

一种通信方法及装置

相关申请的交叉引用

本申请要求在2021年5月10日提交中华人民共和国知识产权局、申请号为202110504785.6、发明名称为“一种通信方法及装置”的中国专利申请的优先权，其全部
5 内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种通信方法及装置。

背景技术

在无线通信领域，为了低吞吐量的机器类型通信设备，4G技术中定义了省电的安全方案，称为为低吞吐量机器类型通信设备设计的省电安全(battery efficient security for very low throughput machine type communication devices, BEST)。其主要目的是通过4G网络架构中的
10 归属公共陆地移动网(home public land mobile network, HPLMN)安全节点(HPLMN security endpoint, HSE)与用户设备(user equipment, UE)分别根据UE的加密密钥(cipher key, CK)和完整性密钥(integrity key, IK)推导出用于保护UE数据的安全密钥，用于
15 保护UE的数据安全。

然而，在5G架构下，HSE是不能获取到UE的CK和IK的，无法根据CK和IK推导安全密钥，因此，4G技术的BEST认证方式不能完全适用在5G架构，导致UE的数据
20 安全风险增加。

发明内容

本申请实施方式的目的在于提供一种通信方法及装置，用以提供适用于5G等网络架构的安全密钥获取方式，以降低5G等网络架构下用户设备的数据安全风险。

第一方面，本申请实施例提供一种通信方法。该方法可由归属网络安全节点执行，包括：归属网络安全节点可接收来自用户设备的第一请求，第一请求包括用户设备的第一标识。归属网络安全节点还可向第一网络功能发送第二请求，第二请求包括用户设备的第二标识，第二标识根据第一标识确定，或者第二标识与第一标识相同。归属网络安全节点接收来自于第一网络功能的第一密钥，第一密钥根据加密密钥、完整性密钥和第一信息生成。
25 归属网络安全节点可根据第一密钥生成第二密钥，第二密钥包括用户设备与归属网络安全节点之间的机密性保护密钥和/或完整性保护密钥。其中，第一信息包括：用户设备的服务网络名称、归属网络安全节点的标识、用户设备的SUPI，以及BEST服务标识中的至少一个。
30

通过上述方法，归属网络安全节点可获取第一密钥，其中，第一密钥是根据加密密钥、完整性密钥和第一信息生成的，因此，归属网络安全节点不需要获取UE的加密密钥和完整性密钥就能够获得第一密钥，后续可根据第一密钥生成用于保护用户设备数据的安全密钥。因此该方案能够提供适用于5G及其他网络架构的安全密钥获取方式，能够降低用户设备的数据安全风险。
35

一种可能的设计中，用户设备的第一标识包括用户设备的SUCI，用户设备的第二标识包括用户设备的SUPI，归属网络安全节点向第一网络功能发送第二请求之前，还可包括：归属网络安全节点根据SUCI获取用户设备的SUPI。或者，归属网络安全节点根据归属网
40

络安全节点的私钥解密 SUCI 获得 SUPI, 其中, SUCI 是根据归属网络安全节点的公钥加密 SUPI 获得的。

一种可能的设计中, 用户设备的第一标识包括归属网络安全节点为用户设备分配的标识, 用户设备的第二标识包括用户设备的 SUPI, 归属网络安全节点向第一网络功能发送第二请求之前, 还可包括: 归属网络安全节点根据归属网络安全节点为用户设备分配的标识获取用户设备的 SUPI。

一种可能的设计中, 归属网络安全节点根据 SUCI 获取用户设备的 SUPI, 可包括: 归属网络安全节点向第一网络功能发送用户设备的 SUCI; 归属网络安全节点接收来自于第一网络功能的 SUPI。

一种可能的设计中, 如果第二标识与第一标识相同, 则第一标识包括用户设备的 SUCI 和/或 SUPI。

通过上述方法, 用户设备与归属网络安全节点之间基于用户设备的 SUCI、SUPI 或归属网络安全节点为 UE 分配的标识进行通信, 而可以不使用 IMSI 进行通信, 以适用于 5G 等网络架构下的通信方式。另外, 通过 SUCI 进行认证和密钥推导能够进一步提高安全性。

一种可能的设计中, 第二请求为用户设备认证获取请求, 用户设备认证获取请求还可包括指示信息, 指示信息用于指示根据加密密钥、完整性密钥和第一信息生成第一密钥。

一种可能的设计中, 第一请求还包括用户设备的服务网络名称, 第二请求还包括服务网络名称。

一种可能的设计中, 第一网络功能包括认证服务功能或统一数据管理功能。

一种可能的设计中, 归属网络安全节点可向用户设备发送随机数和/或认证令牌。

一种可能的设计中, 归属网络安全节点根据第一密钥生成第二密钥, 包括: 归属网络安全节点根据第一密钥和第二信息生成第二密钥, 第二信息包括以下中的至少一个: 归属网络安全节点的标识、用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数, 或者认证令牌。第二信息可来自于第一网络功能。

一种可能的设计中, 第一请求还包括加密指示, 还可包括: 归属网络安全节点开启加密服务。若开启加密服务, 则第二密钥包括机密性保护密钥。

一种可能的设计中, 在归属网络安全节点根据第一密钥生成第二密钥之前, 还可包括: 归属网络安全节点接收来自于第一网络功能的加密指示; 归属网络安全节点根据加密指示判断是否开启用户设备的用户面加密服务。

第二方面, 提供一种通信方法。该通信方法可由统一数据管理功能执行, 包括: 统一数据管理功能接收来自于归属网络安全节点的第二请求, 第二请求包括用户设备的第二标识。统一数据管理功能可根据第二标识生成用户设备的加密密钥和完整性密钥, 并根据加密密钥、完整性密钥和第一信息生成第一密钥。统一数据管理功能可向归属网络安全节点发送第一密钥。其中, 第一信息包括: 用户设备的服务网络名称、归属网络安全节点的标识、用户设备的 SUPI, 以及 BEST 服务标识中的至少一个。

一种可能的设计中, 该方法还可包括: 统一数据管理功能接收来自于归属网络安全节点的用户设备的 SUCI; 统一数据管理功能根据 SUCI 确定用户设备的 SUPI; 统一数据管理功能向归属网络安全节点发送用户设备的 SUPI。

一种可能的设计中，第二标识可包括用户设备的 SUCI 或 SUPI。

一种可能的设计中，该方法还可包括：统一数据管理功能向归属网络安全节点发送加密指示。

5 一种可能的设计中，第二请求为用户设备认证获取请求，用户设备认证获取请求还包括指示信息，统一数据管理功能根据加密密钥和完整性密钥和第一信息生成第一密钥，可包括：统一数据管理功能在收到指示信息后，根据加密密钥和完整性密钥和第一信息生成第一密钥。

一种可能的设计中，第二请求还可包括用户设备的服务网络名称。

10 或者，方法还可包括：统一数据管理功能根据第二标识确定用户设备的注册的或认证的或所在的服务网络名称。

一种可能的设计中，统一数据管理功能可向归属网络安全节点发送第二信息，第二信息包括以下中的至少一个：归属网络安全节点的标识、用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数，或者认证令牌。

15 第三方面，提供一种通信方法。该通信方法可由用户设备执行，包括：用户设备向归属网络安全节点发送第一请求，第一请求包括用户设备的标识。用户设备还可接收归属网络安全节点发送的随机数。用户设备可根据随机数以及用户设备的根密钥生成加密密钥和完整性密钥，用户设备根据加密密钥、完整性密钥和第一信息生成第一密钥，并
20 根据第一密钥生成第二密钥。第二密钥包括用户设备与归属网络安全节点之间的机密性保护密钥和/或完整性保护密钥。其中，第一信息包括：用户设备的服务网络名称、归属网络安全节点的标识、用户设备的 SUPI，以及 BEST 服务标识中的至少一个。

一种可能的设计中，用户设备根据第一密钥生成第二密钥，可包括：根据第一密钥和第三信息生成第二密钥；第三信息包括以下中的至少一个：归属网络安全节点的标识、
25 用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数，或者认证令牌。

一种可能的设计中，第一请求还包括用户设备的服务网络名称；和/或第一请求还包括加密指示，加密指示用于指示用户设备请求用户面加密服务。

30 一种可能的设计中，用户设备的标识包括用户设备的 SUCI、SUPI 或归属网络安全节点为用户设备分配的标识。

35 第四方面，本申请实施例提供一种通信装置，所述通信装置包括处理器，所述处理器与存储器耦合，其中：存储器用于存储指令；处理器用于根据执行存储器存储的指令，以执行上述第一方面至第三方面或以上方面中任一种可能的设计中的方法。可选的，所述通信装置还可以包括所述存储器。可选的，所述通信装置还可以包括收发器，用于支持所述通信装置进行上述方法中的信息发送和/或接收。可选的，该通信装置可以是终端设备，也可以是终端设备中的装置，如芯片或者芯片系统，其中所述芯片系统包含至少一个芯片，所述芯片系统还可以包括其他电路结构和/或分立器件。

40 第五方面，本申请实施例提供一种通信装置，用于实现上述第一方面至第三方面或以上方面中任一种可能的设计中的方法，包括相应的功能模块，例如包括处理单元、通信单

元等，分别用于实现以上方法中的步骤。

第六方面，本申请实施例提供一种计算机可读存储介质，所述计算机存储介质中存储有计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得通信装置执行第一方面至第三方面或以上方面中任一种可能的设计中的方法。

