

安全通信方法及设备

技术领域

本申请涉及通信技术领域，具体涉及安全通信方法及设备。

背景技术

随着网络技术的快速的发展，网络安全成为日益突出的问题。已有的物联网安全框架，可以通过通用引导架构(generic bootstrapping architecture, GBA)技术来建立用户设备(user equipment, UE)与应用功能(application function, AF)服务器之间的安全隧道。其中，GBA技术包括 GBA 认证与密钥协商(authentication and key agreement, AKA)认证。此外，随着第五代移动通信(the 5th generation, 5G)的发展，目前也可以通过 5G 网络来为 UE 与 AF 之间建立安全隧道，即利用 5G 网络实现 UE 和第三方应用服务器之间的安全通信技术，例如，该安全通信技术包括 5G 网络中的应用中认证和密钥协商(authentication and key management for applications, AKMA)技术。

虽然已经有上述的技术用于安全保护用户设备与核心网设备之间交互的信息，但是在现有的通信场景中，例如，在设备到设备(device-to-device, D2D)的通信场景中，用户设备与其他设备之间的交互仍然存在泄漏用户设备的永久标识，从而暴露用户隐私的风险隐患。

综上所述，如何在用户设备与其他设备之间交互的过程中降低泄漏用户设备身份标识以降低暴露用户隐私的风险是本领域技术人员急需解决的技术问题。

发明内容

本申请提供了一种安全通信方法及设备，能够在用户设备与其他设备之间交互的过程中降低泄漏用户设备的永久标识的风险，从而降低暴露用户隐私的风险。

第一方面，本申请提供一种安全通信的方法，该方法包括：

用户设备确定自身与应用功能设备之间的通信数据是否开启机密性保护；

用户设备向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，在没有开启机密性保护的情况下，标识为加密的身份标识。

在本申请中，用户设备在自身与应用功能设备之间的机密性保护未开启的情况下，上述用户面消息中携带的用户设备的标识采用加密的身份标识，该加密的身份标识为用户设备的永久标识经过处理例如加密后得到，或者该加密的身份标识与用户设备的永久标识之间有关联映射关系等等。总之，在用户设备向应用功能设备发送的用户面消息中携带加密的身份标识，而不是携带用户设备的永久标识，能够有效降低泄漏用户设备的永久标识的风险，从而降低暴露用户隐私的风险。

一种可能的实现方式中，该加密的身份标识可以是用户设备的用户隐藏标识(subscription concealed identifier, SUCI)、通用公共用户标识(generic public subscription identifier, GPSI)或者 AKMA 密钥标识(AKMA-key identifier, A-KID)等等。用户设备的永久标识可以是用户永久标识(subscription permanent identifier, SUPI)。

一种可能的实现方式中，上述用户面消息为邻近业务（Prose）流程中的发现请求（Discovery request）。

一种可能的实现方式中，上述方法还包括：用户设备确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互。

在本申请中，用户设备选择具有隐私保护的流程，进一步提高用户设备与应用功能设备之间交互的信息的安全性。

一种可能的实现方式中，上述具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

一种可能的实现方式中，用户设备确定使用具有隐私保护的流程，包括：在满足如下条件中的一项或多项的情况下，用户设备确定使用具有隐私保护的流程：

用户设备启动的应用程序指示用户设备选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，用户设备接收到优先选择具有隐私保护的流程的指示；

或者，用户设备确定自身使用了 5G 全球用户识别卡；

或者，用户设备确定自身中存在有效的公私钥；

或者，用户设备确定用户面消息中需要携带用户设备的永久标识。

本申请提供了多种选择具有隐私保护的流程的方法，能够在需要的情况下尽可能地选择到具有隐私保护的流程，以提高用户设备与应用功能设备之间交互的信息的安全性，降低用户设备永久标识泄密的风险。

一种可能的实现方式中，上述方法还包括：用户设备接收来自应用功能设备的加密算法信息；

上述没有开启机密性保护的情况，包括：加密算法信息指示加密算法为空算法的情况。

在本申请中，用户设备可以通过与应用功能设备协商用于保护该两者之间交互信息的加密算法，在 UE 判断出协商的加密算法为空算法的情况下，上述用户设备发送的用户面消息携带的加密的身份标识，以降低用户设备的永久标识泄密的风险。

第二方面，本申请提供一种安全通信的方法，该方法包括：

用户设备确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；

用户设备基于具有隐私保护的流程确定与应用功能设备的通信密钥和非空加密算法；

用户设备向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，用户面消息由通信密钥和非空加密算法进行机密性保护。

在本申请中，用户设备确定使用具有隐私保护的流程，并在该流程中与应用功能设备协商采用非空加密算法保护该两个设备之间交互的信息，从而降低了用户设备的永久标识泄密的风险。

一种可能的实现方式中，由于用户设备和应用功能设备之间交互的信息有非机密算法机密性保护，那么上述用户面消息中携带的用户设备的标识可以是用户设备加密的身份标识，或者可以是用户设备的永久标识。

一种可能的实现方式中，用户设备确定使用具有隐私保护的流程，包括：在满足如下条件中的一项或多项的情况下，用户设备确定使用具有隐私保护的流程：

用户设备启动的应用程序指示用户设备选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，用户设备接收到优先选择具有隐私保护的流程的指示；

或者，用户设备确定自身使用了 5G 全球用户识别卡；

或者，用户设备确定自身中存在有效的公私钥；

或者，用户设备确定用户面消息中需要携带用户设备的永久标识。

本申请提供了多种选择具有隐私保护的流程的方法，能够在需要的情况下尽可能地选择到具有隐私保护的流程，以提高用户设备与应用功能设备之间交互的信息的安全性，降低用户设备永久标识泄密的风险。

一种可能的实现方式中，用户设备基于具有隐私保护的流程确定与应用功能设备的通信密钥和加密算法，包括：用户设备基于自身存储的锚点密钥生成通信密钥；

用户设备向应用功能设备发送请求消息，请求消息包括密钥标识和指示使用具有隐私保护的流程的信息，密钥标识用于协助应用该功能设备获取通信密钥；

用户设备接收来自应用功能设备的响应消息，响应消息包括上述非空加密算法的信息。

在本申请中，上述请求消息可以是用户设备与应用功能设备之间的密钥协商请求消息，应用功能设备接收到该消息之后，一方面基于消息中的密钥标识获取通信密钥，另一方面，该消息也可以看成是选择非空加密算法的指示消息，应用功能设备基于该消息选择一个非空加密算法，并将该非空加密算法的标识等信息携带在响应消息中发送给用户设备，从而完成了密钥协商的同时完成了非空加密算法的协商。

一种可能的实现方式中，上述请求消息中还包括协商非空加密算法的指示信息。

在本申请中，可以在上述密钥协商请求中携带协商非空加密算法的指示信息，明确指示应用功能设备选择一个非空加密算法，以保证后续的交互信息得到有效的机密性保护。

一种可能的实现方式中，请求消息中还包括用户设备支持的加密算法的信息，用户设备支持的加密算法的信息用于指示应用功能设备选择非空加密算法，用户设备支持的加密算法为非空加密算法。

在本申请中，用户设备向应用功能设备发送请求消息携带的是用户设备支持的非空加密算法的信息，例如是非空加密算法的标识等，应用功能设备基于该请求消息根据自己支持的加密算法集合和用户设备支持的加密算法集合，选择两者都支持的加密算法时，不会选到空的加密算法，从而保证了两者之间的通信信息会受到加密保护。

第三方面，本申请提供一种安全通信的方法，该方法包括：

用户设备确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；

用户设备基于具有隐私保护的流程确定与应用功能设备的通信密钥；

用户设备向应用功能设备发送用户面消息，用户面消息中包括用户设备加密的身份标识；其中，用户面消息由通信密钥进行机密性保护。

在本申请中，用户设备确定选择具有隐私保护的流程来实现与应用功能设备之间的交互，该具有隐私保护的流程中可以使用用户设备的加密的身份标识，因而在用户设备向应用功能设备发送用户面消息时，用户面消息中包括的用户设备标识为用户设备加密的身份标识，从而降低了用户设备的永久标识泄露的风险。本申请相比于上述的方案，不需要协商使用非空加密算法，也不需要判断是否开启了机密性保护，从而可以减少用户设备和/或应用功能设备的资源的占用，减少了用户设备与应用功能设备之间交互的信息还可以减少带宽资源的占用。

一种可能的实现方式中，用户设备确定使用具有隐私保护的流程，包括：在满足如下条件中的一项或多项的情况下，用户设备确定使用具有隐私保护的流程：

用户设备启动的应用程序指示用户设备选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，用户设备接收到优先选择具有隐私保护的流程的指示；

或者，用户设备确定自身使用了 5G 全球用户识别卡；

或者，用户设备确定自身中存在有效的公私钥；

或者，用户设备确定用户面消息中需要携带用户设备的永久标识。

本申请提供了多种选择具有隐私保护的流程的方法，能够在需要的情况下尽可能地选择到具有隐私保护的流程，以提高用户设备与应用功能设备之间交互的信息的安全性，降低用户设备永久标识泄密的风险。

第四方面，本申请提供一种通信方法，该方法包括：

应用功能设备接收来自用户设备的用户面消息，用户面消息包括用户设备加密的身份标识，用户面消息用于请求发起目标流程；

应用功能设备基于加密的身份标识检查用户设备是否被授权参与目标流程。

在本申请中，上述用户面消息携带的是用户设备加密的身份标识，可以有效降低用户设备的永久标识泄露的风险，在此基础上，本申请还可以基于用户设备加密的身份标识检查用户设备是否被授权参与目标流程。

一种可能的实现方式中，上述用户面消息为邻近业务 Prose 流程中的发现请求 Discovery request。那么，检查用户设备是否被授权参与目标流程可是，检查用户设备是否被授权参与 Prose 流程，即检查用户设备是否被授权与邻近的设备通信。

一种可能的实现方式中，应用功能设备基于加密的身份标识检查用户设备是否被授权参与目标流程，包括：

应用功能设备向统一数据管理设备发送第一授权检查请求，第一授权检查请求包括加密的身份标识；

应用功能设备接收来自统一数据管理设备的第一授权检查响应，第一授权检查响应用于指示用户设备是否被授权参与目标流程，第一授权检查响应为基于用户设备的永久标识获得，永久标识为加密的身份标识处理后得到。

在本申请中，即使授权检查请求中携带的是加密的身份标识，统一数据管理设备也能够基于加密的身份标识获取用户设备的永久标识，完成授权的检查。

一种可能的实施方式中，上述第一授权检查响应可以包括用户设备的永久标识。

在本申请中，统一数据管理设备将获得的用户设备的永久标识携带在授权检查响应中反馈给应用功能设备，可以使得应用功能设备后续跟其他核心网网元交互时获得用户设备的其他参数，比如 QoS 信息等。

一种可能的实现方式中，应用功能设备基于加密的身份标识检查用户设备是否被授权参与目标流程，包括：

应用功能设备基于加密的身份标识获取用户设备的永久标识；

应用功能设备向统一数据管理设备发送第二授权检查请求，第二授权检查请求包括永久标识；

应用功能设备接收来自统一数据管理设备的第二授权检查响应，第二授权检查响应用于指示用户设备是否被授权参与目标流程，第一授权检查响应为基于永久标识获得。

在本申请中，应用功能设备可以自己基于加密的身份标识获取用户设备的永久标识，从而进一步可以用于检查用户设备的授权情况。

一种可能的实现方式中，加密的身份标识包括密钥标识；应用功能设备基于加密的身份标识获取用户设备的永久标识之前，还包括：

应用功能设备接收来自应用安全锚功能设备的永久标识，以及接收来自用户设备的密钥标识，将永久标识和密钥标识关联存储。

在本申请中，应用功能设备可以提前存储好用户设备的永久标识和密钥标识之间的映射关系，从而可以在接收到的用户面消息中携带密钥标识时获取用户设备的永久标识，进而检查用户设备的授权情况。

一种可能的实现方式中，加密的身份标识包括用户设备的通用公共用户标识；应用功能设备基于加密的身份标识获取用户设备的永久标识之前，还包括：

应用功能设备接收来自应用安全锚功能设备的通用公共用户标识和永久标识，将通用公共用户标识和永久标识关联存储。

在本申请中，应用功能设备可以提前存储好用户设备的永久标识和通用公共用户标识之间的映射关系，从而可以在接收到的用户面消息中携带用户设备的通用公共用户标识时获取用户设备的永久标识，进而检查用户设备的授权情况。

第五方面，本申请提供一种通信方法，该方法包括：

统一数据管理设备接收来自应用功能设备的第一授权检查请求，第一授权检查请求包

括加密的身份标识；

统一数据管理设备基于加密的身份标识获取用户设备的永久标识，基于永久标识检查用户设备是否被授权参与目标流程；

统一数据管理设备向应用功能设备发送第一授权检查响应，第一授权检查响应用于指示用户设备是否被授权参与目标流程。

在本申请中，即使授权检查请求中携带的是加密的身份标识，统一数据管理设备也能够基于加密的身份标识获取用户设备的永久标识，完成授权的检查。

一种可能的实施方式中，加密的身份标识为用户设备的隐藏标识，统一数据管理设备具体用于：基于隐藏标识获取用户设备的永久标识；

或者，

加密的身份标识为用户设备的通用公共用户标识，统一数据管理设备具体用于：基于通用公共用户标识在本地查找得到用户设备的永久标识；

或者，

加密的身份标识为密钥标识，密钥标识用于标识用户设备的密钥，统一数据管理设备具体用于：基于密钥标识在本地查找得到用户设备的永久标识。

一种可能的实施方式中，在加密的身份标识为密钥标识的情况下，统一数据管理设备基于密钥标识在本地查找得到用户设备的永久标识之前，还包括：

统一数据管理设备从鉴权服务功能设备接收密钥标识，将密钥标识与用户设备的永久标识关联存储。

在本申请中，统一数据管理设备可以提前存储好密钥标识与用户设备的永久标识之间的映射关系，从而可以在接收到的授权检查请求中携带密钥标识时获取用户设备的永久标识，进而检查用户设备的授权情况。

第六方面，本申请提供一种用户设备，所述用户设备包括：

第一确定单元，用于确定用户设备与应用功能设备之间的通信数据是否开启机密性保护；

发送单元，用于向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，在没有开启机密性保护的情况下，标识为加密的身份标识。

一种可能的实施方式中，用户设备还包括：

第二确定单元，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互。

一种可能的实施方式中，具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

一种可能的实施方式中，第二确定单元具体用于：

在满足如下条件中的一项或多项的情况下，确定使用具有隐私保护的流程：

用户设备启动的应用程序指示用户设备选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，用户设备接收到优先选择具有隐私保护的流程的指示；

或者，用户设备确定自身使用了 5G 全球用户识别卡；

或者，用户设备确定自身中存在有效的公私钥；

或者，用户设备确定用户面消息中需要携带用户设备的永久标识。

一种可能的实施方式中，用户设备还包括：

接收单元，用于接收来自应用功能设备的加密算法信息；

没有开启机密性保护的情况，包括：

加密算法信息指示加密算法为空算法的情况。

一种可能的实施方式中，加密的身份标识为用户隐藏标识 SUCI、通用公共用户标识 GPSI 或者密钥标识 A-KID。

一种可能的实施方式中，用户面消息为邻近业务 Prose 流程中的发现请求 Discovery request。

第七方面，本申请提供一种用户设备，所述用户设备包括：

第一确定单元，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；

第二确定单元，用于基于具有隐私保护的流程确定与应用功能设备的通信密钥和非空加密算法；

发送单元，用于向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，用户面消息由通信密钥和非空加密算法进行机密性保护。

一种可能的实施方式中，第一确定单元具体用于：

在满足如下条件中的一项或多项的情况下，确定使用具有隐私保护的流程：

用户设备启动的应用程序指示用户设备选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，用户设备接收到优先选择具有隐私保护的流程的指示；

