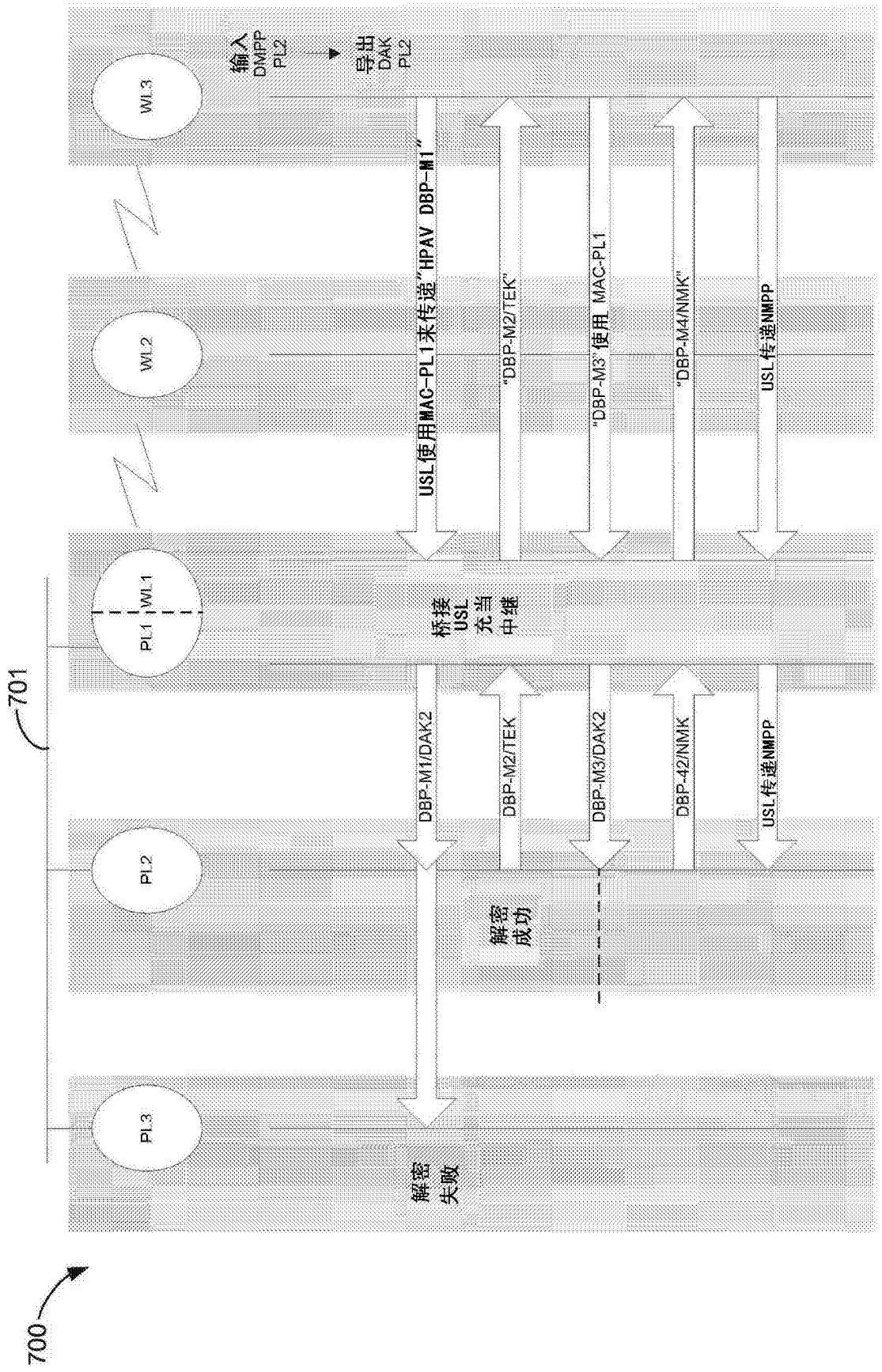

700
701
WL3
WL2
WL1
PL1
PL2
PL3
输入
DMPP
PL2
导出
DAK
PL2
USL使用MAC-PL1来传递"HPAV DBP-M1"
"DBP-M2/TEK"
"DBP-M3"使用 MAC-PL1
"DBP-M4/NMK"
USL传递NMPP
桥接
USL
充当
中继
DBP-M1/DAK2
DBP-M2/TEK
DBP-M3/DAK2
DBP-42/NMK
USL传递NMPP
解密
成功
解密
失败