第七方面，本申请实施例提供一种计算机程序产品，当计算机读取并执行所述计算机程序产品时，使得通信装置执行第一方面至第三方面或以上方面中任一种可能的设计中的方法。

第八方面，本申请实施例提供一种芯片，所述芯片与存储器相连，用于读取并执行所述存储器中存储的软件程序，以执行第一方面至第三方面或以上方面中任一种可能的设计中的方法。

第九方面，本申请实施例提供一种通信装置，包括处理器，所述处理器用于与收发器耦合，读取并执行所述存储器中的指令，以执行第一方面至第三方面或以上方面中任一种可能的设计中的方法。

第十方面，本申请实施例提供一种通信系统，包括用于执行第一方面或第一方面中任一种可能的设计中的方法的装置、用于执行第二方面或第二方面中任一种可能的设计中的方法的装置，和用于执行第三方面或第三方面中任一种可能的设计中的方法的装置。

以上第二方面至第十方面的有益效果可以参照第一方面中有益效果的描述。

附图说明

- 图 1 为本申请实施例提供的一种通信系统的架构示意图；
- 图 2 为 4G BEST 方案的网络架构示意图；
- 图 3 为 4G BEST 方案的密钥架构示意图；
- 图 4 为本申请实施例提供的一种通信系统的架构示意图；
- 图 5 为本申请实施例提供的一种通信方法的流程示意图；
- 图 6 为本申请实施例提供的另一种通信方法的流程示意图；
- 图 7 为本申请实施例提供的另一种通信方法的流程示意图；
- 图 8 为本申请实施例提供的另一种通信方法的流程示意图；
- 图 9 为本申请实施例提供的另一种通信方法的流程示意图；
- 图 10 为本申请实施例提供的另一种通信方法的流程示意图；
- 图 11 为本申请实施例提供的一种通信装置的结构示意图；
- 图 12 为本申请实施例提供的另一种通信装置的结构示意图。

具体实施方式

为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。

下面对本申请涉及术语进行解释：

至少一个，是指一个，或一个以上，即包括一个、两个、三个及以上。

多个，是指两个，或两个以上，即包括两个、三个及以上。

携带，可以是指某消息用于承载某信息或数据，也可以是指某消息由某信息构成。

耦合是指装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。

本申请实施例中，“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 的情况，其中 A、B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一（项）个”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a、b 或 c 中的至少一项（个），可以表示：a，b，c，a 和 b，a 和 c，b 和 c，或 a、b 和 c，其中 a、b、c 可以是单个，也可以是多个。

下面，结合附图对本申请实施例进行详细说明。首先，介绍本申请实施例提供的无线通信系统，本申请提供的中的通信方法可应用于该系统，然后介绍本申请实施例提供的通信方法，最后介绍本申请实施例提供的通信装置。

如图 1 所示，本申请实施例提供的无线通信系统 100 可包括终端设备 101 以及网络设备 102。

应理解，本申请实施例提供的无线通信系统 100，即可适用于低频场景（sub 6G），也适用于高频场景（above 6G）。本申请实施例提供的无线通信系统 100 的应用场景包括但不限于宽带码分多址（wideband code division multiple access, WCDMA）系统、通用分组无线业务（general packet radio service, GPRS）、长期演进（long term evolution, LTE）系统、LTE 频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）、通用移动通信系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）通信系统、第五代系统或新无线（new radio, NR）通信系统等。

以上所示终端设备 101 可以是用户设备、终端（terminal）、移动台（mobile station, MS）、移动终端（mobile terminal）等设备，该终端设备 101 能够与一个或多个通信系统的一个或多个网络设备进行通信，并接受网络设备提供的网络服务，这里的网络设备包括但不限于图示网络设备 102。举例来说，本申请实施例中的终端设备 101 可以是移动电话（或称为“蜂窝”电话）、具有移动终端的计算机等，终端设备 101 还可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置。终端设备 101 也可以是具有通信模块的通信芯片。

以上所示网络设备 102 可包括本申请所述的接入网设备（或称接入网站点）。具体的，网络设备 102 可包括接入网设备。在本申请中，接入网设备是指有提供网络接入功能的设备，如无线接入网（radio access network, RAN）基站等等。网络设备 102 具体可包括基站（base station, BS），或包括基站以及用于控制基站的无线资源管理设备等，该网络设备 102 可以为中继站（中继设备）、接入点、车载设备、可穿戴设备以及未来 5G 等网络中的基站、未来演进的公共陆地移动网络（public land mobile network, PLMN）网络中的基站或者 NR 基站等，本申请实施例并不限定。网络设备 102 也可以是具有通信模块的通信芯片。

在本申请所述方法的执行过程中，网络设备 102 可作为 RAN 基站向终端设备 101 提供无线网络连接，例如，网络设备 102 可作为 4G 接入网——演进的通用移动通信系统（universal mobile telecommunications system, UMTS）陆地无线接入网（evolved UMTS terrestrial radio access network, E-UTRAN）中的接入网基站，或者，网络设备 102 可作为 5G 接入网——5G RAN 中的接入网基站，或者，网络设备 102 可作为未来无线通信系统中

的接入网基站。

目前，4G 为低吞吐量的机器类型通信设备定义了省电的安全方案，称为 BEST，图 2 描述了该方案的网络架构。主要目的是通过 HSE 完成与 UE 的认证以及密钥生成，从而推导出用于保护 UE 数据的安全密钥，密钥整体架构如图 3 所示。

5 其中，4G 网络架构下，HSE 与归属用户服务器（home subscriber server，HSS）之间的交互存在两种可能性，一种是 HSE 与 HSS 之间通过接口直接交互，一种是经过端到中间密钥服务器（end to middle key server，EMKS）与 HSS 交互。为了简化表达，本申请后续所述流程均以第一种方式为代表，但实际应用 HSE 可以通过 EMKS 与 HSS 进行交互。

10 基于图 4 架构，根据 UE 到企业应用服务器（enterprise application server，EAS）数据保护方式的不同，UE 和 HSE 会生成不同的密钥：

一种保护方式中，UE 和 EAS 进行端到端（end to end，E2E）保护，此时 HSE 需要为 EAS 生成中间密钥和 EAS 特定的预共享密钥，即图 3 中的 $K_{Intermediate}$ 和 K_{EAS_PSK} 。然后 EAS 与 UE 根据 K_{EAS_PSK} 再生成 E2E 安全密钥，即图 3 中农的 K_{E2Eenc} 和 K_{E2Eint} ，分别为机密性保护密钥和完整性保护密钥。

15 另一种保护方式中，UE、HSE 和 EAS 进行逐跳（hop-by-hop）保护，此时 HSE 只需要生成其与 UE 之间的安全密钥，即图 3 中的 K_{E2Menc} 和 K_{E2Mint} 。

其中，在上述方式中的密钥生成过程中，UE 可携带 IMSI 向 HSE 请求建立会话，HSE 判断该 UE 是否需要生成密钥，也就是判断是否有该 UE 的具备有效计数器值的有效密钥，判断的方式具体如下：

20 情况 1）如果 HSE 拥有指示的会话的有效密钥集，且 UE ID 对该会话有效，那么 HSE 可以开始 BEST 会话，而无需重新协商密钥。

情况 2）如果 UE ID 对 HSE 来说有效，但 HSE 没有指示的会话的有效密钥集，或 HSE 希望更新密钥，那么 HSE 则需要与 UE 先重新协商密钥，再发起 BEST 会话。

25 情况 3）如果 UE ID 对该会话 ID 无效，或者 UE 不支持 HSE 要求的服务级别，或者企业信息对 HSE 无效，则 HSE 可能会拒绝该命令。

为简化表达，本申请后续将上述判断是否有该 UE 的具备有效计数器值的有效密钥过程称为 HSE 判断该 UE 是否已有合法的密钥，且对上述情况 2）称为 HSE 判断 UE 没有合法的密钥，如果没有则 HSE 会从 HSS 获取鉴权向量，鉴权向量包括随机数（RAND）、认证令牌（AUTN）、CK 和 IK，HSE 根据鉴权向量计算 HSE 密钥。HSE 会向 UE 发送 RAND 和 AUTN 供 UE 认证，UE 校验 AUTN 成功后，可以向 HSE 返回验证数据（RES）供 HSE 30 校验，也可以不返回。认证成功后，UE 和 HSE 会根据 CK 和 IK 推导生成其他密钥，包括但不限于 K_{E2Eenc} 、 K_{E2Eint} 、 K_{E2Menc} 和 K_{E2Mint} 。

目前，在将 BEST 服务引用到 5G 网络架构时，存在不兼容的问题，下面结合 5G 网络架构进行说明。

35 如图 4 所示，5G 网络架构可包括三部分，分别是 UE、数据网络（data network，DN）和运营商网络。

其中，运营商网络可包括网络切片选择（network slice selection function，NSSF）、网络开放功能（network exposure function，NEF）、网络存储功能（network function repository function，NRF）、策略控制功能（policy control function，PCF）、统一数据管理（unified data management，UDM）、应用功能（application function，AF）、网络切片特定鉴权和授权功 40

能 (network slice specific authentication and authorization function, NSSAAF)、鉴权服务器功能 (authentication server function, AUSF)、接入与移动性管理功能 (access and mobility management function, AMF)、会话管理功能 (session management function, SMF)、(无线) 接入网 ((radio)access network, (R)AN)、HSE、EAS 以及用户面功能 (user plane function, UPF) 等网络功能 (network function, NF)。上述运营商网络中, 除 (无线) 接入网部分之外的部分可以称为核心网络 (CN) 部分。为方便说明, 后续以 (R)AN 称为 RAN 为例进行说明。