或者，用户设备确定自身使用了 5G 全球用户识别卡；

或者，用户设备确定自身中存在有效的公私钥；

或者，用户设备确定用户面消息中需要携带用户设备的永久标识。

一种可能的实施方式中，第二确定单元具体用于：

基于自身存储的锚点密钥生成通信密钥；

向应用功能设备发送请求消息，请求消息包括密钥标识和指示使用具有隐私保护的流程的信息，密钥标识用于协助应用该功能设备获取通信密钥；

接收来自应用功能设备的响应消息，响应消息包括非空加密算法的信息。

一种可能的实施方式中，请求消息中还包括协商非空加密算法的指示信息。

一种可能的实施方式中，请求消息中还包括用户设备支持的加密算法的信息，用户设备支持的加密算法的信息用于指示应用功能设备选择非空加密算法，用户设备支持的加密算法为非空加密算法。

第八方面，本申请提供一种用户设备，该用户设备包括：

第一确定单元，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；

第二确定单元，用于基于具有隐私保护的流程确定与应用功能设备的通信密钥；

发送单元，用于向应用功能设备发送用户面消息，用户面消息中包括用户设备加密的身份标识；其中，用户面消息由通信密钥进行机密性保护。

一种可能的实施方式中，具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

一种可能的实施方式中，用第一确定单元具体用于：在满足如下条件中的一项或多项的情况下，确定使用具有隐私保护的流程：

用户设备启动的应用程序指示用户设备选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，用户设备接收到优先选择具有隐私保护的流程的指示；

或者，用户设备确定自身使用了 5G 全球用户识别卡；

或者，用户设备确定自身中存在有效的公私钥；

或者，用户设备确定用户面消息中需要携带用户设备的永久标识。

第九方面，本申请提供一种通信装置，该通信装置可以是用户设备，或者可以是用户设备中的装置，例如芯片系统等。一种设计中，该装置可以包括执行第一方面、第二方面或者第三方面中，以及各种可能性实现方式所描述的方法/操作/步骤/动作所对应的模块，该模块可以是硬件电路，也可以是软件，也可以是硬件电路结合软件实现。一种设计中，该装置可以包括处理模块和收发模块。

对于上述第一方面所述的方法，示例性地，处理模块，用于确定该通信装置与应用功能设备之间的通信数据是否开启机密性保护；

收发模块，用于向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，在没有开启机密性保护的情况下，标识为加密的身份标识。

对于上述第二方面所述的方法，示例性地，处理模块，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；并基于具有隐私保护的流程确定与应用功能设备的通信密钥和非空加密算法；

收发模块，用于向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，用户面消息由通信密钥和非空加密算法进行机密性保护。

对于上述第三方面所述的方法，示例性地，处理模块，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；并基于具有隐私保护的流程确定与应用功能设备的通信密钥；

收发模块，用于向应用功能设备发送用户面消息，用户面消息中包括用户设备加密的身份标识；其中，用户面消息由通信密钥进行机密性保护。

第十方面，本申请提供一种通信装置，该通信装置可以是应用功能设备，或者可以是应用功能设备中的装置，例如芯片系统等。一种设计中，该装置可以包括执行第四方面中，以及各种可能性实现方式所描述的方法/操作/步骤/动作所对应的模块，该模块可以是硬件电路，也可以是软件，也可以是硬件电路结合软件实现。一种设计中，该装置可以包括处理模块和收发模块。

示例性地，处理模块，用于通过收发模块接收来自用户设备的用户面消息，用户面消息包括用户设备加密的身份标识，用户面消息用于请求发起目标流程；基于加密的身份标识检查用户设备是否被授权参与目标流程。

第十一方面，本申请提供一种通信装置，该通信装置可以是统一数据管理设备，或者可以是统一数据管理设备中的装置，例如芯片系统等。一种设计中，该装置可以包括执行第四方面中，以及各种可能性实现方式所描述的方法/操作/步骤/动作所对应的模块，该模块可以是硬件电路，也可以是软件，也可以是硬件电路结合软件实现。一种设计中，该装置可以包括处理模块和收发模块。

示例性地，处理模块，用于通过收发模块接收来自应用功能设备的第一授权检查请求，第一授权检查请求包括加密的身份标识；基于加密的身份标识获取用户设备的永久标识，基于永久标识检查用户设备是否被授权参与目标流程；通过收发模块向应用功能设备发送第一授权检查响应，第一授权检查响应用于指示用户设备是否被授权参与目标流程。

第十二方面，本申请提供一种通信装置，该装置可以是用户设备或者可以是用户设备中的装置，该通信装置包括处理器，用于实现上述第一方面、第二方面或者第三方面描述的方法。该装置还可以包括存储器，用于存储指令和数据。该存储器与该处理器耦合，该处理器执行该存储器中存储的指令时，可以使该装置实现上述第一方面以及第一方面的各个可能实现方式，或第二方面以及第二方面的各个可能实现方式，或第三方面以及第三方面的各个可能实现方式提供的方法。该装置还可以包括通信接口，该通信接口用于该装置与其它设备进行通信，示例性的，通信接口可以是收发器、总线等电路硬件模块，其它设备可以为应用功能设备等。

示例性地，对于上述第一方面所述的方法，在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于确定自身与应用功能设备之间的通信数据是否开启机密性保护；通过通信接口向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，在没有开启机密性保护的情况下，标识为加密的身份标识。

示例性地，对于上述第二方面所述的方法，在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与

应用功能设备之间交互；基于具有隐私保护的流程确定与应用功能设备的通信密钥和非空加密算法；通过通信接口向应用功能设备发送用户面消息，用户面消息中包括用户设备的标识；其中，用户面消息由通信密钥和非空加密算法进行机密性保护。

示例性地，对于上述第三方面所述的方法，在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在用户设备与应用功能设备之间交互；基于具有隐私保护的流程确定与应用功能设备的通信密钥；通过通信接口向应用功能设备发送用户面消息，用户面消息中包括用户设备加密的身份标识；其中，用户面消息由通信密钥进行机密性保护。

第十三方面，本申请提供一种通信装置，该装置可以是应用功能设备或者可以是应用功能设备中的装置，该通信装置包括处理器，用于实现上述第四方面描述的方法。该装置还可以包括存储器，用于存储指令和数据。该存储器与该处理器耦合，该处理器执行该存储器中存储的指令时，可以使该装置实现上述第四方面以及第四方面的各个可能实现方式提供的方法。该装置还可以包括通信接口，该通信接口用于该装置与其它设备进行通信，示例性的，通信接口可以是收发器、总线等电路硬件模块，其它设备可以为用户设备等。

在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于通过通信接口接收来自用户设备的用户面消息，用户面消息包括用户设备加密的身份标识，用户面消息用于请求发起目标流程；基于加密的身份标识检查用户设备是否被授权参与目标流程。

第十四方面，本申请提供一种通信装置，该装置可以是统一数据管理设备或者可以是统一数据管理设备中的装置，该通信装置包括处理器，用于实现上述第五方面描述的方法。该装置还可以包括存储器，用于存储指令和数据。该存储器与该处理器耦合，该处理器执行该存储器中存储的指令时，可以使该装置实现上述第四方面以及第四方面的各个可能实现方式提供的方法。该装置还可以包括通信接口，该通信接口用于该装置与其它设备进行通信，示例性的，通信接口可以是收发器、总线等电路硬件模块，其它设备可以为应用功能设备等。

在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于通过通信接口接收来自应用功能设备的第一授权检查请求，第一授权检查请求包括加密的身份标识；基于加密的身份标识获取用户设备的永久标识，基于永久标识检查用户设备是否被授权参与目标流程；通过通信接口向应用功能设备发送第一授权检查响应，第一授权检查响应用于指示用户设备是否被授权参与目标流程。

第十五方面，本申请提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被执行时使得计算机执行上述第一方面中任一项所述的方法；或者，所述计算机程序被执行时使得计算机执行上述第二方面中任一项所述的方法；所述计算机程序被执行时使得计算机执行上述第三方面中任一项所述的方法；或者，所述计算机程序被执行时使得计算机执行上述第四方面中任一项所述的方法；所述计算机程序被执行时使得计算机执

行上述第五方面中任一项所述的方法。

上述第六方面至第十五方面提供的方案，用于实现或配合实现上述第一方面至第五方面提供的方法，因此可以与第一方面至第五方面达到相同或相应的有益效果，此处不再进行赘述。

综上所述，能够在用户设备与其他设备之间交互的过程中降低泄漏用户设备的永久标识的风险，从而降低暴露用户隐私的风险。

附图说明

图 1 所示为本申请实施例提供的一种安全通信方法使用的系统架构示意图；

图 2 和图 3 所示为用户设备与核心网之间进行身份认真的流程示意图；

图 4 为本申请实施例提供的一种安全通信方法的流程示意图；

图 5A 至图 5D 为本申请实施例提供的安全通信方法的流程示意图；

图 6 至图 9 为本申请实施例提供的安全通信方法的流程示意图；

图 10 至图 12 为本申请实施例提供的装置的逻辑结构示意图；

图 13 为本申请实施例提供的一种通信装置的结构示意图；

图 14 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

为了更好地理解本申请实施例提供的技术方案，首先对本申请实施例涉及的技术术语进行介绍。

1、机密性保护

机密性保护指的是保护信息(该信息可以包括控制面的信令和用户面的数据等)在传输过程中的机密性，也可以称为加密保护，机密性是指无法被直接看出真实内容。本申请所述的机密性保护指的是非空机密性保护，即使用的加密算法为非空加密算法。

2、完整性保护

完整性保护指的是保护信息(该信息可以包括控制面的信令和用户面的数据等)在传输过程中的完整性，完整性是指与原始的信息一致，没有被修改。

3、加密算法

加密算法用于对传输过程的信息(该信息可以包括控制面的信令和用户面的数据等)进行加密。加密算法包括空(null)加密算法和非空加密算法。其中，空加密算法对信息没有实质性的加密，相当于没有加密。非空加密算法则可以对信息进行真正的加密，可以保护信息的机密性。示例性地，非空加密算法可以包括哈希算法、MD5 算法等。

4、完整性保护算法

完整性保护算法用于保护传输过程中的信息的完整性，保证信息不被篡改。完整性保护算法可以和加密算法相同，例如，可以是哈希算法或者 MD5 算法等等。完整性保护算法也可以和加密算法不相同，例如可以是其它的算法：国际数据加密算法(international data encryption algorithm, IDEA)或者对称算法数据加密标准(data encryption standard, DES)等等。

5、传输层安全性(transport layer security, TLS)协议

TLS 协议用于在两个通信应用程序之间提供保密性保护和数据完整性保护。该协议由两层组成：TLS 记录协议 (TLS Record) 和 TLS 握手协议 (TLS Handshake)。

TLS 记录协议是一种分层协议。每一层中的信息可能包含长度、描述和内容等字段。记录协议支持信息传输、将数据分段到可处理块、压缩数据、加密以及传输结果等。对接收到的数据进行解密、校验、解压缩、重组等，然后将它们传送到高层客户机。

TLS 握手协议由三个子协议组构成，允许对等双方在记录层的安全参数上达成一致、自我认证、例示协商安全参数、互相报告出错条件。TLS 握手协议提供的连接安全具有三个基本属性：

1. 可以使用非对称的，或公共密钥的密码术来认证对等方的身份。
2. 共享加密密钥的协商是安全的。对偷窃者来说协商加密是难以获得的。此外经过认证过的连接不能获得加密，即使是进入连接中间的攻击者也不能。
3. 协商是可靠的。没有经过通信方成员的检测，任何攻击者都不能修改通信协商。

为了更好的理解本申请实施例提供的一种安全通信方法、设备、系统及计算机可读存储介质，下面先对本申请实施例适用的安全通信方法的系统构架进行示例性地描述。如图 1 所示的系统架构 100，该系统架构 100 为目前的其中一种 5G 网络架构，可以包括用户设备(user equipment, UE)101、接入网((radio) access network, (R)AN)102、用户面功能(user plane function, UPF)103、数据网络(data network, DN)104、鉴权服务功能(authentication server function, AUSF)105、接入及移动性管理功能(access and mobility management function, AMF)106、会话管理功能(session management function, SMF)107、网络曝光功能(network exposure function, NEF)108、网元数据仓库功能(network function repository function, NRF)109、策略控制功能(policy control function, PCF)110、统一数据管理(unified data management, UDM)111、应用功能(application function, AF)112 和应用安全锚功能(applications security anchor function, AAnF)113。这些功能可以是 5G 网络架构中的独立的一个网元设备，或者，可以是该 5G 网络架构的网元设备中的一种功能实现等。其中，105 至 113 的功能为 5G 核心网中的网元或者功能。

用户设备 UE 101，可以包括接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。终端设备还可以是蜂窝电话、无绳电话、会话启动协议 (session initiation protocol, SIP) 电话、无线本地环路 (wireless local loop, WLL) 站、个人数字助理(personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，未来 5G 网络中的终端设备或者未来演进的公用陆地移动通信网络(public land mobile network, PLMN)中的终端设备等，本申请实施例对此并不限定。

接入网(R)AN 102，可以是第三代伙伴计划(3rd Generation Partnership Project, 3gpp)的接入网，例如长期演进(long term evolution, LTE)，或者 5G 新空口(New Radio, NR)等。或者，接入网(R)AN 102 可以是非第三代伙伴计划 non-3gpp 的接入网(如常见的 wifi 接入等)。若以我们最常见的手机上网来说的话，接入网(R)AN 102 可以是基站。

用户面功能 UPF 103，最主要的功能是负责数据包的路由转发、服务质量流(quality of

service, Qos)流映射, 其类似于 4G 网络的网关。

数据网络 DN 104, 包含运营商服务, 互联网访问或者第三方服务, 类似于 4G 的外部数据网络。

鉴权服务功能 AUSF 105, 网络认证 UE 的功能实体, 用于网络验证 UE 是否是真实的, 可支持 3GPP 框架定义的接入服务鉴权, 同时也可以支持非 3GPP 接入网的鉴权。

接入及移动性管理功能 AMF 106, 用于访问与移动性管理, 该功能是 5G 整体核心网络架构中最为重要的功能, 大体功能类似 4G 的移动管理节点功能(mobility management entity, MME)中移动性管理逻辑功能, 对网络的控制面消息进行处理。具体功能涵盖接入网控制面处理、非接入层(non-access stratum, NAS)消息处理、NAS 消息加密和完整性保护、注册管理、连接管理、接入性管理、移动性管理、合法信息截获、提供给会话管理功能 SMF 一些特殊会话管理消息、访问鉴权&授权、安全锚定功能(security anchor function, SEAF) (SEAF 可以认为是鉴权服务功能 AUSF 的鉴权代理)、位置服务管理、与 4G 核心网演进的分组系统(evolved packet system, EPS)交互时分配 EPS 承载 ID、UE 移动事件通知、5G 物联网中控制面数据传输优化、提供外部配置参数。

会话管理功能 SMF 107, 可以用于为用户面分配会话资源。

网络曝光功能 NEF 108, 是 5G 核心网与外部交互相关能力和信息的接口, 该接口可以对外部提供的网络能力主要包括监控能力、供给能力、策略/计费能力和分析报告能力。

网元数据仓库功能 NRF 109, 可以支持服务发现功能。从一个网元功能或服务通信代理收到网元“发现”请求, 并且可以将被“发现”的网元功能信息予以反馈。

策略控制功能 PCF 110, 支持管控网络行为的统一策略框架, 提供策略规则给控制平面执行, 访问 UDR 中与策略制定相关的订阅信息。

统一数据管理 UDM 111, 可以用于鉴权信用处理; 用户标识处理; 可以实现用户永久标识(subscription permanent identifier, SUPI)的存贮和管理, 同时支持用户隐藏标识(subscription concealed identifier, SUCI)的去隐私化; 提供基于订阅数据的访问授权; 对 UE 提供服务的网元功能注册管理; 通过对会话分配 SMF/数据网络名称(data network name, DNN)保持服务/会话的连续性; 订阅管理; 被叫短消息接收&短消息管理; 合法信息截获; 5G 局域网用户管理; 支持外部提供参数。