图7

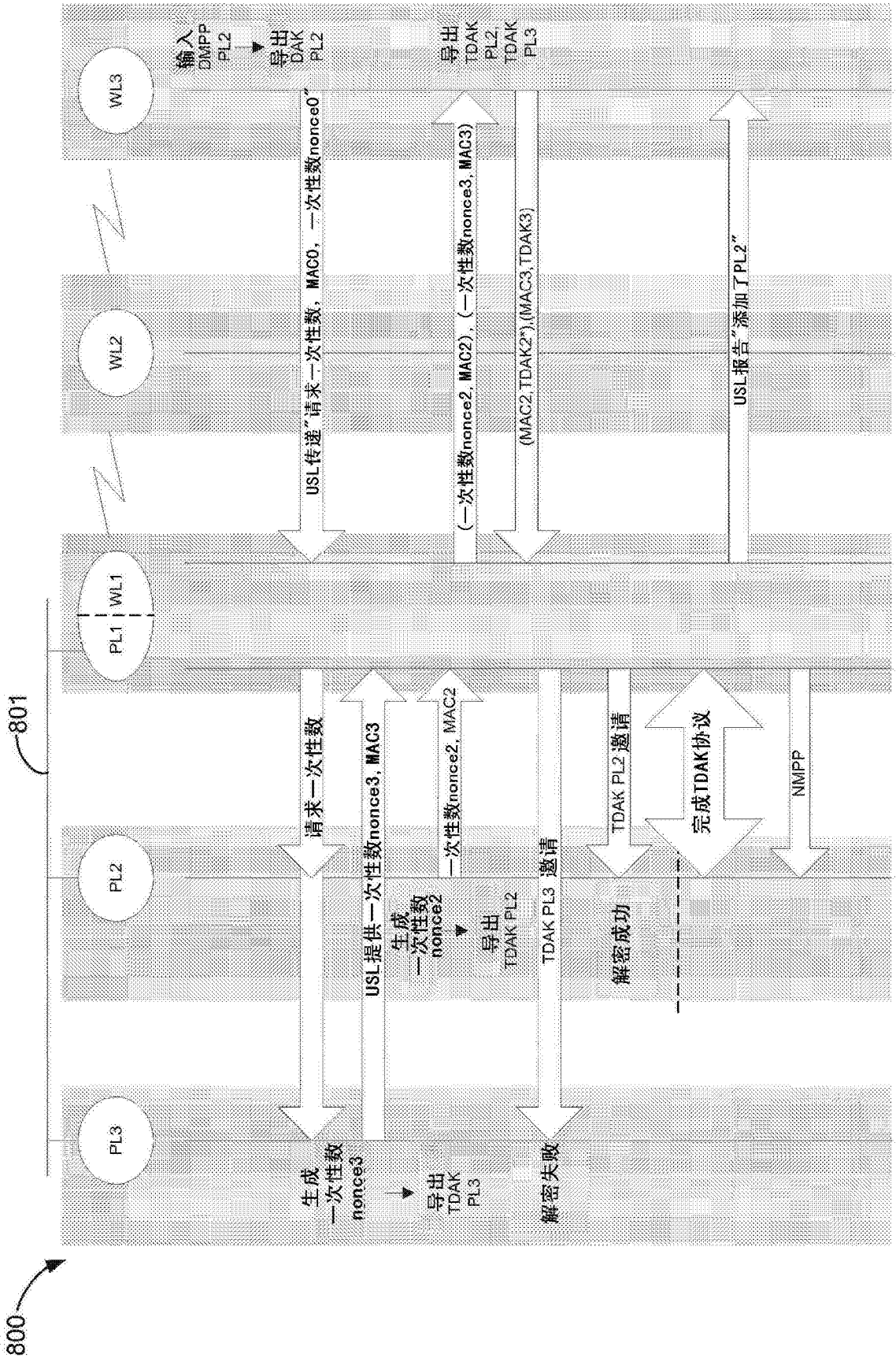

800
801
WL3
WL2
WL1
PL3
PL2
PL1
输入 DMPP PL2
导出 DAK PL2
导出 TDAK PL2, TDAK PL3
USL传递"请求一次性数，MAC0，一次性数nonce0"
(一次性数nonce2, MAC2)，(一次性数nonce3, MAC3)
(MAC2,TDAK2*),(MAC3,TDAK3)
USL报告"添加了PL2"
请求一次性数
USL提供一次性数nonce3, MAC3
一次性数nonce2, MAC2
生成 一次性数 nonce2
导出 TDAK PL2
TDAK PL3 邀请
TDAK PL2 邀请
完成TDAK协议
NMPP
解密成功
生成 一次性数 nonce3
导出 TDAK PL3
解密失败

图8