本申请中, 用户设备可以包括图 4 所示 UE。UE 可以是一种具有无线收发功能的设备, 其可以部署在陆地上, 包括室内或室外、手持或车载; 也可以部署在水面上 (如轮船等); 还可以部署在空中 (例如飞机、气球和卫星上等)。所述 UE 可以是手机 (mobile phone)、平板电脑 (pad)、带无线收发功能的电脑、虚拟现实 (virtual reality, VR) 终端、增强现实 (augmented reality, AR) 终端、工业控制 (industrial control) 中的无线终端、无人驾驶 (self driving) 中的无线终端、远程医疗 (remote medical) 中的无线终端、智能电网 (smart grid) 中的无线终端、运输安全 (transportation safety) 中的无线终端、智慧城市 (smart city) 中的无线终端、智慧家庭 (smart home) 中的无线终端等。UE 还可以是图 1 所示终端设备 101。

上述 UE 可通过运营商网络提供的接口 (例如 N1 等) 与运营商网络建立连接, 使用运营商网络提供的数据和/或语音等服务。UE 还可通过运营商网络访问 DN, 使用 DN 上部署的运营商业务, 和/或第三方提供的业务。其中, 上述第三方可为运营商网络和 UE 之外的服务方, 可为 UE 提供他数据和/或语音等服务。其中, 上述第三方的具体表现形式, 具体可根据实际应用场景确定, 在此不做限制。

此外, 本申请中的归属网络安全节点, 可包括图 4 所示 HSE, 在未来通信如 6G 中, 归属网络安全节点仍可以是 HSE, 或有其它的名称, 本申请不做限定。认证服务功能可包括图 4 所示 AUSF, 在未来通信如 6G 中, 认证服务功能仍可以是 AUSF, 或有其它的名称, 本申请不做限定。统一数据管理功能可包括图 4 所示 UDM, 在未来通信如 6G 中, 统一数据管理功能仍可以是 UDM, 或有其它的名称, 本申请不做限定。

图 4 中 Nnssf、Nnef、Nausf、Nnrf、Npcf、Nudm、Naf、Namf、Nssaaf、Nsmf、Nhse、N1、N2、N3、N4、N6、BEST-C、BEST-U、EAS-C, 以及 EAS-U 分别为接口序号。这些接口序号的含义和用途可参见 3GPP 标准协议中定义的含义, 在此不做限制。

在图 4 所示 5G 网络架构中, 仍可通过 HSE 对 UE 的数据进行认证和保护, 但是, 由于 5G 网络架构中, HSE 无法获得 CK 和 IK, 因此无法沿用 4G 网络架构下密钥的生成方式由 HSE 根据 CK 和 IK 生成密钥, 造成将 4G 网络架构下的 BEST 服务引用到 5G 网络架构时的不兼容问题。

为了解决该技术问题, 使得 BEST 服务能够在 5G 中实施, 本申请实施例提供一种通信方法。该方法可由用户设备、归属网络安全节点和第一网络功能实施。其中, 第一网络功能可以是认证服务功能和/或统一数据管理功能。下面为了方便说明, 以用户设备是 UE, 归属网络安全节点是 HSE, 认证服务功能是 AUSF 以及统一数据管理功能是 UDM 为例进行说明。

如图 5 所示, 该方法可包括以下步骤:

S101: UE 向 HSE 发送第一请求, 第一请求包括 UE 的第一标识。

相应地，HSE 接收来自 UE 的第一请求，第一请求包括 UE 的第一标识。

可选的，第一请求为会话建立请求或称会话请求，则本申请实施例提供的方法可结合会话建立过程实施，用于为 UE 的该会话提供数据安全保护。

5 S102: HSE 向第一网络功能发送第二请求，第二请求包括 UE 的第二标识。第一网络功能可以是 AUSF 和/或 UDM。第二请求例如是认证向量获取请求。认证向量可以是包括密钥或用于推导密钥的参数的集合。

其中，第二标识可根据第一标识确定，例如，第一标识可以是 UE 的用户隐藏标识 (subscription concealed identifier, SUCI)，则第二标识可以是根据该 SUCI 确定的 UE 的用户永久标识 (subscription permanent identifier, SUPI)。又如，第一标识可以是 HSE 为 UE
10 分配的标识，第二标识可以是 UE 的 SUPI。

另外，第二标识也可以与第一标识相同，例如，第一标识和第二标识均为 UE 的 SUCI，或均为 UE 的 SUPI。

相应地，第一网络功能接收来自于 HSE 的第二请求，第二请求包括 UE 的第二标识。

可选的，如果第一网络功能包括 UDM，第二请求可由 HSE 发送至 UDM。如果第一
15 网络功能为 AUSF，第二请求可由 HSE 发送至 AUSF，之后由 AUSF 向 UDM 发送新的请求，该新的请求内容可以与第二请求相同。

S103: 第一网络功能根据 UE 的第二标识生成第一密钥。

其中，如果第一网络功能为 UDM，则 UDM 可根据 UE 的第二标识生成 UE 的 CK 和 IK，并根据 CK、IK 和第一信息生成第一密钥。其中，UDM 可根据 UE 的第二标识获取
20 UE 的长期密钥，然后根据长期密钥生成 UE 的 CK 和 IK，之后 UDM 可根据 CK、IK 和第一信息生成第一密钥。

其中，第一信息包括用户设备的 UE 的服务网络 (serving network, SN) 名称、归属网络安全节点的标识、用户设备的 SUPI，以及 BEST 服务标识中的至少一个。例如，上述
25 第一信息可包括 UE 的服务网络 (serving network, SN) 名称，或者，第一信息可以是 HSE 的标识 (HSE ID)、UE 的 SUPI 以及 BEST 服务标识，或者，第一信息可以是 UE 的服务网络名称、HSE 的标识、UE 的 SUPI 以及 BEST 服务标识。此外，第一信息还可以是由 UE 和 HSE 共享的其他参数，这些参数需要由 HSE 和/或 UE 发送给第一网络功能，例如，HSE 在第二请求中携带这些参数。第一信息还可以是 HSE 确定的参数，HSE 可将这些参数发送至 UE 和第一网络功能。

30 例如，第一网络功能为 UDM，UDM 可使用 CK 和 IK 为密钥，以 UE 的服务网络名称 SQN 异或 AK 为输入参数推导出 Kausf，此时 Kausf 即第一密钥。或者，UDM 使用 CK 和 IK 或 Kausf 为密钥，以 HSE 的标识或 UE 的 SUPI 或 BEST 服务标识为输入参数推导出 Kbest，此时 Kbest 即第一密钥。

如果第一网络功能为 AUSF，则 AUSF 接收第二请求后，向 UDM 发送第四请求，第
35 四请求可携带 UE 的第二标识。UDM 可根据 UE 的第二标识获取 UE 的长期密钥，然后根据长期密钥生成 UE 的 CK 和 IK。UDM 再根据 CK、IK 和第一信息生成第四密钥，第一信息至少包括 UE 的服务网络名称，和/或，HSE 的标识、UE 的 SUPI 或者 BEST 服务标识中的至少一个。UDM 向 AUSF 返回第四密钥。AUSF 根据第四密钥和第一信息生成第一密钥。此一项新还可包括 HSE 的标识、UE 的 SUPI 或者 BEST 服务标识中的至少一个，或
40 包括由 UE 和 HSE 共享的其他参数，或包括 HSE 确定的参数。

例如,第一网络功能为 AUSF,可由 UDM 使用 CK 和 IK 或 Kausf 为密钥,以服务网络名称,和/或, SQN 异或 AK, 和/或, HSE 的标识、UE 的 SUPI 或者 BEST 服务标识中的至少一个为输入参数推导出第四密钥,之后将第四密钥发送至 AUSF,由 AUSF 根据第四密钥生成 Kbest',此时的 Kbest'为第一密钥。

5 如果第一网络功能是 UDM,则第二请求可包括指示信息,第一网络功能会在接收到该指示信息后,执行 S104,即根据加密密钥、完整性密钥和第一信息生成第一密钥。示例性的,指示信息可以是用于指示请求 BEST 的安全参数,如请求 BEST 认证向量或请求 BEST 密钥,或者是用于请求 5G 认证和密钥协商(5G authentication and key agreement, AKA)认证向量或 5G AKA 认证密钥,或者指示请求的认证方法为 5G AKA 或 BEST。

10 需要说明的是,本申请中 UDM 也可以根据指示信息生成 5G AKA 的安全参数或 BEST 的安全参数并在响应中返回所述安全参数,其中安全参数包括所述第一密钥。安全参数还包含认证响应等参数,不作限定。该解释适用本申请所有场景,后续不再赘述。

如果第一网络功能是 AUSF,则第四请求可包括指示信息,UDM 会在接收到该指示信息后,执行 S103,即根据加密密钥、完整性密钥和第一信息生成第一密钥。示例性的,指示信息可以是用于指示请求 BEST 的安全参数,如请求 BEST 认证向量或请求 BEST 密钥,或者是用于请求 5G AKA 认证向量或 5G AKA 认证密钥,或者指示请求的认证方法为 5G AKA 或 BEST。

若第一网络功能是 UDM, HSE 可以使用 UDM 已有的服务,如 UE 认证服务,此时第二请求为 UE 认证获取请求(Nudm_UEAuthentication_Get),则第二请求中需要携带指示信息,UDM 根据指示信息生成并返回第一密钥。本申请还包含在所述 UDM 中定义新的服务,此时第二请求为不同于 UE 认证获取请求中的其他请求,为专用于 BEST 认证的服务请求,此时 UDM 可以根据专用的服务生成并返回第一密钥,而无需在第二请求中携带指示信息。