应用功能 AF 112, 该功能与 5G 核心网交互目的在于提供服务, 例如支持如下功能: 对于业务路由的应用影响, 访问网络能力曝光, 与策略框架交互进行策略管控。根据运营商部署策略, 受信 AF 可以直接访问 5G 核心网内部网元功能提升业务处理效率, 当然也可以采取通用的外部网元功能访问框架通过 NEF 与相应的内部网元功能实现信息交互。

应用安全锚功能 AAnF 113, 该应用安全锚定功能 AAnF 主要用于配合完成认证, 建立 UE 与核心网之间通信的共享密钥。

需要说明的是, 上述图 1 介绍的系统架构 100 是非漫游时的 5G 系统架构参考模型, 采用的是基于业务接口(service-based)的表现形式, 也叫基于服务的架构(service-based architecture, SBA)。5G 网络还有基于参考点(reference point)的表示形式的架构模式等, 也可以是本申请提供的安全通信方法适用的网络架构。

基于前面介绍的系统架构,在设备到设备(device-to-device, D2D)的通信场景中,两个用户设备 UE 实现互相通信之前,需要通过核心网来协助该两个 UE 的互相发现。具体的,假设该两个 UE 称为第一 UE 和第二 UE,那么第一 UE 和第二 UE 需要先和核心网互相认证身份并生成共享密钥以确保可以安全通信,然后,第一 UE 和第二 UE 再向核心网发送发现请求,由核心网基于该发现请求触发该第一 UE 和第二 UE 的发现流程,该发现流程为现有的技术方案,本申请在此不多做赘述。

另外需要说明的是,除了上述 D2D 的通信场景中,还可以是其它的通信场景,在实现具体的用户面数据交互之前,UE 需要先和核心网互相认证身份以及生成共享密钥,本申请对具体应用的通信场景不做限制。

UE 和核心网之间的身份认证和共享密钥生成,具体的可以是 UE 与核心网的网元之间进行认证和生成,为了便于理解,首先可以参见图 2,图 2 示例性示出了 UE 与核心网的网元之间认证身份和生成共享密钥的流程。图 2 以 5G 网络中的应用中认证和密钥协商(authentication and key management for application, AKMA)技术为例介绍。

在图 2 中可以看到,完成 UE 与核心网之间的认证和共享密钥生成,需要用户设备 UE、安全锚定功能 SEAF、鉴权服务功能 AUSF、统一数据管理 UDM 和应用安全锚定功能 AAnF 交互参与。具体的交互过程可以包括如下步骤:

S201、用户设备 UE 向安全锚定功能 SEAF 发送注册请求,该注册请求包括 UE 的标识。

该 UE 的标识可以是该 UE 的 SUCI 或者 5G 全球唯一临时标识(5G global unique temporary identity, 5G-GUTI)。当 UE 本地保存有 5G-GUTI 的时候,UE 在注册请求中携带 5G-GUTI。当 UE 本地没有保存 5G-GUTI 的时候,在注册请求消息携带 SUCI。SUCI 可以理解为是 SUPI 的一种加密形式,例如可以参考 3GPP TS33.501 第 6.12.2 章节以及 TS23.003 第 2.2B 章节所述。具体的, SUCI 中可以包括路由标识以及加密部分。加密部分为用户加密的身份信息。一种可能的实现方式中, SUPI 中除移动国家代码(mobile country code, MCC)之外的部分可以由全球用户识别卡(universal subscriber identity module, USIM)或移动设备(mobile equipment, ME)进行加密计算得到该加密部分。

S202、安全锚定功能 SEAF 向鉴权服务功能 AUSF 发送认证请求,该认证请求包括上述 UE 的标识。

如果 UE 在上述注册请求消息中携带的是 5G-GUTI,则 SEAF 根据 5G-GUTI 确定 SUPI,再将 SUPI 携带在认证请求消息中。如果 UE 在上述注册请求消息中携带的是 SUCI,则 SEAF 直接将 SUCI 放置在认证请求消息中。该认证请求消息可以是 Nausf_UEAuthentication_Authenticate Request message。由于 SEAF 是属于接入及移动性管理功能 AMF 中的一个功能,因此,上述认证请求也可以说是 AMF 向 AUSF 发送的。

S203、鉴权服务功能 AUSF 向统一数据管理 UDM 发送鉴权向量请求,该鉴权向量请求包括 UE 的标识。

如果 AUSF 从 SEAF 处收到的是 SUPI,则鉴权向量请求中包括 SUPI;如果 AUSF 从 SEAF 处收到的是 SUCI,则鉴权向量请求中包括 SUCI。

该鉴权向量请求用于向 UDM 请求鉴权向量,鉴权向量用于触发核心网与 UE 之间的主

鉴权(primary authentication)。

S204、统一数据管理 UDM 向鉴权服务功能 AUSF 发送鉴权向量响应, 该响应包括鉴权向量和 AKMA 指示信息。

当 UDM 接收到的鉴权向量请求中携带的用户标识为 SUCI, 那么 UDM 对 SUCI 解密得到 SUPI, 并将 SUPI 携带在鉴权向量响应中发送给 AUSF。

UDM 可以基于 UE 的标识根据签约信息判断该 UE 是否支持 AKMA 业务, 如果支持, 则传递 AKMA 指示信息给 AUSF, 用于告知 AUSF 该 UE 可以支持 AKMA 业务。

S205、用户设备 UE 和鉴权服务功能 AUSF 基于鉴权向量进行主鉴权。

主鉴权流程可以参考标准 TS 33.501 中第 6 章节的相关描述, 此处不赘述。

在主鉴权的过程中, UE 和 AUSF 可以分别获得 AUSF 密钥 K_{AUSF} 。另外, 在 AUSF 从 UDM 接收的鉴权向量响应中包括 AKMA 指示信息指示消息的情况下, AUSF 保存 AUSF 密钥 K_{AUSF} 。

UE 和 AUSF 之间完成主鉴权之后, 表明 UE 和 AUSF 之间完成了身份的认证, 即 UE 与核心网之间完成了身份的认证。

S206、用户设备 UE 和鉴权服务功能 AUSF 在主鉴权后生成 AKMA 锚点密钥 K_{AKMA} 和密钥标识(AKMA-key identifier, A-KID)。

具体的, UE 和 AUSF 主鉴权完成之后, UE 和 AUSF 根据预先配置的协议使用相同的算法基于 K_{AUSF} 生成 AKMA 锚点密钥 K_{AKMA} 和 AKMA 密钥标识(AKMA-key identifier, A-KID)。A-KID 用于标识密钥 K_{AKMA} , 该密钥 K_{AKMA} 用于后续进一步衍生保护 UE 与应用功能 AF 之间的通信信道的共享密钥 K_{af} 。

A-KID 格式为 username@example。username 部分包括路由标识(routing identifier, RID)和 AKMA 临时用户标识 (AKMA temporary UE identifier, A-TID), RID 它是 SUCI 中的一部分, 由 1~4 个十进制数字表示。A-TID 是根据 K_{AUSF} 生成的一个临时标识, K_{AUSF} 为 AUSF 在主鉴权过程中生成的密钥。example 部分包括家乡网络标识。

S207、鉴权服务功能 AUSF 向应用安全锚定功能 AAnF 发送锚点密钥注册请求, 该锚点密钥注册请求包括 UE 的 SUPI、密钥 K_{AKMA} 和密钥标识 A-KID。

S208、应用安全锚定功能 AAnF 向鉴权服务功能 AUSF 发送锚点密钥注册响应。

通过步骤 207 和步骤 208 可以将 UE 的 SUPI、密钥 K_{AKMA} 和密钥标识 A-KID 注册并关联存储到应用安全锚定功能 AAnF 中, 至此 UE 和核心网之间生成了共享密钥。

上述是以 AKMA 技术为例介绍 UE 与核心网之间认证身份和生成共享密钥的流程, 一种可能的实现方式中, 在 5G 网络中, 也可以使用通用引导架构(generic bootstrapping architecture, GBA)技术实现 UE 与核心网之间生成共享密钥的流程。现有的技术方案中, GBA 技术一般用于在 4G 网络中, 现在将其应用于 5G 网络中, 那么可以称为 5GGBA 技术。为了便于理解, 可以参见图 3, 图 3 示例性示出了 4G 网络中 GBA 技术实现 UE 与核心网之间认证身份和生成共享密钥的流程。

在已定义的 GBA 技术标准中, 参与的网元包括用户设备 UE、引导服务功能 (bootstrapping server function, BSF)和归属用户服务器(home subscriber server, HSS)/归属位

置寄存器(home location register, HLR)。引导服务功能 BSF、归属用户服务器 HSS 和归属位置寄存器 HLR 为 4G 网络架构中核心网的网元或者网元功能, BSF 可以作为中间枢纽, 即可以作为各个网元之间交互的接口; HSS 为可以提供 UE 的信息的服务器, HSS 可以存储 UE 与认证相关的参数。

图 3 所示的流程包括但不限于如下步骤:

S301、用户设备 UE 向引导服务功能 BSF 发送认证请求。

其中, 该认证请求消息中可以包括 UE 标识(identity, ID)。在 4G 网络中, 该 UE 标识可以是国际移动用户识别码(international mobile subscriber identity, IMSI)。可以看到, GBA 流程中 UE 向 BSF 发送认证请求时携带的是 UE 的永久标识 IMSI, 而该认证请求没有保护措施, 容易暴露 IMSI, 进而泄露用户的隐私。

S302、引导服务功能 BSF 向归属用户服务器 HSS/归属位置寄存器 HLR 发送认证请求。

应理解, 用户归属服务分为 HSS 和 HLR, 其中, HSS 可以用于 4G 通信系统, HLR 可以用于 3G 通信系统。

其中, UE 可以向 HSS/HLR 发送 UE 标识。HSS/HLR 可以根据 UE 标识确定该 UE 标识对应的根密钥, 并计算得到认证向量(authentication vector, AV)。具体地, 该认证向量 AV 可以包括随机数 RAND、认证令牌(authentication token, AUTN)、加密密钥(cipher key, CK)、完整性保护密钥(integrity key, IK)以及期望的用户响应(expected user response, XRES), 也即 $AV = (RAND, AUTN, CK, IK, XRES)$ 。

S303、归属用户服务器 HSS/归属位置寄存器 HLR 向引导服务功能 BSF 发送认证响应。

其中, 该认证响应中包括上述认证向量 AV。

S304、引导服务功能 BSF 向用户设备 UE 发送认证响应。

其中, 引导服务功能 BSF 接收归属用户服务器 HSS/归属位置寄存器 HLR 发送的认证向量 AV 后, 可以将该 AV 包括的随机数 RAND 和认证令牌 AUTN 发送给 UE, 即该随机数 RAND 和认证令牌 AUTN 包括在 BSF 向用户设备 UE 发送的认证响应中。

S305、用户设备 UE 验证认证令牌 AUTN, 并计算密钥和用户响应 RES。

当 UE 接收引导服务功能 BSF 发送的随机数 RAND 和认证令牌 AUTN 后, 可以验证认证令牌 AUTN, 并计算共享密钥和用户响应(user response, RES)。具体地, UE 可以计算并得到加密密钥 CK 和完整性保护密钥 IK, 其中, 加密密钥 CK 和完整性保护密钥 IK 可以用于计算 UE 的密钥。

S306、用户设备 UE 向引导服务功能 BSF 发送用户响应 RES。

S307、引导服务功能 BSF 对比期望的用户响应 XRES 和 RES, 以验证 RES 是否正确。且引导服务功能 BSF 计算密钥。

若引导服务功能 BSF 验证 RES 正确, 则引导服务功能 BSF 可以计算其密钥, 其中, 密钥 $K_s = CK \parallel IK$ 。

S308、引导服务功能 BSF 向 UE 发送密钥标识和密钥生存期。

其中, 密钥标识为引导事务标识(bootstrapping transaction identifier, B-TID), 是引导服务功能 BSF 基于随机数 RAND 和引导服务功能 BSF 服务器名称(server name)生成的。其中, B-TID 可以是 $\text{base64encode}(RAND)@BSF_servers_domain_name$, 其中, base64encode

e(RAND)可以表示对随机数 RAND 进行 base64 编码转换。

S309、UE 计算密钥。

UE 根据计算获得的加密密钥 CK 和完整性保护密钥 IK 计算与引导服务功能 BSF 生成的密钥对应的密钥 $K_s = CK \parallel IK$ 。

至此 UE 和 BSF 之间完成身份认证即至此 UE 和核心网之间完成身份认证。UE 和 BSF 还获得了共享密钥 K_s 和密钥标识 B-TID，UE 和 BSF 还将共享密钥 K_s 和密钥标识 B-TID 关联存储，该共享密钥可以用于后续 UE 和核心网之间的交互通信。

若将上述图 3 的 GBA 流程应用在 5G 网络中，则成为 5G GBA 的流程，那么，上述引导服务功能 BSF 在 4G 网络中的作用与应用安全锚定功能 AAnf 在 5G 网络中的作用类似；上述归属用户服务器 HSS 在 4G 网络中的作用与统一数据管理 UDM 在 5G 网络中的作用类似。

在 5G GBA 中，除了归属用户服务器 HSS 替换成统一数据管理 UDM 设备，基本上依然沿用 4G 网络中 GBA 流程的各个网元。另外，在 5G GBA 中，上述图 3 所示流程中的 UE 标识可以是 SUPI；上述图 3 所示流程中的密钥标识 B-TID 可以是类似于 5G 网络中的密钥标识 A-KID；上述图 3 所示流程中的共享密钥 K_s 与上述图 2 中的共享密钥 K_{AKMK} 作用类似。若在 5G 网络中选择 GBA 流程(即 5G GBA)，在 UE 向 BSF 发送认证请求时携带的是 UE 的永久标识 SUPI，而该认证请求没有保护措施，暴露了 SUPI，进而泄露用户的隐私。

上述 UE 和核心网之间完成身份认证并生成共享密钥之后，用户设备 UE 与核心网的网元之间需要进一步协商共享密钥才可以进行进一步的用户面消息的交互，该用户面消息例如可以是 D2D 通信场景中 UE 向应用功能 AF 发送的发现请求，以用于触发发现邻近可通信设备的流程。

由于现有的技术方案中，例如 4G 网络中的 D2D 通信场景中，用户设备 UE 互相发现的交互过程中直接使用 UE 明文的永久标识，具体的，UE 向核心网发送的发现请求中就携带 UE 的永久标识，该永久标识没有进行加密等处理，容易被窃取，通过该 UE 的永久标识可以关联到一个具体的用户，会暴露用户的隐私，存在安全隐患。为了解决这个问题，本申请提供了一种安全通信方法，该方法包括多个可能的实施方式，下面将逐一进行介绍。

本申请的一种可能的实施方式，就是在 UE 和核心网的网元进行共享密钥协商过程中，为用户设备 UE 与核心网之间的通信信息配置机密性保护，具体的，可以示例性地参见图 4、图 5A、图 5B、图 5C 和图 5D，该几个图示例性示出了本申请提供的 UE 和核心网的网元进行共享密钥协商的流程。

首先参见图 4，用户设备 UE 和核心网的网元进行共享密钥协商的流程可以包括但不限于如下步骤：

S401、用户设备 UE 选择使用 AKMA 交互方式。

具体的，UE 可以根据用户是否有隐私需求来选择交互方式，交互方式也可以称为交互流程或者流程等。该交互方式指的是用户设备 UE 与核心网的网元之间的交互方式。若有隐私需求，那么可以选择具有隐私保护的交互方式，例如可以选择 AKMA 交互方式，或者

具有隐私保护能力的 5G GBA 交互方式,若无隐私需求,那么选择 AKMA 或者 5G GBA 交互方式均可以。该具有隐私保护能力的 5G GBA 交互方式指的是 UE 与核心网的网元之间可以使用不会暴露 UE 的永久标识的标识,例如隐藏标识 SUCI 等进行信息的交互,而不使用明文的永久标识例如 SUPI 进行信息的交互。

UE 可以通过如下方式中的一项或多项来选择交互方式:

(1) 如果 UE 已经接入 5G 网络,并且该 UE 的应用程序(application, APP)指示 UE 该应用程序只能使用 AKMA 交互方式,那么 UE 确定使用 AKMA。该应用程序可以包括安装在该 UE 上的任意一个应用程序。例如,假设该应用程序为应用市场,那么该应用市场预先配置了只要 UE 接入了 5G 网络,那么该 UE 与 5G 核心网之间的交互方式为 AKMA 交互方式。

需要说明的是,该 UE 的应用程序为 UE 启动的应用程序,应用功能 AF 中包括该应用程序的服务器,应用功能 AF 中该应用程序对应的服务器可以通过多种协议来为应用程序提供(serves)商业逻辑(business logic)服务。

(2) 如果 UE 已经接入 5G 网络,并且应用程序指示 UE 该应用程序既可以使用 AKMA,又可以使用 GBA 的情况下,UE 首先使用 AKMA。可选的,如果 UE 接入的是 4G 网络,那么 UE 只能使用 GBA。即可以理解为只要是在 5G 网络,就是优先使用 AKMA 交互方式。如果是 4G 网络,就使用 GBA 交互方式,既通过 UE 接入的网络区分。

(3) 如果 UE 已经接入了 5G 网络,并且应用程序指示 UE 该应用既可以使用 AKMA,又可以使用 GBA 的情况下,UE 可以根据其他信息判断究竟要使用 AKMA 还是使用 GBA。示例性地,可以根据网络下发的优先级来确定,该优先级可以是预配置在 UE 上的,例如,可以通过类似于 3GPP 标准 TS 23.303 中的第 5.2 章节介绍的 service authorization 等与 ProSe 发现流程相关的流程进行预配置该优先级;或者,也可以在应用程序中由应用程序提供商进行预配置该优先级;或者,还可以通过家乡网络下发的用户路由选择策略(user route selection policy, URSP)规则进行预配置该优先级,即 URSP 规则中包括要优先使用 AKMA 交互方式还是优先使用 GBA 交互方式。

(4) 如果是漫游情况,那么,在现有的标准中,UE 只能使用 GBA 交互方式,因为 AKMA 交互方式目前还不支持漫游情况。一种可能的实现方式中,如果 AKMA 交互方式支持漫游,则根据 UE 拜访的网络的规则确定优先使用 GBA 交互方式还是优先使用 AKMA 交互方式。UE 拜访的网络可以在协议数据单元(protocol data unit, PDU)会话流程中下发规则给 UE,例如通过通知 notification 流程告知 UE 优先使用的交互方式。

(5) 如果 UE 使用了 5G 全球用户识别卡(universal subscriber identity module, USIM),则优先选择使用 AKMA 交互方式。因为使用 5G USIM 的用户可以理解为有更强烈的隐私需求。相应地,如果 UE 使用了 4G USIM,那么 UE 既可以选择 AKMA 交互方式,又可以选择 GBA 交互方式,但依然可以优先选择 AKMA 交互方式。本实施例不做限定。这个本质原因在于 SUCI 计算时要使用的参数只有 5G USIM 中才有存储。4G USIM 中是没有的。当一个 5G UE 使用了 4G USIM 的时候,其也可以计算出 SUCI,但是这个 SUCI 是使用空加密的。空加密就是没有产生实质的加密效果,跟没有加密一样。具体地,UE 可以有很多方法判断一个 USIM 是 5G USIM 还是 4G USIM。具体地,UE 可以根据只在 5G 才有的特

定参数进行判断是一个 5G USIM 还是一个 4G USIM。比如，特定参数可以是公钥，即根据 USIM 中是否存储有运营商的公钥进行判断。如果有就是 5G USIM。如果没有就是 4G USIM。再比如，特定参数可以是公钥标识符，根据 USIM 中是否有公钥标识符进行判断。如果有就是 5G USIM。如果没有就是 4G USIM。再比如，USIM 会有内在指示信息使得 UE 知晓是一个 5G USIM 还是一个 4G USIM。

(6) 根据默认的预配置。默认的预配置可以是一段计算机程序，运行该段计算机程序可以自动选择使用 AKMA 交互方式还是 GBA 交互方式。

(7) UE 接收用户输入的指示，并根据该指示选择使用 GBA 交互方式还是 AKMA 交互方式。

(8) UE 判断后续流程是否要发送永久标识，比如，是否需要将 SUPI 发送给 AF，如果确定要发送，则 UE 优先使用具有隐私保护能力的交互方式。比如，UE 确定要发送 Discovery Request 消息给 AF，消息中需要携带 SUPI，在这种情况下，虽然 UE 可以选择 GBA 或 AKMA 流程，但是 UE 确定 GBA 流程不是具备隐私保护能力的交互方式，会导致 SUPI 泄露，因此 UE 确定不选择 GBA，要选择 AKMA 流程。

或者，例如如果 UE 确定要发送 Discovery Request 消息给 AF，消息中携带 SUPI，且 UE 确定 GBA 或 AKMA 流程均为具有隐私保护能力的交互方式，那么 UE 可以选择 GBA 或者 AKMA 中的任一种交互方式。

上述示例性地给出了集中的交互方式选择方法，但本方案中交互方式的选择方式不限于上述介绍的几种，本申请对具体的选择交互方式的方法不做限制。

通过上述的一种或多种方式的选择，假设最后 UE 确定出选择的交互方式为 AKMA 交互方式。

S402、UE 向应用功能 AF 发送密钥协商请求，该密钥协商请求包括 UE 的密钥标识 A-KID。

需要说明的是，在 5G 网络中，在 D2D 场景下的邻近业务(proximity-based services, ProSe)发现流程中，应用功能 AF 可以是 5G 网络中的直连通信发现名称管理功能(direct discovery name management function, 5GDDNMF)。

一种可能的实施方式中，在 UE 选择使用 AKMA 交互方式之后，若 UE 进一步使用传输层安全性协议 TLS 流程协商密钥，那么，UE 向应用功能 AF 发送的密钥协商请求可以是 Client Hello 消息。

另一种可能的实施方式中，UE 也可以不使用 TLS 流程，那么，UE 向应用功能 AF 发送的密钥协商请求可以是 Application session establishment Request 消息。

不管是哪一种消息，密钥协商请求中均包括 UE 的密钥标识 A-KID。该密钥标识 A-KID 可以是上述图 2 所示的流程中 UE 获得的密钥标识 A-KID。

一种可能的实施方式中，上述密钥协商请求中还包括指示使用所述 AKMA 交互方式的信息，该信息用于通知应用功能 AF 用户设备选择的交互流程为 AKMA 流程，应用功能 AF 可以基于该指示信息按照 AKMA 流程的规定操作，以实现与用户设备 UE 之间的密钥协商。

S403、应用功能 AF 向应用安全锚定功能 AAnF 发送应用密钥获取请求，该请求携带

UE 的 A-KID 和 AF 的标识 AF_ID。

具体的, AAnF 接收到 AF 的应用密钥获取请求, 获取请求中的 A-KID 和 AF_ID, 然后, 根据 AF_ID 在配置的本地策略、授权信息或者由网元数据仓库功能 NRF 提供的策略中检查该 AAnF 是否能够为该 AF 提供服务。若确定 AAnF 可以为该 AF 提供服务, 那么, 该 AAnF 根据 A-KID 在本地查找 UE 的密钥 K_{AKMK} (在上述图 2 所示的流程中, 已经将 UE 的 SUPI、密钥 K_{AKMK} 和密钥标识 A-KID 关联存储到应用安全锚定功能 AAnF 中), 然后, 根据该 UE 的密钥 K_{AKMK} 验证该 UE 是否被授权使用 AKMA 交互方式。在确定 UE 被授权使用 AKMA 交互方式的情况下, AAnF 根据该 UE 的密钥 K_{AKMK} 生成应用密钥 Kaf。

S404、应用安全锚定功能 AAnF 向应用功能 AF 发送请求响应, 该请求响应包括密钥 Kaf。

应用安全锚定功能 AAnF 生成上述密钥 Kaf 之后, 将该密钥 Kaf 携带在对上述密钥获取请求的响应消息中发送给 AF。

S405、应用功能 AF 向用户设备 UE 发送密钥协商响应。

该密钥协商响应是对于上述 AF 接收到的密钥协商请求的响应消息。

若上述 UE 向应用功能 AF 发送密钥协商请求是 Client Hello 消息, 那么, 对该密钥协商请求的响应消息可以是 Server Hello 消息。

若上述 UE 向应用功能 AF 发送密钥协商请求是 Application session establishment Request 消息, 那么, 对该密钥协商请求的响应消息可以是 Application session establishment Response 消息。

由于上述 AF 从 AAnF 获得了应用密钥 Kaf, 表明 AF 可以与 UE 进一步交互通信, 那么 AF 向 UE 发送的密钥协商响应, 然后, UE 可以开始向 AF 发送用户面消息。

若上述 AF 没有从 AAnF 获得了应用密钥 Kaf, 则表明 AF 无法进一步与 UE 进行通信, 则 AF 向 UE 发送的密钥协商响应指示 UE 和 AF 无法进一步进行通信, 且该密钥协商响应中包括 UE 和 AF 进一步通信失败的原因。

另外, 用户设备 UE 可以在上述 UE 向 AF 发送密钥协商请求之前根据密钥 K_{AKMK} 生成应用密钥 Kaf, 或者, UE 可以在上述 UE 向 AF 发送密钥协商请求之后根据密钥 K_{AKMK} 生成应用密钥 Kaf。在 AF 从 AAnF 获得了同样是由 K_{AKMK} 生成的应用密钥 Kaf 后, AF 和 UE 可以基于该应用密钥 Kaf 进一步实现通信。

可选的, 若在 UE 选择使用 AKMA 交互方式之后, UE 进一步使用传输层安全性协议 TLS 流程协商密钥, 那么, 用户设备 UE 接收到应用功能 AF 发送的密钥协商响应之后, 用户设备 UE 向应用功能 AF 发送密钥协商完成的消息。

S406、用户设备 UE 向应用功能 AF 发送用户面消息, 该用户面消息中包括 UE 加密的身份标识。

在 UE 和 AF 之间的密钥协商完成之后, 表明 UE 与 AF 之间已经建立了安全通信, 可以进一步交互发送消息。

可选的, 若是在 D2D 的通信场景中, 那么, UE 可以向 AF 发送的用户面消息可以是发现请求 Discover Request, 用于触发发现 UE 邻近的可通信的设备。由于上述使用了 AKMA 交互方式, 那么, 为了增加 UE 的安全性, 减少 UE 的用户隐私泄露的风险, 该发现请求中

携带的 UE 标识可以是, UE 的加密的身份标识, 例如可以是 UE 的隐藏标识 SUCI, 或者 UE 的通用公共用户标识(generic public subscription identifier, GPSI)或密钥标识 A-KID。

除了上述 D2D 的通信场景中, 上述图 4 所示的流程还可以应用于其它的通信场景, 此时, UE 向 AF 发送的用户面消息可以是其它的请求消息等, 本方案对此不做限制。

本申请通过选择使用 AKMA 交互方式来实现 UE 与 AF 之间的密钥协商, 并在后续的用户面交互流程中, UE 和 AF 之间交互的用户面消息使用 UE 的隐藏标识 SUCI, 由于 SUCI 是对 UE 的永久标识 SUPI 进行处理例如加密后得到的, 因此即使攻击者获取到 SUCI 后也无法轻易获得 SUPI, 从而有效减少了用户的永久标识泄露的风险, 进而减少了用户隐私泄露的风险。

参见图 5A, 图 5A 所示为本申请实施例提供的在 UE 和核心网的网元协商共享密钥的过程中, 为用户设备 UE 与核心网之间的通信信息配置机密性保护的另一种可能的实施方式。图 5A 所示的用户设备 UE 和核心网的网元协商共享密钥流程可以包括但不限于如下步骤:

S5A01、用户设备 UE 选择交互方式。

具体的, UE 选择交互方式的方法可以参见上述图 4 所示的步骤 S401 中对应的描述, 此处不再赘述。在本申请实施例中, 一种可能的实施方式, UE 确定出选择的交互方式为 AKMA 交互方式。另一种可能的实施方式, UE 确定出选择的交互方式为 GBA 交互方式, 该 GBA 的交互方式包括 4G GBA 的交互方式和 5G GBA 的交互方式。若 UE 接入的是 4G 网络, 那么选择的为 4G GBA 交互方式, 若 UE 接入的是 5G 网络, 那么选择的为 5G GBA 的交互方式。图 5A 所示的流程中先以 UE 确定出选择的交互方式为 AKMA 交互方式为例进行介绍。

S5A02、UE 向应用功能 AF 发送密钥协商请求, 该密钥协商请求包括 UE 的密钥标识 A-KID。

S5A03、应用功能 AF 向应用安全锚定功能 AAnF 发送应用密钥获取请求, 该请求携带 UE 的 A-KID 和 AF 的标识 AF_ID。

S5A04、应用安全锚定功能 AAnF 向应用功能 AF 发送请求响应, 该请求响应包括密钥 K_{af}。

步骤 S5A02、S5A03 和 S5A04 的具体描述可以参见上述图 4 所示的 S402、S403 和 S404 中对应的描述。

S5A05、应用功能 AF 选择一个非空加密算法。

具体的, 本申请实施例中, 通过应用功能 AF 配置一个非空加密算法, 该非空加密算法可以是哈希 256、哈希 128 或者 MD5 等加密算法, 用于为后续 UE 和 AF 之间的交互消息进行加密, 以保护 UE 的信息, 避免泄漏用户隐私。

一种可能的实施方式中, AF 选择一个非空加密算法可以是基于用户设备 UE 的指示而选择的。具体的, 上述 UE 向应用功能 AF 发送密钥协商请求时, 该密钥协商请求可以包括一个指示 AF 选择一个非空加密算法的指示信息, 该指示信息可以是比特位指示信息, 也可以是预先约定好的标识符或者代号等等, 本方案对此不做限制。AF 根据非空加密算法指

示信息确定一个非空加密算法。非空加密算法用于 UE 和 AF 之间连接的机密性保护。

在一种可能的实施方式中，UE 向应用功能 AF 发送密钥协商请求时，该密钥协商请求携带 UE 支持的加密算法的指示信息，其中，不包括非空加密算法的指示信息，该指示信息可以是 UE 支持的非空加密算法的标识、代号或名称等。AF 在做加密算法选择时，AF 会从 UE 支持的加密算法和 AF 支持的加密算法的交集中选择，因为 UE 没有传递非空加密算法的指示信息，从 AF 看来 UE 不支持非空加密算法，因此 AF 会从交集中选择一个非空加密算法。

另一种可能的实施方式中，假设上述指示 AF 选择一个非空加密算法的指示信息称为加密算法协商信息，该加密算法协商信息也可以不携带在上述密钥协商请求中，而是单独由用户设备 UE 发送给应用功能 AF。

S5A06、应用功能 AF 向用户设备 UE 发送密钥协商响应，该密钥协商响应包括非空加密算法的标识。

该密钥协商响应是对于上述 AF 接收到的密钥协商请求的响应消息。

应用功能 AF 在上述步骤 S5A04 中获取到密钥 Kaf 后，选择了一个非空加密算法，然后将该非空加密算法的标识携带在对上述密钥协商请求的响应消息中发送给 UE。该非空加密算法的标识可以是该非空加密算法的名称或者能够指示该算法的一个符号或代号等等。