若第一网络功能为 AUSF,则 AUSF 可以使用 UDM 已有的服务,如 UE 认证服务,此时第四请求为 UE 认证获取请求,则第四请求中需要携带指示信息,UDM 根据指示信息生成并向 AUSF 返回所述 Kausf。本申请还包含在所述 UDM 中定义新的服务,此时第四请求为不同于 UE 认证获取请求中的其他请求,为专用于 BEST 认证的服务请求,此时 UDM 可以根据专用的服务生成并返回所述 Kausf,而无需在第四请求中携带指示信息。其中指示信息可以是 AUSF 携带,也可以是 AUSF 从 HSE 的第二请求中获取,然后携带在第四请求中。

S104: 第一网络功能向 HSE 发送第一密钥。

相应地, HSE 接收来自于第一网络功能的第一密钥。

35 可选的,第一网络功能可向 HSE 发送认证向量,相应地, HSE 接收认证向量。认证向量包括第一密钥。其中,认证向量还可包括随机数、认证令牌和 RES 或 RES*。RES* 是使用 CK||IK 为密钥, UE 的服务网络名称、RAND 和 RES 为输入参数生成的。

S105: HSE 根据第一密钥生成第二密钥。

第二密钥包括 UE 与 HSE 之间的机密性保护密钥和/或完整性保护密钥。

40 其中,如果第一请求中携带加密指示,则第二密钥包括机密性保护密钥,例如,第二密钥包括机密性保护密钥和完整性保护密钥。或者, HSE 接收到来自于第一网络功能的加密指示,则第二密钥包括机密性保护密钥。如果第一请求中未包括加密指示,且 HSE 未接

收到来自于第一网络功能的加密指示，则第二密钥可以是完整性保护密钥，也可以包括机密性保护密钥和完整性保护密钥，只是不开启机密性保护服务，不使用机密性保护密钥即可。

可选的，如果 HSE 接收认证向量，HSE 可根据认证向量生成第二密钥。

- 5 另外，可选的，HSE 在 S101 之后，HSE 判断该 UE 是否已有合法的密钥。如果有，则跳过 S102-S104，执行 S105 即可；否则，如果 HSE 判断 UE 没有合法的密钥，则可以执行 S102-S105。本申请后续，合法的密钥包括第一密钥或第二密钥。

- 10 可选的，UE 的合法的密钥可以是 UE 此前建立会话的过程中 HSE 获取的。HSE 可存储 UE 的 SUPI 与合法密钥之间的对应关系，当接收到第一请求中携带的 SUPI 后，HSE 可根据 SUPI 查询 UE 是否有合法密钥，或者，当接收到第一请求中携带的 UE 的 SUCI 或 HSE 为 UE 分配的标识后，HSE 可根据 UE 的 SUCI 或 HSE 为 UE 分配的标识获得 UE 的 SUPI，并根据 SUPI 查询 UE 是否有合法密钥。

S106: UE 接收随机数。

其中，随机数可由 HSE 发送，例如，S104 之后，HSE 向 UE 发送随机数。

- 15 可选的，随机数携带在会话开始消息中。会话开始消息中还可发送认证令牌。

S107: UE 根据随机数以及 UE 的根密钥生成加密密钥和完整性密钥。

可选的，CK 与 RAND 有关，或者说，CK 根据 RAND 确定。

可选的，IK 与 RAND 有关，或者说，IK 根据 RAND 确定。

S108: UE 根据加密密钥、完整性密钥和第一信息生成第一密钥。

- 20 第一信息和第一密钥可参见 S103 中的说明。

S109: UE 根据第一密钥生成第二密钥，第二密钥包括 UE 与 HSE 之间的机密性保护密钥和/或完整性保护密钥。

可选的，在 S105 和 S108 中，UE 和/或 HSE 可根据第一密钥和第二信息生成第二密钥。

- 25 其中，第二信息可包括 HSE 的标识、UE 的 BEST 服务的算法类型标识符、UE 的用于计算认证令牌的序列号、隐藏密钥（anonymity key，AK）、UE 的 SUPI、随机数或者认证令牌中的至少一个。

- 30 采用以上方法，归属网络安全节点可获取第一密钥，其中，第一密钥是根据加密密钥、完整性密钥和第一信息生成的，因此，归属网络安全节点不需要获取 UE 的加密密钥和完整性密钥就能够获得第一密钥，后续可根据第一密钥生成用于保护用户设备数据的安全密钥。因此该方案能够提供适用于 5G 网络架构的安全密钥获取方式，降低用户设备的数据安全风险。

下面通过举例的方式，说明 S104 和/或 S109 中确定第一密钥的方式。其中，第一密钥可以是 Kausf、Kbest 或者 Kbest'。

- 35 （1）如果第一密钥为 Kausf，Kausf 可根据 CK 和 IK，以及服务网络名称、用于确定 UE 的认证令牌的序列号（sequence number，SQN）或 AK 中的至少一个确定。例如，Kausf 可根据 CK 和 IK、服务网络名称、服务网络名称的长度、SQN 异或 AK、SQN 异或 AK 的长度，通过密钥派生函数（key derivation function，KDF）确定。密钥派生函数例如是安全散列算法 256（secure hash algorithm 256，SHA-256）函数，安全散列算法 256 为基于哈希的消息验证码（hash-based message authentication code，HMAC）算法中的一种。
- 40

本申请中, UE 的服务网络名称可携带在第一请求中发送至 HSE, 并由 HSE 通过第二请求或 AUSF 通过第四请求发送至 UDM。或者, UDM 使用存储的 UE 认证所在的服务网络名称或注册所在的服务网络名称。如果 HSE 在第二请求中或 AUSF 在第四请求携带了 UE 的服务网络名称, UDM 还可根据 UE 认证所在的服务网络名称或注册所在的服务网络名称判断 HSE 中携带的服务网络名称是否正确。

可选的, AK 可以与 RAND 有关, 例如, CK 根据 RAND 确定。

(2) 如果第一密钥为 Kbest, Kbest 是由 Kausf 推演的密钥, 推演方式可以是以 Kausf 为密钥, 额外参数为输入传输, 使用 HMAC 算法生成的新的密钥, 例如, 参照公式 1 确定新的密钥。可选的, 额外参数可以是 HSE 的标识、SUPI、BEST 服务标识等, 不作限定。

此时 HSE 可以直接从 UDM 获取 Kbest 或包括 Kbest 的认证向量, 也可以经过 AUSF 从 UDM 获取 Kbest, 或获取包括 Kbest 的认证向量。如果是后者, UDM 向 AUSF 发送的认证向量可以包括 Kausf、RAND、AUTN、RES 或 RES* 中的至少一个, AUSF 根据 Kausf 进行进一步推导 Kbest。或者也可由 UDM 推导 Kbest, 由 AUSF 向 HSE 转发 Kbest 或转发包括 Kbest 的认证向量。

其中, AUTN 可根据 SQN、AK、AMF 值和 MAC 值推导, AMF 值为 16 比特 (bit) 的字段, 可以是设定的。MAC 值可根据 SQN、RAND 和 AMF 值推导。

(3) 如果第一密钥为 Kbest', 可选的, Kbest' 可根据 CK 和 IK, 以及 UE 的服务网络名称, HSE 的标识、SUPI、BEST 服务标识等中的至少一个确定。

应理解, 以上图 6 所示流程中, CK 也可替换为 CK', 且 IK 可以替换为 IK', 此时 5G 为了系统中的 UE 主认证方式可以是扩展认证协议' 认证和密钥协商 (extensible authentication protocol - authentication and key agreement, EAP-AKA')。其中, CK' 和 IK' 可根据 CK 和 IK 推导。

下面说明 HSE 根据 UE 的第一标识确定 S102 涉及的 UE 的第二标识的方法。

方法 1, 第一标识可以是 SUCI, 第二标识为 SUPI, HSE 可通过 UDM 确定该第二标识。

UDM 可以从 SUCI 中解密获取 SUPI, 因此, 当 HSE 获取第一请求中携带的 SUCI 时, 可向 UDM 发送 UE 的 SUCI, 并请求 UE 的 SUPI, 之后接收 UDM 返回的 SUPI。HSE 可向 UDM 发送第三请求, 其中携带 UE 的 SUCI, 该第三请求可以是 UE 标识获取请求, UDM 在解密出 SUPI 后可向 HSE 发送 UE 标识获取响应消息, 其中携带 UE 的 SUPI。

方法 2, 第一标识可以是 SUCI, 第二标识为 SUPI, HSE 可在本地对第一标识进行处理后获得第二标识。

由于 SUCI 可以是 SUPI 加密获得的, 则可以令 HSE 存储可用于解密 SUCI 以获得 SUPI 的密钥。例如, UE 根据 HSE 的公钥加密 SUPI 获得 SUCI, 并在第一请求中携带 SUCI, 在接收到第一请求后, HSE 可根据 HSE 的私钥解密第一请求中的 SUCI, 获得 UE 的 SUPI。

方法 3, 第一标识可以是 HSE 为 UE 分配的标识, 第二标识为 SUPI, HSE 可在本地对第一标识进行处理后获得第二标识。

HSE 可存储 HSE 为 UE 分配的标识与 UE 的 SUPI 之间的对应关系, 用于确定第一请求中的标识所对应的 UE 的 SUPI。

比如, 在此前 UE 接入网络或此前的建立会话的过程中, HSE 根据 UE 的 SUPI 为 UE 分配了标识, 则 HSE 可存储其为 UE 的标识与 UE 的 SUPI 之间的对应关系, 在发送第二