若上述 UE 向应用功能 AF 发送密钥协商请求是 Client Hello 消息，那么，对该密钥协商请求的响应消息可以是 Server Hello 消息。

若上述 UE 向应用功能 AF 发送密钥协商请求是 Application session establishment Request 消息，那么，对该密钥协商请求的响应消息可以是 Application session establishment Response 消息。

由于上述 S5A04 中，AF 从 AAnF 获得了应用密钥 Kaf，表明 AF 可以与 UE 进一步交互通信，那么 AF 向 UE 发送的密钥协商响应，然后，UE 可以开始向 AF 发送用户面消息。

若上述 AF 没有从 AAnF 获得了应用密钥 Kaf，则表明 AF 无法进一步与 UE 进行通信，则 AF 向 UE 发送的密钥协商响应指示 UE 和 AF 无法进一步进行通信，且该密钥协商响应中包括 UE 和 AF 进一步通信失败的原因。

另外，用户设备 UE 可以在上述 UE 向 AF 发送密钥协商请求之前根据密钥 K_{AKMK} 生成应用密钥 Kaf，或者，UE 可以在上述 UE 向 AF 发送密钥协商请求之后根据密钥 K_{AKMK} 生成应用密钥 Kaf。在 AF 从 AAnF 获得了同样是由 K_{AKMK} 生成的应用密钥 Kaf 后，AF 和 UE 可以基于该应用密钥 Kaf 进一步实现通信。

可选的，若在 UE 选择使用 AKMA 交互方式之后，UE 进一步使用传输层安全性协议 TLS 流程协商密钥，那么，用户设备 UE 接收到应用功能 AF 发送的密钥协商响应之后，用户设备 UE 向应用功能 AF 发送密钥协商完成的消息。

S5A07、用户设备 UE 向应用功能 AF 发送使用上述非空加密算法加密的用户面消息，该用户面消息中包括 UE 的标识。

在 UE 和 AF 之间的密钥协商完成之后，表明 UE 与 AF 之间已经建立了安全通信，可以进一步交互发送信息。

可选的，若是在 D2D 的通信场景中，那么，UE 可以向 AF 发送的用户面消息可以是

发现请求 Discover Request, 用于触发发现 UE 邻近的可通信的设备。

上述应用功能 AF 与 UE 协商了使用非空加密算法对 AF 与 UE 之间交互的消息进行加密, 那么, 该 UE 向 AF 发送的用户面消息使用上述选择的非空加密算法进行加密, 从而增加了 UE 的安全性, 减少 UE 的用户隐私泄露的风险。

一种可能的实现方式中, 由于该用户面消息已经使用非空加密算法进行加密, 用户设备 UE 向 AF 发送的用户面消息中携带的 UE 标识可以是 UE 的永久标识 SUPI。

一种可能的实现方式中, 即使该用户面消息已经使用非空加密算法进行加密, 但为了进一步保护用户的隐私, 用户设备 UE 向 AF 发送的用户面消息中携带的 UE 标识可以是 UE 的隐藏标识 SUCI 等加密的身份标识。

一种可能的实现方式中, 用户设备 UE 在向应用功能 AF 发送上述用户面消息之前, 可以先检查 UE 和 AF 之间的机密性保护是否开启。可选的, 用户设备检查机密性保护是否开启可以是: 检查 UE 和 AF 之间是否协商使用非空加密算法来对交互的信息进行加密, 若使用了非空加密算法, 则表明机密性保护开启, 若没有选择非空加密算法, 则表明机密性保护没有开启。可选的, 用户设备检查机密性保护是否开启可以是: 检查上述密钥协商请求中是否携带有指示 AF 选择非空加密算法的信息, 若携带有, 则表明机密性保护开启, 需要说明的是, 若没有携带, 不一定表明机密性保护没有开启, 可以通过其它方式进一步确认。在机密性保护开启的情况下, UE 向 AF 发送的用户面消息中携带的 UE 标识可以是 UE 的永久标识 SUPI。

一种可能的实施方式中, 基于上述图 5A, 若上述步骤 S5A02 中, UE 向应用功能 AF 发送密钥协商请求是 Application session establishment Request 消息, 步骤 S5A06 中, 对该密钥协商请求的响应消息是 Application session establishment Response 消息的情况下, 在步骤 S5A05 中, 应用功能 AF 可以先不选择非空加密算法, 该 Application session establishment Response 消息中也可以先不包括非空加密算法的标识。在 UE 收到 Application session establishment Response 之后, UE 和 AF 之间可以再根据上述图 5A 之间的流程配置非空加密算法, 此时, 上述步骤 S5A02 中, UE 向应用功能 AF 发送密钥协商请求为 Client Hello 消息, 上述步骤 S5A06 中, 对该密钥协商请求的响应消息为 Server Hello 消息。

一种可能的实现方式中, 参见图 5B, 图 5B 示例性示出了 UE 选择 GBA 的交互方式实现 UE 和核心网的网元协商共享密钥的过程, 该过程可以包括但不限于如下步骤:

S5B01、用户设备 UE 选择交互方式。

具体的, UE 选择交互方式的方法可以参见上述图 4 所示的步骤 S401 中对应的描述, 此处不再赘述。图 5B 所示的流程中以 UE 确定出选择的交互方式为 GBA 的交互方式为例进行介绍。

基于前面的描述可知, 5G GBA 的交互方式基本沿用 4G GBA 交互方式的网元, 因此, GBA 交互方式相比于上述图 5A 所示的 AKMA 交互方式, 交互的网元上主要是将应用安全锚定功能 AAnF 替换成了引导服务功能 BSF 设备。

S5B02、UE 向应用功能 AF 发送密钥协商请求, 该密钥协商请求包括 UE 的密钥标识

B-TID。

该密钥标识 B-TID 为 UE 在上述图 3 所示的流程中获得。另外，应用功能 AF 可以是网络应用功能(network application function, NAF)。

可选的，在 D2D 场景下的邻近业务 ProSe 发现流程中，应用功能 AF 可以是直连通信发现名称管理功能 5GDDNMF。

一种可能的实施方式中，在 UE 选择使用 GBA 交互方式之后，若 UE 进一步使用传输层安全性协议 TLS 流程协商密钥，那么，UE 向应用功能 AF 发送的密钥协商请求可以是 Client Hello 消息。

另一种可能的实施方式中，UE 也可以不使用 TLS 流程，那么，UE 向应用功能 AF 发送的密钥协商请求可以是 Application Request 消息等。

不管是哪一种消息，密钥协商请求中均包括 UE 的密钥标识 B-TID。

S5B03、应用功能 AF 向应用引导服务功能 BSF 发送应用密钥获取请求，该请求携带 UE 的 B-TID 和 AF 的标识 AF_ID。

具体的，BSF 接收到 AF 的应用密钥获取请求，获取请求中的 B-TID 和 AF_ID，然后，根据 AF_ID 检查该 BSF 是否能够为该 AF 提供服务。若确定 BSF 可以为该 AF 提供服务，那么，该 BSF 根据 B-TID 在本地查找 UE 的密钥 Ks (在上述图 3 所示的流程中，BSF 已经关联存储共享密钥 Ks 和密钥标识 B-TID)，然后，根据该 UE 的密钥 Ks 验证该 UE 是否被授权使用 GBA 交互方式。在确定 UE 被授权使用 GBA 交互方式的情况下，BSF 根据该 UE 的密钥 Ks 生成应用密钥 Kaf。若应用功能 AF 为网络应用功能 NAF，那么该密钥 Kaf 可以是 Ks_ext/int_NAF。

可选的，若 UE 进一步使用传输层安全性协议 TLS 流程协商密钥，那么，AF 向 BSF 发送的应用密钥获取请求可以是 Authentication Request 消息等。

可选的，若 UE 没有使用 TLS 流程协商密钥，而是使用其它的流程协商密钥，那么该密钥获取请求也可以是 Authentication Request 消息等。

S5B04、应用引导服务功能 BSF 向应用功能 AF 发送请求响应，该请求响应包括密钥 Kaf。

应用引导服务功能 BSF 生成上述密钥 Kaf 之后，将该密钥 Kaf 携带在对上述密钥获取请求的响应消息中发送给 AF。

可选的，若 UE 进一步使用传输层安全性协议 TLS 流程协商密钥，那么，BSF 向 AF 发送的请求响应可以是 Authentication Answer 消息等。

可选的，若 UE 没有使用 TLS 流程协商密钥，那么该请求响应也可以是 Authentication Answer 消息等。

S5B05、应用功能 AF 选择一个非空加密算法。

具体的，本申请实施例中，通过应用功能 AF 配置一个非空加密算法，该非空加密算法可以是哈希 256、哈希 128 或者 MD5 等加密算法，用于为后续 UE 和 AF 之间的交互消息进行加密，以保护 UE 的信息，避免泄漏用户隐私。

一种可能的实施方式中，AF 选择一个非空加密算法可以是基于用户设备 UE 的指示而选择的。具体的，上述 UE 向应用功能 AF 发送密钥协商请求时，该密钥协商请求可以包括

一个指示 AF 选择一个非空加密算法的指示信息，该指示信息可以是比特位指示信息，也可以是预先约定好的标识符或者代号等等，本方案对此不做限制。AF 根据非空加密算法指示信息确定一个非空加密算法。非空加密算法用于 UE 和 AF 之间连接的机密性保护。

在一种可能的实施方式中，UE 向应用功能 AF 发送密钥协商请求时，该密钥协商请求携带 UE 支持的加密算法的指示信息，其中，不包括非空加密算法的指示信息。AF 在做加密算法选择时，AF 会从 UE 支持的加密算法和 AF 支持的加密算法的交集中选择，因为 UE 没有传递非空加密算法的指示信息，从 AF 看来 UE 不支持非空加密算法，因此 AF 会从交集中选择一个非空加密算法。

另一种可能的实施方式中，假设上述指示 AF 选择一个非空加密算法的指示信息称为加密算法协商信息，该加密算法协商信息也可以不携带在上述密钥协商请求中，而是单独由用户设备 UE 发送给应用功能 AF。

S5B06、应用功能 AF 向用户设备 UE 发送密钥协商响应，该密钥协商响应包括非空加密算法的标识。

该密钥协商响应是对于上述 AF 接收到的密钥协商请求的响应消息。

应用功能 AF 在上述步骤 S5B04 中获取到密钥 Kaf 后，选择了一个非空加密算法，然后将该非空加密算法的标识携带在对上述密钥协商请求的响应消息中发送给 UE。该非空加密算法的标识可以是该非空加密算法的名称或者能够指示该算法的一个符号或代号等等。

若上述 UE 向应用功能 AF 发送密钥协商请求是 Client Hello 消息，那么，对该密钥协商请求的响应消息可以是 Server Hello 消息。

若上述 UE 向应用功能 AF 发送密钥协商请求是 Application Request 消息，那么，对该密钥协商请求的响应消息可以是 Application Answer 消息。

由于上述 S5B04 中，AF 从 BSF 获得了应用密钥 Kaf，表明 AF 可以与 UE 进一步交互通信，那么 AF 向 UE 发送的密钥协商响应，然后，UE 可以开始向 AF 发送用户面消息。

若上述 AF 没有从 BSF 获得了应用密钥 Kaf，则表明 AF 无法进一步与 UE 进行通信，则 AF 向 UE 发送的密钥协商响应指示 UE 和 AF 无法进一步进行通信，且该密钥协商响应中包括 UE 和 AF 进一步通信失败的原因。

另外，用户设备 UE 可以在上述 UE 向 AF 发送密钥协商请求之前根据密钥 Ks 生成应用密钥 Kaf，或者，UE 可以在上述 UE 向 AF 发送密钥协商请求之后根据密钥 Ks 生成应用密钥 Kaf。在 AF 从 BSF 获得了同样是由 Ks 生成的应用密钥 Kaf 后，AF 和 UE 可以基于该应用密钥 Kaf 进一步实现通信。

可选的，若在 UE 选择使用 GBA 交互方式之后，UE 进一步使用传输层安全性协议 TLS 流程协商密钥，那么，用户设备 UE 接收到应用功能 AF 发送的密钥协商响应之后，用户设备 UE 向应用功能 AF 发送密钥协商完成的消息。

S5B07、用户设备 UE 向应用功能 AF 发送使用上述非空加密算法加密的用户面消息，该用户面消息中包括 UE 的标识。

在 UE 和 AF 之间的密钥协商完成之后，表明 UE 与 AF 之间已经建立了安全通信，可以进一步交互发送信息。

可选的，若是在 D2D 的通信场景中，那么，UE 可以向 AF 发送的用户面消息可以是

发现请求 Discover Request, 用于触发发现 UE 邻近的可通信的设备。

上述应用功能 AF 与 UE 协商了使用非空加密算法对 AF 与 UE 之间交互的消息进行加密, 那么, 该 UE 向 AF 发送的用户面消息使用上述选择的非空加密算法进行加密, 从而增加了 UE 的安全性, 减少 UE 的用户隐私泄露的风险。

一种可能的实现方式中, 由于该用户面消息已经使用非空加密算法进行加密, 用户设备 UE 向 AF 发送的用户面消息中携带的 UE 标识可以是 UE 的永久标识 SUPI。

一种可能的实现方式中, 即使该用户面消息已经使用非空加密算法进行加密, 但为了进一步保护用户的隐私, 用户设备 UE 向 AF 发送的用户面消息中携带的 UE 标识可以是 UE 的隐藏标识 SUCI 等加密的身份标识。

一种可能的实现方式中, 用户设备 UE 在向应用功能 AF 发送上述用户面消息之前, 可以先检查 UE 和 AF 之间的机密性保护是否开启。可选的, 用户设备检查机密性保护是否开启可以是: 检查 UE 和 AF 之间是否协商使用非空加密算法来对交互的信息进行加密, 若使用了非空加密算法, 则表明机密性保护开启, 若没有选择非空加密算法, 则表明机密性保护没有开启。可选的, 用户设备检查机密性保护是否开启可以是: 检查上述密钥协商请求中是否携带有指示 AF 选择非空加密算法的信息, 若携带有, 则表明机密性保护开启, 需要说明的是, 若没有携带, 不一定表明机密性保护没有开启, 可以通过其它方式进一步确认。在机密性保护开启的情况下, UE 向 AF 发送的用户面消息中携带的 UE 标识可以是 UE 的永久标识 SUPI。

一种可能的实施方式中, 可以参见图 5C, 图 5C 是基于上述图 5A 所示的流程, 在用户设备 UE 侧增加了一个步骤, 该增加的步骤为图 5C 中的步骤 S5C07: UE 确定密钥协商响应中指示的算法为非空加密算法。具体的, UE 接收到 AF 发送的密钥协商响应后, 可以基于该密钥协商响应中的携带的算法的标识进一步验证该算法是否为非空加密算法。示例性地, 可以将该接收到的算法的标识与本地存储的非空加密算法的标识比较, 若该接收到的算法的标识与本地的某个非空加密算法的标识相同, 则验证了该接收到的算法的标识为非空加密算法标识。图 5C 中, 除了步骤 S5C07 之外的其它步骤的具体实现可以参见上述对图 5A 的具体描述, 此处不再赘述。

一种可能的实施方式中, 可以参见图 5D, 图 5D 是基于上述图 5B 所示的流程, 在用户设备 UE 侧增加了一个步骤, 该增加的步骤为图 5D 中的步骤 S5D07: UE 确定密钥协商响应中指示的算法为非空加密算法。具体的, UE 接收到 AF 发送的密钥协商响应后, 可以基于该密钥协商响应中的携带的算法的标识进一步验证该算法是否为非空加密算法。示例性地, 可以将该接收到的算法的标识与本地存储的非空加密算法的标识比较, 若该接收到的算法的标识与本地的某个非空加密算法的标识相同, 则验证了该接收到的算法的标识为非空加密算法标识。图 5D 中, 除了步骤 S5D07 之外的其它步骤的具体实现可以参见上述对图 5B 的具体描述, 此处不再赘述。

一种可能的实现方式中, 在上述图 5A 的步骤 S5A05, 或者, 在上述图 5B 的步骤 S5B05,

或者，在上述图 5C 的步骤 S5C05 中，如果应用功能 AF 只有空加密算法可以选择；或者，对于图 5C，在步骤 S5C07 中，如果 UE 侧检验接收到的算法标识为空算法的标识；或者，对于图 5D，在步骤 S5D07 中，如果 UE 侧检验接收到的算法标识为空算法的标识；那么，一种可能的实现方式中，为了避免 UE 的永久标识泄露，UE 可以终止后续的流程，即不再发起发现请求。

可选的，终止流程后，UE 可以向 AF 发送指示终止流程原因的消息。

可选的，终止流程之后，UE 可以再次发起上述图 5A、图 5B、图 5C 或者图 5D 所示的密钥协商流程，若 UE 再次检验到接收到的算法标识为空算法标识，那么，为了避免 UE 无法入网，UE 可以不终止后续的流程，继续向 AF 发送发现请求触发发现可通信的邻近设备。或者，若 UE 再次检验到接收到的算法标识为空算法标识，为了 UE 信息的安全，UE 也可以再次终止后续的流程。

可选的，再次终止流程后，UE 也可以再次向 AF 发送指示终止流程原因的消息。

可选的，再次终止流程后，UE 可以启动一个计时器，该计时器用于阻止 UE 再次入网，即在计时器计时的时间段内，UE 不会再次发起上述图 5A 至图 5C 所示的密钥协商流程。可选的，在解决了隐私安全的问题之后，例如，在上述 AF 不再选择空加密算法之后，UE 可以再次发起上述图 5A、图 5B、图 5C 或者图 5D 所示的密钥协商流程。

一种可能的实施方式中，若在图 5C 的步骤 S5C07 中或者在图 5D 的步骤 S5D07 中，UE 侧检验接收到的算法标识为空算法的标识，那么，UE 可以再次向应用功能 AF 发送一个获取非空加密算法的请求，可选的，该请求可以是上述 UE 向 AF 发送的密钥协商请求。该获取非空加密算法的请求中包括一个指示 AF 选择一个非空加密算法的指示信息，该指示信息可以是比特位指示信息，也可以是预先约定好的标识符或者代号等等，本方案对此不做限制。AF 根据非空加密算法指示信息确定一个非空加密算法。非空加密算法用于 UE 和 AF 之间连接的机密性保护。

在一种可能的实施方式中，UE 向应用功能 AF 发送获取非空加密算法的请求时，该请求不包括指示 AF 选择一个非空加密算法的指示信息，该请求本申请即为指示信息，AF 收到后会从 UE 支持的加密算法和 AF 支持的加密算法的交集中选择非空加密算法，并反馈给 UE。

在一种可能的实施方式中，UE 向应用功能 AF 发送获取非空加密算法的请求时，该请求不包括指示 AF 选择一个非空加密算法的指示信息，AF 收到后，AF 根据自身的特定服务功能决定了 AF 会从 UE 支持的加密算法和 AF 支持的加密算法的交集中选择非空加密算法，并反馈给 UE。其中，AF 根据自身的特定服务功能的含义是该 AF 有预配置信息知晓为 UE 做哪些服务。比如若 AF 是 5G DDNMF，那么该 AF 可以只配置有非空的加密算法，所以当 AF 选择加密算法的时候，AF 也只能选择出非空的加密算法。

一种可能的实现方式中，上述图 4、图 5A 至图 5D 及其可能的实施方式中，主要为用户设备 UE 与核心网网元或者第三方应用服务器之间的通信连接配置机密性保护，可选的，还可以为用户设备 UE 与核心网网元或者第三方应用服务器之间的通信连接配置完整性保

护,具体的配置可以参见现有的技术方案,本申请对此不做限制。

或者,在本申请实施例中,还可以在应用功能 AF 选择一个非空加密算法的时,还选择一个完整性保护算法,用于保护 UE 和 AF 之间交互通信的信息的完整性,然后,将该非空加密算法的标识和完整性保护算法的标识一起携带在认证响应中向用户设备 UE 发送。

可选的,非空加密算法和完整性保护算法也可以不同时选择,可以分开选择,AF 先选择非空加密算法,并将非空加密算法的标识发送给 UE。然后,AF 再选择完整性保护算法,并将完整性保护算法的标识发送给 UE。或者,该两种算法的选择顺序反过来也可以,本方案对此不做限制。

一种可能的实现方式中,用户设备 UE 在向应用功能 AF 发送上述发现请求之前,可以先检查 UE 和 AF 之间的机密性保护和完整性保护是否开启。可选的,用户设备检查机密性保护是否开启可以是:检查 UE 和 AF 之间是否协商使用非空加密算法来对交互的信息进行加密,若使用了非空加密算法,则表明机密性保护开启,若没有选择非空加密算法,则表明机密性保护没有开启。可选的,用户设备检查机密性保护是否开启可以是:检查上述密钥协商请求中是否携带有指示 AF 选择非空加密算法的信息,若携带有,则表明机密性保护开启,需要说明的是,若没有携带,不一定表明机密性保护没有开启,可以通过其它方式进一步确认。完整性保护指的就是 UE 和 AF 之间是否协商使用完整性保护算法来对交互的信息进行加密以保证信息的完整性。在机密性保护和完整性保护均开启的情况下,UE 向 AF 发送的发现请求中携带的 UE 标识可以是 UE 的永久标识 SUPI。

上述介绍的是在 UE 和核心网网元协商共享密钥的过程中,为用户设备 UE 与核心网网元之间的通信连接配置机密性保护的实施方式。本申请中还可以提供另一种可能的实施方式,即在 UE 向核心网网元例如 AF(该 AF 可以是 5GDDNMF)发送用户面消息触发进一步的交互通信的过程中,例如 UE 想 AF 发送发现请求触发发现 UE 邻近的可通信设备的过程中,为 UE 和核心网网元之间的通信连接配置机密性保护策略。本申请实施例不管 UE 和核心网网元协商共享密钥的过程中是否已经配置了机密性保护的策略,均可以实施执行。具体的,可以示例性参见图 6 至图 9 所示的几种可能的实现方式,下面逐一介绍。

参见图 6,示例性示出了在 UE 向核心网网元发送用户面消息触发进一步的交互通信的过程中,为 UE 和核心网网元之间的通信信息配置机密性保护策略的一种可能的实现方式,包括但不限于如下步骤:

S601、用户设备 UE 向应用功能 AF 发送用户面消息,该用户面消息中包括 UE 的隐藏标识 SUCI。

需要说明的是,在 5G 网络中,在 D2D 场景下的邻近业务 ProSe 发现流程中,应用功能 AF 可以是 5G 网络中的直连通信发现名称管理功能 5GDDNMF。在该场景下,UE 可以向 AF 发送的用户面消息可以是发现请求 Discover Request,用于触发发现 UE 邻近的可通信的设备。

除了上述 D2D 的通信场景中,本申请还可以应用于其它的通信场景,此时,UE 想 AF 发送的用户面消息可以是其它的请求消息等,本方案对此不做限制。下面以用户面消息是发现请求 Discover Request 为例介绍。

在本申请实施例中，在发现请求中携带 UE 的隐藏标识，可以减少 UE 的用户隐私泄露的风险。

一种可能的实现方式中，用户设备 UE 向应用功能 AF 发送发现请求之前，UE 还可以先检查 UE 和 AF 之间的机密性保护是否开启，例如，可以参见图 9，图 9 中 S901 用户设备 UE 确定自身与应用功能 AF 之间的通信数据是否开启机密性保护的具体实现可以参见前面机密性保护开启的详细介绍，此处不再赘述。UE 检查完机密性保护是否开启后，可以向 AF 发送用户面消息，参见步骤 S902。若机密性保护开启，那么用户面消息中携带的用户设备的标识可以是永久标识也可以是加密的身份标识，如果机密性保护没有开启，那么用户面消息中携带的用户设备的标识为加密的身份标识。若该加密的身份标识为 UE 的隐藏标识 SUCI，那么，S902 和上述 S601 对应。

一种可能的实现方式中，用户设备 UE 向应用功能 AF 发送发现请求之前，UE 还可以先检查 UE 和 AF 之间的完整性保护是否开启，若没有开启，那么 UE 向 AF 发送的发现请求包括的 UE 的标识为 UE 的隐藏标识。检查完整性保护开启的方式可以参见前面的描述，此处及下文不再赘述。

S602、应用功能 AF 向统一数据管理 UDM 设备发送授权检查请求，该授权检查请求包括 UE 的隐藏标识 SUCI。

具体的，该 AF 向 UDM 发送的授权检查请求用于确定该 UE 是否被授权与邻近设备进行通信，只有被授权的情况下，AF 才会继续基于 UE 发送过来的发现请求为其寻找发现邻近的可通信设备。

UDM 需要基于 UE 的永久标识才可以进行授权检查。AF 从 UE 的发现请求中获取的 UE 标识为 SUCI，因此，AF 向 UDM 发送的授权请求中包括 SUCI，UDM 可以基于 SUCI 获取到 UE 的永久标识。

当前网络架构中，AF 可以直接或者间接的与 UDM 进行通信。本实施例以 AF 可以直接与 UDM 进行通信为例进行说明。可以理解的是，如果当一个 AF 只能间接与 UDM 进行通信，比如通过网络曝光功能 NEF，那么本实施例可以自动扩展并适配到该场景中，此时本实施中的 AF 和 UDM 之间的交互自动包括了 AF-NEF-UDM 三者之间的交互过程。

S603、统一数据管理 UDM 设备根据 SUCI 确定 UE 的 SUPI，基于 SUPI 对 UE 进行授权检查。

具体的，UDM 接收到 AF 的授权检查请求后，获取该授权检查请求中的 SUCI。由于 UDM 可以实现用户永久标识 SUPI 的存贮和管理，同时可以将用户隐藏标识 SUCI 的恢复出 SUPI，比如通过解密功能（UDM 的一部分，或 UDM 外的一个功能）将 SUCI 进行解密。因此，UDM 可以对从授权检查请求中获得的 SUCI 得到 UE 的永久标识 SUPI。

由于 UE 在注册时的签约信息中有规定该 UE 是否可以被授权与邻近设备进行通信，且该签约信息存储在 UDM 中。那么，UDM 获得 UE 的永久标识 SUPI 后，根据该 SUPI 查找该 UE 的签约信息，以判断该 UE 是否被授权与邻近设备进行通信。若签约信息中有规定 UE 可以与邻近设备进行通信，那么，UE 的授权检查通过，否则授权检查不通过。

S604、统一数据管理 UDM 设备向应用功能 AF 发授权检查响应。

具体的，若上述步骤 S603 中 UE 的授权检查通过，那么，UDM 向 AF 发送的授权检

查响应隐式的（比如什么都不传递）或者通过指示信息显式的（比如发送具体的授权结果，或者消息中携带 UE 邻近业务相关参数）指示该 UE 的授权检查通过，AF 可以进一步执行寻找发现可以该 UE 通信的邻近设备的操作。可选的，该指示 UE 授权检查通过的授权检查响应可以包括 UE 的永久标识 SUPI，SUPI 用于 AF 后续跟其他核心网网元交互以获得 UE 的其他参数，比如 QoS 信息；或者，该指示 UE 授权检查通过的授权检查响应可以不包括该 SUPI，甚至可以不包括任何有效的信息，回复一个空的响应。

若上述步骤 S603 中 UE 的授权检查不通过，那么，UDM 向 AF 发送的授权检查响应指示该 UE 的授权检查不通过，AF 还可以进一步执行寻找发现可以该 UE 通信的邻近设备的操作。

参见图 7，示例性示出了在 UE 向核心网网元发送用户面消息触发进一步的交互通信的过程中，为 UE 和核心网网元之间的通信信息配置机密性保护策略的另一种可能的实现方式，包括但不限于如下步骤：

S701、用户设备 UE 向应用功能 AF 发送用户面消息，该用户面消息中包括 UE 的通用公共用户标识(generic public subscription identifier, GPSI)或密钥标识 A-KID。

其中，该 A-KID 可以是 UE 新生成的，AF 也可以相应地自己生成或者从 AAnF 处获取与 UE 相同的新的 A-KID。该 A-KID 也可以是步骤 SA502 或步骤 SC502 中携带的，即已经使用过的 A-KID。本发明不做具体限制。

需要说明的是，在 5G 网络中，在 D2D 场景下的邻近业务 ProSe 发现流程中，应用功能 AF 可以是 5G 网络中的直连通信发现名称管理功能 5GDDNMF。在该场景下，UE 可以向 AF 发送的用户面消息可以是发现请求 Discover Request，用于触发发现 UE 邻近的可通信的设备。

除了上述 D2D 的通信场景中，本申请还可以应用于其它的通信场景，此时，UE 想 AF 发送的用户面消息可以是其它的请求消息等，本方案对此不做限制。下面以用户面消息是发现请求 Discover Request 为例介绍。

具体的，一般情况下，UE 的 GPSI 是 UE 在核心网外部使用的 UE 的标识，SUPI 和 GPSI 之间不一定一一对应，SUPI 一个 UE 只有一个，但是一个 UE 可以有多个 GPSI，因此用户如果访问不同的数据网络，就会存在多个 GPSI 标识，网络需要将外部网络 GPSI 与 SUPI 建立关系，UDM 上保存有 GPSI 与 SUPI 的映射关系。

UE 本地存储有或可以临时生成该 UE 的 GPSI，而密钥标识 A-KID 则是 UE 从上述图 2 所示的流程中获得。

在本申请实施例中，在发现请求中携带 UE 的通用公共用户标识 GPSI 或密钥标识 A-KID，可以减少 UE 的用户隐私泄露的风险。

一种可能的实现方式中，用户设备 UE 向应用功能 AF 发送发现请求之前，UE 还可以先检查 UE 和 AF 之间的机密性保护是否开启，例如，可以参见图 9，图 9 中 S901 用户设备 UE 确定自身与应用功能 AF 之间的通信数据是否开启机密性保护的具体实现可以参见前面机密性保护开启的详细介绍，此处不再赘述。UE 检查完机密性保护是否开启后，可以向 AF 发送用户面消息，参见步骤 S902。若机密性保护开启，那么用户面消息中携带的用户

设备的标识可以是永久标识也可以是加密的身份标识, 如果机密性保护没有开启, 那么用户面消息中携带的用户设备的标识为加密的身份标识。若该加密的身份标识为 UE 的通用公共用户标识 GPSI 或密钥标识 A-KID, 那么, S902 和上述 S701 对应。

一种可能的实现方式中, 用户设备 UE 向应用功能 AF 发送发现请求之前, UE 还可以先检查 UE 和 AF 之间的完整性保护是否开启, 若没有开启, 那么 UE 向 AF 发送的发现请求包括的 UE 的标识为 UE 的隐藏标识。检查完整性保护开启的方式可以参见前面的描述, 此处及下文不再赘述。

S702、应用功能 AF 向统一数据管理 UDM 设备发送授权检查请求, 该授权检查请求包括 UE 的 GPSI 或 A-KID。

具体的, 该 AF 向 UDM 发送的授权检查请求用于确定该 UE 是否被授权与邻近设备进行通信, 只有被授权的情况下, AF 才会继续基于 UE 发送过来的发现请求为其寻找发现邻近的可通信设备。

UDM 需要基于 UE 的永久标识才可以进行授权检查。AF 从 UE 的发现请求中获取的 UE 标识为 GPSI 或 A-KID, 因此, AF 向 UDM 发送的授权请求中包括 UE 的 GPSI 或 A-KID, UDM 可以基于 GPSI 或 A-KID 获取到 UE 的永久标识。