请求之前, 根据该对应关系确定第一请求中携带的 UE 的标识对应的 UE 的 SUPI。

可选的, 在 S102 之前, 如果 HSE 根据用户设备的第一标识或第二标识, 判断该 UE 已有合法的密钥, 则可跳过 S102-S104, 执行 S105。

如图 6 所示, 基于图 5 所示流程, 如果第一信息包括 UE 的服务网络名称, 则本申请
5 实施例提供的一种示例性的通信方法可包括以下步骤:

S201: UE 向 HSE 发送会话请求, 其中携带 UE 的第一标识。

可选的, 会话请求中还可包括 UE 的服务网络名称和/或加密指示。其中, 加密指示可用于请求加密服务。

S202: HSE 判断该 UE 是否已有合法的密钥, 如果没有, 则执行 S203, 如果有, 则执行
10 S206。

其中, 第一标识为 UE 的 SUPI。或者, 第一标识为 SUCI 或 HSE 分配的标识, 则 HSE 根据第一标识确定 UE 的 SUPI。

S203: HSE 向第一网络功能发送认证向量获取请求, 其中, 携带 UE 的第二标识。可
15 选的, 如果会话请求中包括 UE 的服务网络名称, 则认证向量获取请求可包括 UE 的服务网络名称。

第一网络功能可以是 UDM 或 AUSF, UDM 或 AUSF 的具体实现方式可参见 S103 中的说明。

S204: 第一网络功能根据 UE 的第二标识生成第一密钥, 其中, 第一密钥的生成过程需要第一信息作为输入参数。第一信息至少包括 UE 的服务网络名称。第一信息还可包括
20 HSE 的标识、UE 的 SUPI 或 BEST 服务标识中的至少一个。也就是说, 第一密钥至少根据 UE 的服务网络名称的标识生成。

可选的, 如果第二请求中未携带 UE 的服务网络名称, 则第一网络功能可根据 UE 的第二标识获取 UE 的服务网络名称。比如, 第一网络功能为 UDM, UDM 可根据 UE 的第二标识获取 UE 的服务网络名称。如果第一网络功能为 AUSF, 则 AUSF 可根据 UE 的第二标识向 UDM 查询 UE 的服务网络名称。
25

S205: 第一网络功能向 HSE 发送认证向量获取响应消息, 其中携带认证向量, 认证向量至少包括第一密钥。

可选的, 认证向量还可包括 RAND、AUTN、RES 或 RES*中的至少一个。

可选的, 认证向量获取响应消息还可包括加密指示。

S206: HSE 根据认证向量生成第二密钥。
30

其中, 如果第一请求中包括加密指示, 和/或, HSE 接收到来自于第一网络功能的加密指示 (如携带在认证向量获取响应消息或其他消息中), 则 HSE 根据所述加密指示判断是否开启与 UE 的机密性保护服务。

S207: HSE 向 UE 发送会话开始消息。

其中, 会话开始消息中可包括 RAND, 或者, HSE 通过其他消息向 UE 发送 RAND。RAND 的获取方式可参照已有标准, 本申请不具体限定。
35

可选的, 会话开始消息中携带 HSE 为 UE 分配的标识。

可选的, UE 在接收到会话开始消息后, 可以向 HSE 发送会话开始确认消息。

S208: UE 根据随机数和 UE 的根密钥生成 CK 和 IK。

40 S209: UE 根据 CK、IK 和第一信息生成第一密钥。

这里的第一信息与 S204 中生成第一密钥使用的第一信息相同。

S210: UE 根据第一密钥生成第二密钥。

应理解, S207-S210 与 S206 的时序没有严格限制, 比如, S207-S210 可能在 S206 之前或之后执行。

5 基于图 6 所示流程, UE 和 HSE 可分别获得第二密钥, 其中, 第二密钥的生成过程中至少引入 UE 的服务网络名称, 因此 HSE 不需要获知 CK 和 IK, 能够适用于 5G 网络架构。另外, 图 6 所示方法根据 UE 的第一标识发起, 在 HSE 和第一网络功能之间根据 UE 的第二标识进行, 不需要引入 UE 的 IMSI, 能够更好地适用于 5G 网络架构以支持 5G BEST。如果第一标识是 SUCI, 则进一步满足了 UE 使用 SUCI 进行通信以保护 SUPI 传输安全性的要求。

10 基于图 6 所示流程, 如果需要启用加密服务, UE 可在会话请求中携带加密指示, 则 HSE 可根据加密指示生成机密性保护密钥。

15 如图 7 所示, 基于图 5 所示流程, 如果第一信息不包括 UE 的服务网络名称, 则本申请实施例提供的一种通信方法包括以下步骤:

S301: UE 向 HSE 发送会话请求, 其中携带 UE 的第一标识。

可选的, 会话请求中还可包括 UE 的服务网络名称。其中, UE 的服务网络名称可用于指示获取加密服务。

20 S302: HSE 判断该 UE 是否已有合法的密钥, 如果没有, 则执行 S303, 如果有, 则执行 S306。

其中, 第一标识为 UE 的 SUPI。或者, 第一标识为 SUCI 或 HSE 分配的标识, 则 HSE 根据第一标识确定 UE 的 SUPI。

S303: HSE 向第一网络功能发送认证向量获取请求, 其中, 携带 UE 的第二标识。

25 第一网络功能可以是 UDM 或 AUSF, UDM 或 AUSF 的具体实现方式可参见 S103 中的说明。

S304: 第一网络功能根据 UE 的第二标识生成第一密钥, 其中, 第一密钥的生成过程需要第一信息作为输入参数。第一信息可包括 HSE 的标识、UE 的 SUPI 或 BEST 服务标识中的至少一个。也就是说, 第一密钥至少根据 HSE 的标识、UE 的 SUPI 或 BEST 服务标识中的一个生成。

30 S305: 第一网络功能向 HSE 发送认证向量获取响应消息, 其中携带认证向量, 认证向量至少包括第一密钥。

可选的, 认证向量还可包括 RAND、AUTN、RES 或 RES*中的至少一个。

可选的, 认证向量获取响应消息还可包括加密指示。

S306: HSE 根据认证向量生成第二密钥。

35 其中, 如果第一请求中包括 UE 的服务网络名称, 和/或, HSE 接收到来自于第一网络功能的加密指示 (如携带在认证向量获取响应消息或其他消息中), 则 HSE 根据所述服务网络名称或加密指示, 判断是否开启与 UE 的机密性保护服务。

S307: HSE 向 UE 发送会话开始消息。

40 其中, 会话开始消息中可包括 RAND, 或者, HSE 通过其他消息向 UE 发送 RAND。RAND 的获取方式可参照已有标准, 本申请不具体限定。

可选的, UE 在接收到会话开始消息后, 可以向 HSE 发送会话开始确认消息。

S308: UE 根据随机数和 UE 的根密钥生成 CK 和 IK。

S309: UE 根据 CK、IK 和第一信息生成第一密钥。

这里的第一信息与 S204 中生成第一密钥使用的第一信息相同。

5 S310: UE 根据第一密钥生成第二密钥。

应理解, S307-S310 与 S306 的时序没有严格限制, 比如, S307-S310 可能在 S306 之前或之后执行。

基于图 7 所示流程, UE 和 HSE 可分别获得第二密钥, 其中, 第二密钥的生成过程中至少引入 RAND、AUTN、RES 或 RES* 中的一个, 因此 HSE 不需要获知 CK 和 IK, 能够
10 适用于 5G 网络架构。另外, 图 7 所示方法根据 UE 的第一标识发起, 在 HSE 和第一网络功能之间根据 UE 的第二标识进行, 不需要引入 UE 的 IMSI, 能够更好地适用于 5G 网络架构以支持 5G BEST。如果第一标识是 SUCI, 则进一步满足了 UE 使用 SUCI 进行通信以保护 SUPI 传输安全性的要求。

基于图 7 所示流程, 如果需要启用加密服务, UE 可在会话请求中携带服务网络名称,
15 则 HSE 可根据服务网络名称生成机密性保护密钥。

在本申请实施例提供的另一种通信方法中, 可使用 UE 和 PLMN 主认证中生成的 Kausf 进行隐式的认证, 而不使用 4G BEST 中显式的认证方式。其中, 隐式的认证是指不需要
20 UE 和 HSE 之间不需要进行 AUTN 和 RES 的认证, 显式的认证是指 UE 和 HSE 之间需要先进行 AUTN 和 RES 的认证, 再进行密钥的生成。

此种实施方式的前提是 UE 和网络已完成主认证, UE 和 AUSF 均获取了主认证中的 Kausf。若 UE 签约了 BEST 服务, 则 UDM 在主认证中给 AUSF 返回认证向量时, 也会返回 BEST 指示。其中, 认证向量可包括 Kausf 和 RAND、AUTN 或 RES 中的至少一个。
AUSF 根据该指示将生成的 Kbest 以及密钥标识 (key ID) 推送给 HSE。

25 后续 UE 可以根据 Kausf 生成 Kbest 以及 key ID, 并携带该 key ID 向 HSE 发起会话请求, HSE 则根据 Key ID 找到对应的 Kbest, 即获得 UE 的 Kbest。此时 UE 和 HSE 便也可以共享相同的 Kbest。然后以 Kbest 为根密钥, 推导产生后续 E2M 或 E2E 密钥。Kbest 的生成可以考虑引入 BEST 服务代码, SUPI、HSE ID 等参数; Key ID 的计算可以引入 SUPI、key ID 代码等参数。推导的密钥均可以使用 Kausf。

30 可选的, AUSF 和/或 UE 生成 Kbest 的过程中, 可将 Kausf 作为密钥, 以及以 BEST 服务代码、SUPI 或 HSE 的标识等参数作为额外参数。同理, key ID 的生成过程中可将 Kausf 作为密钥, 以及以 SUPI 或 key ID 代码等参数作为额外参数。

其中, key ID 代码例如与 BEST 临时 UE 标识 (BEST temporary UE identifier, B-TID) 或应用的认证和密钥管理 (authentication and key management for applications, AKMA) 临时 UE 标识 (AKMA temporary UE identifier, A-TID) 等有关, 例如是 B-TID 或者 A-TID 等字符串。
35

如图 8 所示, 在使用 UE 和 PLMN 主认证中生成的 Kausf 进行隐式的认证时, 本申请实施例提供的通信方法可包括以下步骤:

40 S401: UDM 确定 UE 签约 BEST 服务。

其中, UDM 可查询 UDM 的签约数据, 确定 UE 是否签约 BEST 服务。

S402: AUSF 向 UDM 发送 UE 认证获取请求。

其中, 本申请对于 S401 和 S402 的执行时序不进行严格限定。

S403: UDM 向 AUSF 返回 UE 认证获取响应消息, 其中携带 UE 的 SUPI 和指示信息。

5 其中, 指示信息可以是 BEST indication, 即表明 UE 需要使用 BEST 服务。

S404: 在接收到指示信息后, AUSF 根据 Kausf 生成 Kbest 和 key ID。

可选的, AUSF 存储 Kbest 和 key ID 之间的对应关系。

S405: AUSF 向 HSE 发送密钥登记请求, 其中, 携带 UE 的 SUPI、Kbest 和 key ID。

S406: HSE 向 AUSF 返回密钥登记响应。

10 S407: UE 根据 Kausf 生成 Kbest 和 key ID。

其中, S407 可以在 UE 发送会话请求之前或之后执行, 也可以是在生成 Kausf 之后, 不具体限定。比如, 当 UE 希望建立会话, 则生成 Kbest 和 key ID。

S408: UE 向 HSE 发送会话请求, 其中携带 key ID。

S409: HSE 获取来自于 UE 的 key ID 所对应的 Kbest。

15 S410: HSE 根据 Kbest 生成 UE 的安全密钥。

其中, UE 的安全密钥包括机密性保护密钥和/或完整性保护密钥。

S411: HSE 向 UE 发送会话开始消息。

S412: UE 根据 Kbest 生成安全密钥。

其中, UE 的安全密钥包括机密性保护密钥和/或完整性保护密钥。

20 根据图 8 所示流程, HSE 可根据 UE 的 key ID 查询 Kbest, 以根据 Kbest 获得 UE 的机密性保护密钥和/或完整性保护密钥。该过程复用 UE 主认证的结果和密钥来完成 UE 和 HSE 之间的密钥共享, 节省了 UE 和 HSE 单独的认证流程, 从而更匹配 BEST 节能省电的需求。

在本申请实施例提供的另一种通信方法中, 可沿用 4G 网络架构下的密钥生成方式, 25 由 UDM 向 HSE 提供 CK 和 IK, 由 UE 和 HSE 根据 CK 和 IK 生成 BEST 密钥。

可选的, HSE 可向 UDM 发送 UE 认证获取请求, 在收到该 UE 认证获取请求后, 可由 UDM 生成第三密钥, 或者通过 UE 认证服务以外的新的服务生成第三密钥。其中, 第三密钥可包括 CK 和 IK。

30 例如, 如果 UE 认证获取请求中携带指示信息, 则 UDM 可根据该指示信息生成该第三密钥, 否则, UDM 可通过 UE 认证服务以外的其他服务生成第三密钥。这里的指示信息可以是用于指示请求 BEST 的安全参数, 如请求 BEST 认证向量或请求 BEST 密钥, 或者是用于请求 5G 认证和密钥协商认证向量或 5G AKA 认证密钥, 或者指示请求的认证方法为 5G AKA 或 BEST。

此后 UDM 可向 HSE 发送认证向量, 其中包括第三密钥, 还可包括 RAND、AUTN 或 RES 中的至少一个, 由 HSE 接收认证向量后生成 UE 的安全密钥。相应地, UE 根据相同的参数生成安全密钥。其中, UE 的安全密钥包括机密性保护密钥和/或完整性保护密钥。

如图 9 所示, 由 UE 和 HSE 根据 CK 和 IK 生成认证密钥的过程可包括以下步骤:

S501: UE 向 HSE 发送会话请求, 其中携带 UE 的 SUPI。

S502: HSE 根据 UE 的 SUPI 判断该 UE 是否已有合法的密钥。

40 如果有合法的密钥, 则可根据合法的密钥生成 UE 的认证密钥, 之后执行 S506, 否则,

如果没有合法的密钥，则执行 S503。

S503: HSE 向 UDM 发送 BEST 认证向量获取请求，其中携带 UE 的 SUPI。

S504: UDM 在接收到 BEST 认证向量获取请求后，生成第三密钥。

5 S505: UDM 向 HSE 发送 BEST 认证向量获取响应消息，其中携带认证向量，认证向量包括第三密钥，还可包括 RAND、AUTN 或 RES 中的至少一个。

此后，HSE 可根据第三密钥生成 UE 的安全密钥。

其中，UE 的安全密钥包括机密性保护密钥和/或完整性保护密钥。相应地，在 UE 侧可生成相同的 UE 安全密钥，即机密性保护密钥和/或完整性保护密钥。

S506: HSE 向 UE 发送会话开始消息。

10 S507: 可选的，UE 向 HSE 返回会话开始响应消息。

根据图 9 所述方法，可通过从 UDM 获取与 4G BEST 认证向量一致的认证向量，使得 UE 和 HSE 完成认证和密钥生成的同时，能够更好地兼容现有安全设计，因为 UE 侧改动较小。

15 在本申请实施例提供的另一种通信方法中，当 UE 通过 4G 网络接入时，可由 HSE 通过 HSS 获取认证向量，即由 HSS 向 UDM 请求获取认证向量，再由 HSS 发送至 HSE。

其中，当 UE 通过 4G 网络接入时，携带的 UE 的标识为 IMSI。

20 可选的，HSS 可向 UDM 发送 UE 认证获取请求，在收到该 UE 认证获取请求后，可由 UDM 生成第四密钥，或者通过 UE 认证服务以外的新的服务生成第四密钥。例如，如果 UE 认证获取请求中携带指示信息，则 UDM 可根据该指示信息生成该第四密钥，否则，UDM 可通过 UE 认证服务以外的其他服务生成第四密钥。这里的指示信息可以是用于指示请求 BEST 的安全参数，如请求 BEST 认证向量或请求 BEST 密钥，或者是用于请求 5G 认证和密钥协商认证向量或 5G AKA 认证密钥，或者指示请求的认证方法为 5G AKA 或 BEST。其中，第四密钥可包括 CK 和 IK。

25 此后 UDM 可向 HSS 发送认证向量，其中包括第四密钥，还可包括 RAND、AUTN 或 RES 中的至少一个。HSS 将认证向量转发至 HSE，由 HSE 接收认证向量后生成 UE 的安全密钥。相应地，UE 根据相同的参数生成安全密钥。其中，UE 的安全密钥包括机密性保护密钥和/或完整性保护密钥。

如图 10 所示，由 UE 和 HSE 根据 CK 和 IK 生成认证密钥可包括以下步骤：

S601: UE 向 HSE 发送会话请求，其中携带 UE 的 IMSI。

30 S602: HSE 根据 UE 的 IMSI 判断该 UE 是否已有合法的密钥。

如果有合法的密钥，则可根据合法的密钥生成 UE 的认证密钥，之后执行 S608，否则，如果没有合法的密钥，则执行 S603。

S603: HSE 向 HSS 发送认证信息请求，携带 UE 的 IMSI。

S604: HSS 向 UDM 发送 BEST 认证向量获取请求，其中携带 UE 的 IMSI。

35 S605: UDM 在接收到 BEST 认证向量获取请求后，生成第四密钥。

S606: UDM 向 HSS 发送 BEST 认证向量获取响应，其中携带认证向量，认证向量包括第四密钥，还可包括 RAND、AUTN 或 RES 中的至少一个。

S607: HSS 向 HSE 发送认证信息响应消息，该响应消息携带认证向量，认证向量中包括第四密钥，还可包括 RAND、AUTN 或 RES 中的至少一个。

40 此后，HSE 可根据第四密钥生成 UE 的安全密钥。

其中, UE 的安全密钥包括机密性保护密钥和/或完整性保护密钥。相应地, 在 UE 侧可生成相同的机密性保护密钥和/或完整性保护密钥。

S608: HSE 向 UE 发送会话开始消息。

可选的, UE 在收到会话开始消息后, 向 HSE 返回会话开始响应消息。

- 5 根据图 10 所述方法, 可在 UE 通过 4G 网络接入时, 通过 HSS 从 UDM 获取鉴权向量, 能够使得 UE 从 4G 接入时也能使用 5G 凭据访问 BEST 服务。

另外, 类似图 9 所示流程, HSE 也可以直接向 UDM 发送认证服务获取请求, 区别在于这里的认证服务获取请求中携带的是 UE 的 IMSI。

- 10 与上述构思相同, 如图 11 所示, 本申请实施例还提供一种装置 1100 用于实现上述方法。例如, 该装置可以为软件模块或者芯片系统。本申请实施例中, 芯片系统可以由芯片构成, 也可以包含芯片和其他分立器件。该装置 1100 可以包括: 处理单元 1101 和通信单元 1102。