当前网络架构中, AF 可以直接或者间接的与 UDM 进行通信。本实施例以 AF 可以直接与 UDM 进行通信为例进行说明。可以理解的是, 如果当一个 AF 只能间接与 UDM 进行通信, 比如通过网络曝光功能 NEF, 那么本实施例可以自动扩展并适配到该场景中, 此时本实施中的 AF 和 UDM 之间的交互自动包括了 AF-NEF-UDM 三者之间的交互过程。

S703、统一数据管理 UDM 设备根据 UE 的 GPSI 或 A-KID 确定 UE 的 SUPI, 基于 SUPI 对 UE 进行授权检查。

具体的, UDM 接收到 AF 的授权检查请求后, 获取该授权检查请求中的 GPSI 或 A-KID。假设获取的是 GPSI, 那么, 由于 UDM 上保存有 GPSI 与 SUPI 的映射关系, 因此, UDM 可以以 GPSI 为索引查找到 UE 的 SUPI, 然后, 基于 SUPI 对 UE 进行授权检查。

假设上述 UDM 从授权检查请求中获取的是密钥标识 A-KID, 那么, 由于 UDM 上保存有 A-KID 与 SUPI 的映射关系, 因此, UDM 可以以 A-KID 为索引查找到 UE 的 SUPI, 然后, 基于 SUPI 对 UE 进行授权检查。

具体的, UDM 上保存有 A-KID 与 SUPI 的映射关系可以通过如下方式实现: UDM 可以在上述图 2 所示的流程中, 在步骤 S206 中 AUSF 生成 AKMA 锚点密钥 K_{AKMA} 和密钥标识 A-KID 后, AUSF 将生成的密钥标识 A-KID 和/或 SUPI 发送给 UDM, 由 UDM 将该密钥标识 A-KID 和 UE 的 SUPI 关联存储。

上述 UDM 基于 SUPI 对 UE 进行授权检查可以通过如下方式实现: 由于 UE 在注册时的签约信息中有规定该 UE 是否可以被授权与邻近设备进行通信, 且该签约信息存储在 UDM 中。那么, UDM 获得 UE 的永久标识 SUPI 后, 根据该 SUPI 查找该 UE 的签约信息, 以判断该 UE 是否被授权与邻近设备进行通信。若签约信息中有规定 UE 可以与邻近设备进行通信, 那么, UE 的授权检查通过, 否则授权检查不通过。

S704、统一数据管理 UDM 设备向应用功能 AF 发送授权检查响应。

具体的, 若上述步骤 S703 中 UE 的授权检查通过, 那么, UDM 向 AF 发送的授权检

查响应隐式的（比如什么都不传递）或者通过指示信息显式的（比如发送具体的授权结果，或者消息中携带 UE 邻近业务相关参数）指示该 UE 的授权检查通过，AF 可以进一步执行寻找发现可以该 UE 通信的邻近设备的操作。可选的，该指示 UE 授权检查通过的授权检查响应可以包括 UE 的永久标识 SUPI，SUPI 用于 AF 后续跟其他核心网网元交互以获得 UE 的其他参数，比如 QoS 信息；或者，该指示 UE 授权检查通过的授权检查响应可以不包括该 SUPI，甚至可以不包括任何有效的信息，回复一个空的响应。

若上述步骤 S703 中 UE 的授权检查不通过，那么，UDM 向 AF 发送的授权检查响应指示该 UE 的授权检查不通过，AF 还不可以进一步执行寻找发现可以该 UE 通信的邻近设备的操作。

参见图 8，示例性示出了在 UE 向核心网网元发送用户面消息触发进一步的交互通信的过程中，为 UE 和核心网网元之间的通信信息配置机密性保护策略的另一种可能的实现方式，包括但不限于如下步骤：

S801、用户设备 UE 向应用功能 AF 发送用户面消息，该用户面消息中包括 UE 的通用公共用户标识 GPSI 或密钥标识 A-KID。

需要说明的是，在 5G 网络中，在 D2D 场景下的邻近业务 ProSe 发现流程中，应用功能 AF 可以是 5G 网络中的直连通信发现名称管理功能 5GDDNMF。在该场景下，UE 可以向 AF 发送的用户面消息可以是发现请求 Discover Request，用于触发发现 UE 邻近的可通信的设备。

除了上述 D2D 的通信场景中，本申请还可以应用于其它的通信场景，此时，UE 想 AF 发送的用户面消息可以是其它的请求消息等，本方案对此不做限制。下面以用户面消息是发现请求 Discover Request 为例介绍。

具体的，一般情况下，UE 的 GPSI 是 UE 在核心网外部使用的 UE 的标识，SUPI 和 GPSI 之间不一定一一对应，用户如果访问不同的数据网络，就会存在多个 GPSI 标识，网络需要将外部网络 GPSI 与 SUPI 建立关系，UDM 上保存有 GPSI 与 SUPI 的映射关系。

UE 本地存储有该 UE 的 GPSI，而密钥标识 A-KID 则是 UE 从上述图 2 所示的流程中获得。

在本申请实施例中，在发现请求中携带 UE 的通用公共用户标识 GPSI 或密钥标识 A-KID，可以减少 UE 的用户隐私泄露的风险。

一种可能的实现方式中，用户设备 UE 向应用功能 AF 发送发现请求之前，UE 还可以先检查 UE 和 AF 之间的机密性保护是否开启，例如，可以参见图 9，图 9 中 S901 用户设备 UE 确定自身与应用功能 AF 之间的通信数据是否开启机密性保护的具体实现可以参见前面机密性保护开启的详细介绍，此处不再赘述。UE 检查完机密性保护是否开启后，可以向 AF 发送用户面消息，参见步骤 S902。若机密性保护开启，那么用户面消息中携带的用户设备的标识可以是永久标识也可以是加密的身份标识，如果机密性保护没有开启，那么用户面消息中携带的用户设备的标识为加密的身份标识。若该加密的身份标识为 UE 的通用公共用户标识 GPSI 或密钥标识 A-KID，那么，S902 和上述 S801 对应。

一种可能的实现方式中，用户设备 UE 向应用功能 AF 发送发现请求之前，UE 还可以

先检查 UE 和 AF 之间的完整性保护是否开启, 若没有开启, 那么 UE 向 AF 发送的发现请求包括的 UE 的标识为 UE 的隐藏标识。检查完整性保护开启的方式可以参见前面的描述, 此处及下文不再赘述。

S802、应用功能 AF 根据 GPSI 或 A-KID 确定 UE 的 SUPI。

具体的, AF 中存储有 A-KID 与 SUPI 的映射关系, 或者, 应用功能 AF 中存储有 GPSI 与 UE 的 SUPI 的映射关系, 或者 AF 中存储有 GPSI、A-KID 和 SUPI 三者之间的映射关系。那么, AF 可以以 GPSI 或 A-KID 为索引查找到 UE 的 SUPI。

应用功能 AF 中存储有 A-KID 与 UE 的 SUPI 的映射关系可以通过如下方式实现: 在上述图 5A(或图 5C)所示的流程中, 在步骤 S5A03(或图步骤 S5C03)中应用安全锚定功能 AAnF 接收到应用功能 AF 发送的应用密钥获取请求(该请求携带 UE 的 A-KID 和 AF 的标识 AF_ID)后, AAnF 根据 AF 的标识 AF_ID 确定 AF 为 5G 网络中的直连通信发现名称管理功能 5GDDNMF, 然后, 在步骤 SA504(或图步骤 S5C04)中, 应用安全锚定功能 AAnF 向应用功能 AF 发送请求响应时, 可以将 UE 的永久标识 SUPI 发送给 AF, 然后 AF 将 UE 的 SUPI 与 UE 的密钥标识 A-KID 关联存储。

应用功能 AF 中存储有 GPSI 与 UE 的 SUPI 的映射关系可以通过如下方式实现: 应用安全锚定功能 AAnF 可以与鉴权服务器功能 AUSF 交互获取 UE 的 GPSI, 例如, 在上述图 2 所示的流程中, 步骤 S207 中 AUSF 向 AAnF 发送密钥注册请求时, 可以将 GPSI 一起发送给 AAnF; 而 AUSF 获取 GPSI 的方式可以是: 在步骤 S204 中 UDM 向 AUSF 发送鉴权向量响应时, 一起将 GPSI 发送给 AUSF。或者, AAnF 可以向 UDM 发送获取请求消息, 请求获取 UE 的 GPSI, 该请求消息可以携带 UE 的 SUPI, UDM 基于该 SUPI 获取 UE 的 GPSI, 并将该 UE 的 GPSI 发送给 AAnF。AAnF 获取到 UE 的 GPSI 后, 将 GPSI 和 SUPI 关联存储, 或者 GPSI、A-KID 和 SUPI 关联存储。然后, 在应用安全锚定功能 AAnF 接收到应用功能 AF 发送的应用密钥获取请求(该请求携带 UE 的 A-KID 和 AF 的标识 AF_ID)后, AAnF 根据 AF 的标识 AF_ID 确定 AF 为 5G 网络中的直连通信发现名称管理功能 5GDDNMF, 然后, 在步骤 SA504(或步骤 S5C04)中, 应用安全锚定功能 AAnF 向应用功能 AF 发送请求响应时, 可以将 UE 的永久标识 SUPI 和 UE 的 GPSI 一起发送给 AF, 然后 AF 将 UE 的 SUPI 与 UE 的 GPSI 关联存储, 或者 AF 将 UE 的 SUPI、GPSI 与 UE 的密钥标识 A-KID 关联存储。

S803、应用功能 AF 向统一数据管理 UDM 设备发送授权检查请求, 该授权检查请求包括 UE 的 SUPI。

具体的, 该 AF 向 UDM 发送的授权检查请求用于确定该 UE 是否被授权与邻近设备进行通信, 只有被授权的情况下, AF 才会继续基于 UE 发送过来的发现请求为其寻找发现邻近的可通信设备。

UDM 需要基于 UE 的永久标识才可以进行授权检查。AF 从 UE 的发现请求中获取的 UE 标识为永久标识 SUPI, 因此, AF 向 UDM 发送的授权检查请求中包括 UE 的 SUPI。

当前网络架构中, AF 可以直接或者间接的与 UDM 进行通信。本实施例以 AF 可以直接与 UDM 进行通信为例进行说明。可以理解的是, 如果当一个 AF 只能间接与 UDM 进行通信, 比如通过网络曝光功能 NEF, 那么本实施例可以自动扩展并适配到该场景中, 此时

本实施中的 AF 和 UDM 之间的交互自动包括了 AF-NEF-UDM 三者之间的交互过程。

S804、统一数据管理 UDM 设备基于 SUPI 对 UE 进行授权检查。

具体的, 由于 UE 在注册时的签约信息中有规定该 UE 是否可以被授权与邻近设备进行通信, 且该签约信息存储在 UDM 中。那么, UDM 获得 UE 的永久标识 SUPI 后, 根据该 SUPI 查找该 UE 的签约信息, 以判断该 UE 是否被授权与邻近设备进行通信。若签约信息中有规定 UE 可以与邻近设备进行通信, 那么, UE 的授权检查通过, 否则授权检查不通过。

S805、统一数据管理 UDM 设备向应用功能 AF 发送授权检查响应。

具体的, 若上述步骤 S804 中 UE 的授权检查通过, 那么, UDM 向 AF 发送的授权检查响应隐式的 (比如什么都不传递) 或者通过指示信息显式的 (比如发送具体的授权结果, 或者消息中携带 UE 邻近业务相关参数) 指示该 UE 的授权检查通过, AF 可以进一步执行寻找发现可以该 UE 通信的邻近设备的操作。

若上述步骤 S804 中 UE 的授权检查不通过, 那么, UDM 向 AF 发送的授权检查响应指示该 UE 的授权检查不通过, AF 还不可以进一步执行寻找发现可以该 UE 通信的邻近设备的操作。

需要说明的是, 上述图 6 至图 9 所示的流程中是以 UE 选择 AKMA 交互方式为前提实现的。一种可能的实现方式中, 上述图 6 至图 9 所示的流程中, 若在 UE 和核心网进行身份认证的过程中, 例如在上述图 5B 或图 5D 及其可能的实施方式的流程中 UE 选择的是 GBA 的交互方式, 那么, 上述图 6 至图 9 所示的流程中的密钥标识 A-KID 可以换成是密钥标识 B-TID, 应用安全锚定功能 AAnF 替换成引导服务功能 BSF, 统一数据管理 UDM 替换成归属用户服务器 HSS, 上述步骤 S802 中对图 5A、图 5C 和图 2 的相关描述对应替换为图 5B、图 5D 和图 3 中的相关描述, 其它的网元和实现过程类似, 此处不再赘述。

上述图 6 至图 9 所示的流程中, 不管在 UE 和核心网的授权检查过程中是否配置了安全通信策略, UE 和 AF 之间交互的信息均使用具有隐私属性的用户标识, 从而减少了 UE 的永久标识泄露的风险, 进而减少了用户隐私泄露的风险。

一种可能的实现方式中, 上述图 6 至图 9 所示的流程不一定是在上述图 4、图 5A 至图 5D 所示的流程完成之后执行的, 可以是任何有需要的情况下尽可以发起上述图 6 至图 9 所示的流程, 本方案对发起该图 6 至图 9 所示的流程的具体场景不做限制。

一种可能的实现方式中, 上述图 6 至图 9 中 AF 向 UDM 发起授权检查的流程也不限于是接收到 UE 的用户面消息触发的, 可以是接收到其它的设备, 例如接入网设备等的消息触发的, 本方案对此不做限制。

一种可能的实现方式中, 上述图 6 至图 9 中 AF 向 UDM 发起授权检查的流程不限于检查 UE 是否被授权与邻近设备通信, 也可以是检查其它设备是否被授权与邻近设备通信或者是否被授权参与其它的某个流程等等, 本方案对此不做限制。

上述主要对本申请实施例提供的安全通信方法进行了介绍。可以理解的是, 各个设备为了实现上述对应的功能, 其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到, 结合本文中所公开的实施例描述的各示例的单元及算法步骤, 本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算

机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用使用不同方法来实现所描述的功能，但这种实现不应认为超出本申请的范围。

本申请实施例可以根据上述方法示例对设备进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

在采用对应各个功能划分各个功能模块的情况下，图 10 示出了装置的一种可能的逻辑结构示意图，该装置可以是上述的用户设备，或者可以是该用户设备中的芯片，或者可以是该用户设备中的处理系统等。该装置 1000 包括第一确定单元 1001 和发送单元 1002。其中：

第一确定单元 1001，用于确定装置 1000 与应用功能设备之间的通信数据是否开启机密性保护；

发送单元 1002，用于向应用功能设备发送用户面消息，用户面消息中包括装置 1000 的标识；其中，在没有开启机密性保护的情况下，标识为加密的身份标识。

一种可能的实施方式中，装置 1000 还包括：

第二确定单元，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在装置 1000 与应用功能设备之间交互。

一种可能的实施方式中，具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

一种可能的实施方式中，第二确定单元具体用于：

在满足如下条件中的一项或多项的情况下，确定使用具有隐私保护的流程：

装置 1000 启动的应用程序指示装置 1000 选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，装置 1000 接收到优先选择具有隐私保护的流程的指示；