应理解, 该装置可包括以上方法实施例中所示的 HSE、UDM 或 UE, 或者包括具备以上方法实施例中所示的 HSE、UDM 或 UE 的功能的装置。

- 15 本申请实施例中, 通信单元也可以称为收发单元, 可以包括发送单元和/或接收单元, 分别用于执行上文方法实施例中 HSE、UDM 或 UE 发送和接收的步骤。

以下, 结合图 11 至图 10 详细说明本申请实施例提供的通信装置。应理解, 装置实施例的描述与方法实施例的描述相互对应, 因此, 未详细描述的内容可以参见上文方法实施例, 为了简洁, 这里不再赘述。

- 20 通信单元 1102 也可以称为收发器、收发机、收发装置等。处理单元 1101 也可以称为处理器, 处理单板, 处理模块、处理装置等。可选的, 可以将通信单元 1102 中用于实现接收功能的器件视为接收单元, 将通信单元 1102 中用于实现发送功能的器件视为发送单元, 即通信单元 1102 包括接收单元和发送单元。通信单元 1102 有时也可以称为收发机、收发器、或收发电路等。接收单元有时也可以称为接收机、接收器、或接收电路等。发送单元有时也可以称为发射机、发射器或者发射电路等。

- 25 举例来说, 如果该装置 1100 是 HSE, 则通信单元 1102 可用于接收来自 UE 的第一请求, 第一请求包括 UE 的第一标识。通信单元 1102 还可用于向第一网络功能发送第二请求, 第二请求包括 UE 的第二标识, 第二标识根据第一标识确定, 或者第二标识与第一标识相同。通信单元 1102 还可用于接收来自于第一网络功能的第一密钥, 第一密钥根据加密密钥、完整性密钥和第一信息生成。处理单元 1101 可用于根据第一密钥生成第二密钥, 第二密钥包括 UE 与 HSE 之间的机密性保护密钥和/或完整性保护密钥。其中, 第一信息包括 UE 的服务网络名称、HSE 的标识、UE 的 SUPI, 以及 BEST 服务标识中的至少一个。

- 30 可选的, 通信单元和处理单元还可以执行其他操作, 例如通信单元 1102 用于执行上述图 5 至图 10 所示的方法实施例中 HSE 的发送操作和接收操作, 处理单元 1101 用于执行上述图 5 至图 10 所示的方法实施例中 HSE 除了收发操作之外的其他操作, 具体可以参考前面的描述, 在此不再赘述。

- 35 又如, 如果该装置 1100 是 UDM, 则通信单元 1102 可用于接收来自于 HSE 的第二请求, 第二请求包括 UE 的第二标识。处理单元 1101 可用于根据第二标识生成 UE 的加密密钥和完整性密钥, 并根据加密密钥、完整性密钥和第一信息生成第一密钥。通信单元 1102 还可用于向 HSE 发送第一密钥。其中, 第一信息包括 UE 的服务网络名称、HSE 的标识、

40

UE 的 SUPI, 以及 BEST 服务标识中的至少一个。

可选的, 通信单元和处理单元还可以执行其他操作, 例如通信单元 1102 用于执行上述图 5 至图 10 所示的方法实施例中 UDM 的发送操作和接收操作, 处理单元 1101 用于执行上述图 5 至图 10 所示的方法实施例中 UDM 除了收发操作之外的其他操作, 具体可以参考前面的描述, 在此不再赘述。

又如, 如果该装置 1100 是 UE, 则通信单元 1102 可用于备向 HSE 发送第一请求, 第一请求包括 UE 的标识, 以及接收 HSE 发送的随机数。处理单元 1101 可用于根据随机数以及 UE 的根密钥生成加密密钥和完整性密钥, 根据加密密钥、完整性密钥和第一信息生成第一密钥, 并根据第一密钥生成第二密钥。第二密钥包括 UE 与 HSE 之间的机密性保护密钥和/或完整性保护密钥。其中, 第一信息包括 UE 的服务网络名称、HSE 的标识、UE 的 SUPI, 以及 BEST 服务标识中的至少一个。

可选的, 通信单元和处理单元还可以执行其他操作, 例如通信单元 1102 用于执行上述图 5 至图 10 所示的方法实施例中 UDM 的发送操作和接收操作, 处理单元 1101 用于执行上述图 5 至图 10 所示的方法实施例中 UDM 除了收发操作之外的其他操作, 具体可以参考前面的描述, 在此不再赘述。

如图 12 所示为本申请实施例提供的另一种通信装置, 图 12 所示的装置可以为图 11 所示的装置的一种硬件电路的实现方式。该通信装置可适用于前面所示出的流程图中, 执行上述方法实施例中 HSE、UDM 或 UE 的功能。为了便于说明, 图 12 仅示出了该通信装置的主要部件。

装置 1200 还可以包括至少一个存储器 1230, 用于存储程序指令和/或数据。存储器 1230 和处理器 1220 耦合。本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接, 可以是电性, 机械或其它的形式, 用于装置、单元或模块之间的信息交互。处理器 1220 可能和存储器 1230 协同操作。处理器 1220 可能执行存储器 1230 中存储的程序指令。所述至少一个存储器中的至少一个可以包括于处理器中。

图 12 所示的装置 1200 包括至少一个处理器 1220 以及通信接口 1210, 处理器 1220 用于执行存储器 1230 中存储的指令或程序。存储器 1230 中存储的指令或程序被执行时, 该处理器 1220 用于执行上述实施例中处理单元 1101 执行的操作, 通信接口 1210 用于执行上述实施例中通信单元 1102 执行的操作。

在本申请实施例中, 通信接口可以是收发器、电路、总线、模块或其它类型的通信接口。在本申请实施例中, 通信接口为收发器时, 收发器可以包括独立的接收器、独立的发射器; 也可以集成收发功能的收发器、或者是通信接口。

装置 1200 还可以包括通信线路 1240。其中, 通信接口 1210、处理器 1220 以及存储器 1230 可以通过通信线路 1240 相互连接; 通信线路 1240 可以是外设部件互连标准 (peripheral component interconnect, 简称 PCI) 总线或扩展工业标准结构 (extended industry standard architecture, 简称 EISA) 总线等。所述通信线路 1240 可以分为地址总线、数据总线、控制总线等。为便于表示, 图 12 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

本申请还提供了一种通信系统, 用于执行上面任一流程中提供的方法, 如执行图 5 至图 10 中任一流程。该通信系统可包括图 5 所示架构。

本申请还提供了一种计算机可读存储介质, 用于存储计算机程序, 该计算机程序包

括用于执行上面任一流程中提供的方法的指令。

本申请还提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行上面任一流程中提供的方法。

5 本申请还提供一种芯片，包括处理器，所述处理器与存储器耦合，用于执行所述存储器中存储的计算机程序或指令，当所述处理器执行所述计算机程序或指令时，使得上面任一流程中提供的方法被实现。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、光学存储器等）上实施的计算机程序产品的形式。

15 本申请是参照根据本申请的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

20 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

25 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的保护范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1.一种通信方法，其特征在于，包括：

归属网络安全节点接收来自于用户设备的第一请求，所述第一请求包括所述用户设备的第一标识；

5 所述归属网络安全节点向第一网络功能发送第二请求，所述第二请求包括所述用户设备的第二标识，所述第二标识根据所述第一标识确定，或者所述第二标识与第一标识相同；

 所述归属网络安全节点接收来自于所述第一网络功能的第一密钥，所述第一密钥根据加密密钥、完整性密钥和第一信息生成，所述第一信息包括：所述用户设备的服务网络名称、所述归属网络安全节点的标识、所述用户设备的用户永久标识 SUPI，以及为低吞吐量
10 机器类型通信设备设计的省电安全 BEST 服务标识中的至少一个；

 所述归属网络安全节点根据所述第一密钥和第三信息生成第二密钥，所述第三信息包括：归属网络安全节点的标识、用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数，或者认证令牌；

 所述第二密钥包括所述用户设备与所述归属网络安全节点之间的机密性保护密钥和/
15 或完整性保护密钥。

2.如权利要求 1 所述的方法，其特征在于，所述用户设备的第一标识包括所述用户设备的用户隐藏标识 SUCI，所述用户设备的第二标识包括所述用户设备的 SUPI，所述归属网络安全节点向第一网络功能发送第二请求之前，还包括：

20 所述归属网络安全节点根据所述 SUCI 获取所述用户设备的 SUPI。

3.如权利要求 2 所述的方法，其特征在于，所述归属网络安全节点根据所述 SUCI 获取所述用户设备的 SUPI，包括：

25 所述归属网络安全节点根据所述归属网络安全节点的私钥解密所述 SUCI 获得所述 SUPI，其中，所述 SUCI 是根据所述归属网络安全节点的公钥加密所述 SUPI 获得的；

 或者，包括：

 所述归属网络安全节点向所述第一网络功能发送所述用户设备的 SUCI；

 所述归属网络安全节点接收来自于所述第一网络功能的所述 SUPI。

30 4.如权利要求 1-3 中任一所述的方法，其特征在于，所述第二请求为用户设备认证获取请求，所述用户设备认证获取请求还包括指示信息，所述指示信息用于指示根据所述加密密钥、所述完整性密钥和所述第一信息生成所述第一密钥。

35 5.如权利要求 1-4 中任一所述的方法，其特征在于，所述第一请求还包括所述用户设备的服务网络名称，所述第二请求还包括所述服务网络名称。

6.如权利要求 1-5 中任一所述的方法，其特征在于，所述第一网络功能包括认证服务功能或统一数据管理功能。

7.如权利要求 1-6 中任一所述的方法,其特征在于,所述第一请求还包括加密指示,所述加密指示用于指示所述用户设备请求用户面加密服务。

8.一种通信方法,其特征在于,包括:

5 统一数据管理功能接收来自于归属网络安全节点的第二请求,所述第二请求包括用户设备的第二标识;

所述统一数据管理功能根据所述第二标识生成所述用户设备的加密密钥和完整性密钥;

10 所述统一数据管理功能根据所述加密密钥、完整性密钥和第一信息生成第一密钥,所述第一信息包括:所述用户设备的服务网络名称、所述归属网络安全节点的标识、所述用户设备的用户永久标识 SUPI,以及为低吞吐量机器类型通信设备设计的省电安全 BEST 服务标识中的至少一个;

所述统一数据管理功能向所述归属网络安全节点发送所述第一密钥。

15 9.如权利要求 8 所述的方法,其特征在于,还包括:

所述统一数据管理功能接收来自于所述归属网络安全节点的所述用户设备的用户隐藏标识 SUCI;

所述统一数据管理功能根据所述 SUCI 确定所述用户设备的 SUPI;

所述统一数据管理功能向所述归属网络安全节点发送所述用户设备的 SUPI。

20

10.如权利要求 8 或 9 所述的方法,其特征在于,所述第二请求为用户设备认证获取请求,所述用户设备认证获取请求还包括指示信息,所述统一数据管理功能根据所述加密密钥和完整性密钥和第一信息生成第一密钥,包括:

25 所述统一数据管理功能在收到所述指示信息后,根据所述加密密钥和完整性密钥和第一信息生成所述第一密钥。

11.如权利要求 8-10 中任一所述的方法,其特征在于,

所述第二请求还包括所述用户设备的服务网络名称;

或者,所述方法还包括:

30 所述统一数据管理功能根据所述第二标识确定所述用户设备的注册的或认证的或所在的服务网络名称。

12.一种通信方法,其特征在于,包括:

用户设备向归属网络安全节点发送第一请求,所述第一请求包括所述用户设备的标识;

35 所述用户设备接收来自于所述归属网络安全节点的随机数;

所述用户设备根据所述随机数以及所述用户设备的根密钥生成加密密钥和完整性密钥;

40 所述用户设备根据所述加密密钥、完整性密钥和第一信息生成第一密钥,所述第一信息包括:所述用户设备的服务网络名称、所述归属网络安全节点的标识、所述用户设备的用户永久标识 SUPI,以及为低吞吐量机器类型通信设备设计的省电安全 BEST 服务标识中

的至少一个;

所述用户设备根据所述第一密钥和第三信息生成第二密钥,所述第三信息包括: 归属网络安全节点的标识、用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数, 或者认证令牌;

- 5 所述第二密钥包括所述用户设备与所述归属网络安全节点之间的机密性保护密钥和/或完整性保护密钥。

- 13.如权利要求 12 所述的方法, 其特征在于, 所述第一请求还包括所述用户设备的服务网络名称; 和/或所述第一请求还包括加密指示, 所述加密指示用于指示所述用户设备请求用户面加密服务。

14.一种通信装置, 其特征在于, 包括通信单元和处理单元:

所述通信单元用于, 接收来自于用户设备的第一请求, 所述第一请求包括所述用户设备的第一标识;

- 15 所述通信单元还用于, 向第一网络功能发送第二请求, 所述第二请求包括所述用户设备的第二标识, 所述第二标识根据所述第一标识确定, 或者所述第二标识与第一标识相同;

- 所述通信单元还用于, 接收来自于所述第一网络功能的第一密钥, 所述第一密钥根据加密密钥、完整性密钥和第一信息生成, 所述第一信息包括: 所述用户设备的服务网络名称、所述归属网络安全节点的标识、所述用户设备的用户永久标识 SUPI, 以及为低吞吐量机器类型通信设备设计的省电安全 BEST 服务标识中的至少一个;

- 20 所述处理单元用于, 根据所述第一密钥和第三信息生成第二密钥, 所述第三信息包括: 归属网络安全节点的标识、用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数, 或者认证令牌;

- 25 所述第二密钥包括所述用户设备与归属网络安全节点之间的机密性保护密钥和/或完整性保护密钥。

15.如权利要求 14 所述的通信装置, 其特征在于, 所述第一标识包括所述用户设备的用户隐藏标识 SUCI, 所述处理单元还用于:

根据所述 SUCI 获取所述用户设备的 SUPI。

30

16.如权利要求 15 所述的通信装置, 其特征在于, 所述处理单元具体用于:

根据所述归属网络安全节点的私钥解密所述 SUCI 获得所述 SUPI, 其中, 所述 SUCI 是根据所述归属网络安全节点的公钥加密所述 SUPI 获得的;

或者, 所述通信单元还用于:

- 35 向所述第一网络功能发送所述用户设备的 SUCI;

接收来自于所述第一网络功能的所述 SUPI。

- 17.如权利要求 14-16 中任一所述的通信装置, 其特征在于, 所述第二请求为用户设备认证获取请求, 所述用户设备认证获取请求还包括指示信息, 所述指示信息用于指示根据所述加密密钥、所述完整性密钥和所述第一信息生成所述第一密钥。

40

18.如权利要求 14-17 中任一所述的通信装置,其特征在于,所述第一请求还包括所述用户设备的服务网络名称,所述第二请求还包括所述服务网络名称。

19.如权利要求 14-18 中任一所述的通信装置,其特征在于,所述第一网络功能包括认证服务功能或统一数据管理功能。

20.如权利要求 14-19 中任一所述的通信装置,其特征在于,所述第一请求还包括加密指示,所述加密指示用于指示所述用户设备请求用户面加密服务。

21.一种通信装置,其特征在于,包括通信单元和处理单元:

所述通信单元用于,接收来自于归属网络安全节点的第二请求,所述第二请求包括用户设备的第二标识;

所述处理单元用于,根据所述第二标识生成所述用户设备的加密密钥和完整性密钥;

所述处理单元还用于,根据所述加密密钥、完整性密钥和第一信息生成第一密钥,所述第一信息包括:所述用户设备的服务网络名称、所述归属网络安全节点的标识、所述用户设备的用户永久标识 SUPI,以及为低吞吐量机器类型通信设备设计的省电安全 BEST 服务标识中的至少一个;

所述通信单元还用于,向所述归属网络安全节点发送所述第一密钥。

22.如权利要求 21 所述的通信装置,其特征在于,所述通信单元还用于:

接收来自于所述归属网络安全节点的所述用户设备的用户隐藏标识 SUCI;

所述处理单元还用于:

所述统一数据管理功能根据所述 SUCI 确定所述用户设备的 SUPI;

所述通信单元还用于:

向所述归属网络安全节点发送所述用户设备的 SUPI。

23.如权利要求 21 或 22 所述的通信装置,其特征在于,所述第二请求为用户设备认证获取请求,所述用户设备认证获取请求还包括指示信息,所述处理单元具体用于:

在收到所述指示信息后,根据所述加密密钥和完整性密钥和第一信息生成所述第一密钥。

24.如权利要求 21-23 中任一所述的通信装置,其特征在于,所述第二请求还包括所述用户设备的服务网络名称;

或者,所述处理单元还用于:

根据所述第二标识确定所述用户设备的注册的或认证的或所在的服务网络名称。

25.一种通信装置,其特征在于,包括通信单元和处理单元:

所述通信单元用于,向归属网络安全节点发送第一请求,所述第一请求包括所述用户设备的标识;

所述通信单元还用于,接收来自于所述归属网络安全节点的随机数;

所述处理单元用于，根据所述随机数以及所述用户设备的根密钥生成加密密钥和完整性密钥；

5 所述处理单元还用于，根据所述加密密钥、完整性密钥和第一信息生成第一密钥，所述第一信息包括：所述用户设备的服务网络名称、所述归属网络安全节点的标识、所述用户设备的用户永久标识 SUPI，以及为低吞吐量机器类型通信设备设计的省电安全 BEST 服务标识中的至少一个；

所述处理单元还用于，根据所述第一密钥和第三信息生成第二密钥，所述第三信息包括：归属网络安全节点的标识、用户设备的 BEST 服务的算法类型标识符、用户设备中用于计算认证令牌的序列号、隐藏密钥、用户设备的 SUPI、随机数，或者认证令牌；

10 所述第二密钥包括所述用户设备与所述归属网络安全节点之间的机密性保护密钥和/或完整性保护密钥。

26.如权利要求 25 所述的通信装置，其特征在于，所述第一请求还包括所述用户设备的服务网络名称；和/或所述第一请求还包括加密指示，所述加密指示用于指示所述用户设备请求用户面加密服务。

27.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序或指令，当所述计算机程序或指令被计算设备执行时，以使得所述计算设备执行如权利要求 1 至 7 中任一项所述的方法，或使得所述计算设备执行如权利要求 8 至 11 中任一项所述的方法，或使得所述计算设备执行如权利要求 12 或 13 所述的方法。

28.一种通信系统，其特征在于，包括如权利要求 14-20 中任一所述的通信装置，和如权利要求 21-24 中任一所述的通信装置，和如权利要求 25 或 26 所述的通信装置。

25 29.一种计算机程序产品，其特征在于，所述计算机程序产品包括计算机指令，当所述计算机指令被信令保护装置执行时，使得所述信令保护装置执行如权利要求 1 至 7 中任一项所述的方法，或执行如权利要求 8 至 11 中任一项所述的方法，或执行如权利要求 12 或 13 所述的方法。