或者，装置 1000 确定自身使用了 5G 全球用户识别卡；

或者，装置 1000 确定自身中存在有效的公私钥；

或者，装置 1000 确定用户面消息中需要携带装置 1000 的永久标识。

一种可能的实施方式中，装置 1000 还包括：

接收单元，用于接收来自应用功能设备的加密算法信息；

没有开启机密性保护的情况，包括：

加密算法信息指示加密算法为空算法的情况。

一种可能的实施方式中，加密的身份标识为用户隐藏标识 SUCI、通用公共用户标识

GPSI 或者密钥标识 A-KID。

一种可能的实施方式中，用户面消息为邻近业务 Prose 流程中的发现请求 Discovery request。

图 10 所示装置 1000 中各个单元的具体操作以及有益效果可以参见上述图 4 至图 9 所述方法及其可能的实施方式中对应的描述，此处不再赘述。

在采用对应各个功能划分各个功能模块的情况下，图 11 示出了装置的一种可能的逻辑结构示意图，该装置可以是上述的用户设备，或者可以是该用户设备中的芯片，或者可以是该用户设备中的处理系统等。该装置 1100 包括第一确定单元 1101、第二确定单元 1102 和发送单元 1103。其中：

第一确定单元 1101，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在装置 1100 与应用功能设备之间交互；

第二确定单元 1102，用于基于具有隐私保护的流程确定与应用功能设备的通信密钥和非空加密算法；

发送单元 1103，用于向应用功能设备发送用户面消息，用户面消息中包括装置 1100 的标识；其中，用户面消息由通信密钥和非空加密算法进行机密性保护。

一种可能的实施方式中，第一确定单元 1101 具体用于：

在满足如下条件中的一项或多项的情况下，确定使用具有隐私保护的流程：

装置 1100 启动的应用程序指示装置 1100 选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，装置 1100 接收到优先选择具有隐私保护的流程的指示；

或者，装置 1100 确定自身使用了 5G 全球用户识别卡；

或者，装置 1100 确定自身中存在有效的公私钥；

或者，装置 1100 确定用户面消息中需要携带装置 1100 的永久标识。

一种可能的实施方式中，第二确定单元 1102 具体用于：

基于自身存储的锚点密钥生成通信密钥；

向应用功能设备发送请求消息，请求消息包括密钥标识和指示使用具有隐私保护的流程的信息，密钥标识用于协助应用该功能设备获取通信密钥；

接收来自应用功能设备的响应消息，响应消息包括非空加密算法的信息。

一种可能的实施方式中，请求消息中还包括协商非空加密算法的指示信息。

一种可能的实施方式中，请求消息中还包括装置 1100 支持的加密算法的信息，装置 1100 支持的加密算法的信息用于指示应用功能设备选择非空加密算法，装置 1100 支持的加密算法为非空加密算法。

图 11 所示装置 1100 中各个单元的具体操作以及有益效果可以参见上述图 4 至图 9 所

述方法及其可能的实施方式中对应的描述，此处不再赘述。

在采用对应各个功能划分各个功能模块的情况下，图 12 示出了装置的一种可能的逻辑结构示意图，该装置可以是上述的用户设备，或者可以是该用户设备中的芯片，或者可以是该用户设备中的处理系统等。该装置 1200 包括第一确定单元 1201、第二确定单元 1202 和发送单元 1203。其中：

第一确定单元 1201，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在装置 1200 与应用功能设备之间交互；

第二确定单元 1202，用于基于具有隐私保护的流程确定与应用功能设备的通信密钥；

发送单元 1203，用于向应用功能设备发送用户面消息，用户面消息中包括装置 1200 加密的身份标识；其中，用户面消息由通信密钥进行机密性保护。

一种可能的实施方式中，具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

一种可能的实施方式中，用第一确定单元 1201 具体用于：在满足如下条件中的一项或多项的情况下，确定使用具有隐私保护的流程：

装置 1200 启动的应用程序指示装置 1200 选择具有隐私保护的流程，应用程序的服务器包括在应用功能设备中；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程；

或者，应用程序指示能够选择多种交互流程中的一种，多种交互流程包括具有隐私保护的流程，具有隐私保护的流程的优先级最高；

或者，装置 1200 接收到优先选择具有隐私保护的流程的指示；

或者，装置 1200 确定自身使用了 5G 全球用户识别卡；

或者，装置 1200 确定自身中存在有效的公私钥；

或者，装置 1200 确定用户面消息中需要携带装置 1200 的永久标识。

图 12 所示装置 1200 中各个单元的具体操作以及有益效果可以参见上述图 4 至图 9 所述方法及其可能的实施方式中对应的描述，此处不再赘述。

请参见图 13，为本申请提供的一种通信装置的结构示意图。

请参见图 13，为本申请提供的一种通信装置的结构示意图。图 13 所示的通信装置 1300 包括收发模块 1301 和处理模块 1302。

在一种设计中，装置 1300 为用户设备：

示例性的，处理模块 1302，用于确定该通信装置与应用功能设备之间的通信数据是否开启机密性保护；

收发模块 1301，用于向应用功能设备发送用户面消息，用户面消息中包括装置 1300 的标识；其中，在没有开启机密性保护的情况下，标识为加密的身份标识。

示例性地，处理模块 1302，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在装置 1300 与应用功能设备之间交互；并基于具有隐私保护的流程确定与应用功能设

备的通信密钥和非空加密算法；

收发模块 1301，用于向应用功能设备发送用户面消息，用户面消息中包括装置 1300 的标识；其中，用户面消息由通信密钥和非空加密算法进行机密性保护。

示例性地，处理模块 1302，用于确定使用具有隐私保护的流程，具有隐私保护的流程用于在装置 1300 与应用功能设备之间交互；并基于具有隐私保护的流程确定与应用功能设备的通信密钥；

收发模块 1301，用于向应用功能设备发送用户面消息，用户面消息中包括装置 1300 加密的身份标识；其中，用户面消息由通信密钥进行机密性保护。

该示例用于实现上述图 4 至图 9 所述方法及其可能的实施方式中用户设备对应的功能。

请参见图 14，为本申请提供的另一种通信装置的结构示意图。图 14 所示的通信装置 1400 包括至少一个处理器 1401、存储器 1402，可选的，还可包括通信接口 1403。

存储器 1402 可以是易失性存储器，例如随机存取存储器；存储器也可以是非易失性存储器，例如只读存储器，快闪存储器，硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD）、或者存储器 1402 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器 1402 可以是上述存储器的组合。

本申请实施例中不限定上述处理器 1401 以及存储器 1402 之间的具体连接介质。本申请实施例在图中以存储器 1402 和处理器 1401 之间通过总线 1404 连接，总线 1404 在图中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。该总线 1404 可以分为地址总线、数据总线、控制总线等。为便于表示，图 14 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。

处理器 1401 可以具有数据收发功能，能够与其他设备进行通信，在如图 14 装置中，也可以设置独立的数据收发模块，例如通信接口 1403，用于收发数据；处理器 1401 在与其他设备进行通信时，可以通过通信接口 1403 进行数据传输。

一种示例中，当用户设备采用图 14 所示的形式时，图 14 中的处理器可以通过调用存储器 1402 中存储的计算机执行指令，使得用户设备执行上述任一方法实施例中的用户设备执行的方法。

具体的，图 13 的处理模块和收发模块的功能/实现过程均可以通过图 14 中的处理器 1401 调用存储器 1402 中存储的计算机执行指令来实现。或者，图 13 的处理模块的功能/实现过程可以通过图 14 中的处理器 1401 调用存储器 1402 中存储的计算机执行指令来实现，图 13 的收发模块的功能/实现过程可以通过图 14 中的通信接口 1403 来实现。

本申请还提供了一种计算机可读介质，其上存储有计算机程序，该计算机程序被计算机执行时实现上述任一方法实施例的功能。

本申请还提供了一种计算机程序产品，该计算机程序产品被计算机执行时实现上述任一方法实施例的功能。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。

当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line, DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，高密度数字视频光盘（digital video disc, DVD））、或者半导体介质（例如，固态硬盘（solid state disk, SSD））等。

可以理解，说明书通篇中提到的“实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各个实施例未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。可以理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本申请实施例的实施过程构成任何限定。

可以理解，在本申请中，“当...时”、“若”以及“如果”均指在某种客观情况下装置会做出相应的处理，并非是限定时间，且也不要求装置实现时一定要有所判断的动作，也不意味着存在其它限定。

本申请中对于使用单数表示的元素旨在用于表示“一个或多个”，而并非表示“一个且仅一个”，除非有特别说明。本申请中，在没有特别说明的情况下，“至少一个”旨在用于表示“一个或者多个”，“多个”旨在用于表示“两个或两个以上”。

另外，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种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 这三种情况，其中 A 可以是单数或者复数，B 可以是单数或者复数。

本申请中的预定义可以理解为定义、预先定义、存储、预存储、预协商、预配置、固化、或预烧制。

本领域普通技术人员可以理解，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

本申请中各个实施例之间相同或相似的部分可以互相参考。在本申请中各个实施例、以及各实施例中的各个实施方式/实施方法/实现方法中，如果没有特殊说明以及逻辑冲突，不同的实施例之间、以及各实施例中的各个实施方式/实施方法/实现方法之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例、以及各实施例中的各个实施方式/实施方法/实现方法中的技术特征根据其内在的逻辑关系可以组合形成新的实施例、实施方式、实施方法、或实现方法。以上所述的本申请实施方式并不构成对本申请保护范围的限定。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。

权 利 要 求

- 1、一种安全通信的方法，其特征在于，包括：
用户设备确定自身与应用功能设备之间的通信数据是否开启机密性保护；
所述用户设备向所述应用功能设备发送用户面消息，所述用户面消息中包括所述用户设备的标识；其中，在没有开启所述机密性保护的情况下，所述标识为加密的身份标识。
- 2、根据权利要求1所述的方法，其特征在于，所述方法还包括：
所述用户设备确定使用具有隐私保护的流程，所述具有隐私保护的流程用于在所述用户设备与所述应用功能设备之间交互。
- 3、根据权利要求2所述的方法，其特征在于，所述具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。
- 4、根据权利要求2或3所述的方法，其特征在于，所述用户设备确定使用具有隐私保护的流程，包括：在满足如下条件中的一项或多项的情况下，所述用户设备确定使用所述具有隐私保护的流程：
所述用户设备启动的应用程序指示所述用户设备选择所述具有隐私保护的流程，所述应用程序的服务器包括在所述应用功能设备中；
或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述具有隐私保护的流程；
或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述所述具有隐私保护的流程，所述具有隐私保护的流程的优先级最高；
或者，所述用户设备接收到优先选择所述所述具有隐私保护的流程的指示；
或者，所述用户设备确定自身使用了 5G 全球用户识别卡；
或者，所述用户设备确定自身中存在有效的公私钥；
或者，所述用户设备确定所述用户面消息中需要携带所述用户设备的永久标识。
- 5、根据权利要求1-4任一所述的方法，其特征在于，所述方法还包括：
所述用户设备接收来自所述应用功能设备的加密算法信息；
所述没有开启所述机密性保护的情况，包括：
所述加密算法信息指示加密算法为空算法的情况。
- 6、根据权利要求1-5任一所述的方法，其特征在于，所述加密的身份标识为用户隐藏标识 SUCI、通用公共用户标识 GPSI 或者密钥标识 A-KID。
- 7、根据权利要求1-6任一所述的方法，其特征在于，所述用户面消息为邻近业务 Prose 流程中的发现请求 Discovery request。

8、一种安全通信的方法，其特征在于，包括：

用户设备确定使用具有隐私保护的流程，所述具有隐私保护的流程用于在所述用户设备与应用功能设备之间交互；

所述用户设备基于所述具有隐私保护的流程确定与所述应用功能设备的通信密钥和非空加密算法；

所述用户设备向所述应用功能设备发送用户面消息，所述用户面消息中包括所述用户设备的标识；其中，所述用户面消息由所述通信密钥和所述非空加密算法进行机密性保护。

9、根据权利要求8所述的方法，其特征在于，所述用户设备确定使用具有隐私保护的流程，包括：在满足如下条件中的一项或多项的情况下，所述用户设备确定使用所述具有隐私保护的流程：

所述用户设备启动的应用程序指示所述用户设备选择所述具有隐私保护的流程，所述应用程序的服务器包括在所述应用功能设备中；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述具有隐私保护的流程；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述所述具有隐私保护的流程，所述具有隐私保护的流程的优先级最高；

或者，所述用户设备接收到优先选择所述所述具有隐私保护的流程的指示；

或者，所述用户设备确定自身使用了5G全球用户识别卡；

或者，所述用户设备确定自身中存在有效的公私钥；

或者，所述用户设备确定所述用户面消息中需要携带所述用户设备的永久标识。

10、根据权利要求8或9所述的方法，其特征在于，所述用户设备基于所述具有隐私保护的流程确定与所述应用功能设备的通信密钥和非空加密算法，包括：

所述用户设备基于自身存储的锚点密钥生成所述通信密钥；

所述用户设备向所述应用功能设备发送请求消息，所述请求消息包括密钥标识和指示使用所述具有隐私保护的流程的信息，所述密钥标识用于协助所述应用该功能设备获取所述通信密钥；

所述用户设备接收来自所述应用功能设备的响应消息，所述响应消息包括所述非空加密算法的信息。

11、根据权利要求10所述的方法，其特征在于，所述请求消息中还包括协商非空加密算法的指示信息。

12、根据权利要求10所述的方法，其特征在于，所述请求消息中还包括所述用户设备支持的加密算法的信息，所述用户设备支持的加密算法的信息用于指示所述应用功能设备选择非空加密算法，所述用户设备支持的加密算法为非空加密算法。

13、一种安全通信的方法，其特征在于，包括：

用户设备确定使用具有隐私保护的流程，所述具有隐私保护的流程用于在所述用户设备与应用功能设备之间交互；

所述用户设备基于所述具有隐私保护的流程确定与所述应用功能设备的通信密钥；

所述用户设备向所述应用功能设备发送用户面消息，所述用户面消息中包括所述用户设备加密的身份标识；其中，所述用户面消息由所述通信密钥进行机密性保护。

14、根据权利要求 13 所述的方法，其特征在于，所述具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

15、根据权利要求 13 所述的方法，其特征在于，所述用户设备确定使用具有隐私保护的流程，包括：在满足如下条件中的一项或多项的情况下，所述用户设备确定使用所述具有隐私保护的流程：

所述用户设备启动的应用程序指示所述用户设备选择所述具有隐私保护的流程，所述应用程序的服务器包括在所述应用功能设备中；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述具有隐私保护的流程；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述所述具有隐私保护的流程，所述具有隐私保护的流程的优先级最高；

或者，所述用户设备接收到优先选择所述所述具有隐私保护的流程的指示；

或者，所述用户设备确定自身使用了 5G 全球用户识别卡；

或者，所述用户设备确定自身中存在有效的公私钥；

或者，所述用户设备确定所述用户面消息中需要携带所述用户设备的永久标识。

16、一种用户设备，其特征在于，所述用户设备包括：

第一确定单元，用于确定所述用户设备与应用功能设备之间的通信数据是否开启机密性保护；

发送单元，用于向所述应用功能设备发送用户面消息，所述用户面消息中包括所述用户设备的标识；其中，在没有开启所述机密性保护的情况下，所述标识为加密的身份标识。

17、根据权利要求 16 所述的用户设备，其特征在于，所述用户设备还包括：

第二确定单元，用于确定使用具有隐私保护的流程，所述具有隐私保护的流程用于在所述用户设备与所述应用功能设备之间交互。

18、根据权利要求 17 所述的用户设备，其特征在于，所述具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

19、根据权利要求 17 或 18 所述的用户设备，其特征在于，所述第二确定单元具体用于：

在满足如下条件中的一项或多项的情况下，确定使用所述具有隐私保护的流程：

所述用户设备启动的应用程序指示所述用户设备选择所述具有隐私保护的流程，所述应用程序的服务器包括在所述应用功能设备中；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述具有隐私保护的流程；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述所述具有隐私保护的流程，所述具有隐私保护的流程的优先级最高；

或者，所述用户设备接收到优先选择所述所述具有隐私保护的流程的指示；

或者，所述用户设备确定自身使用了 5G 全球用户识别卡；

或者，所述用户设备确定自身中存在有效的公私钥；

或者，所述用户设备确定所述用户面消息中需要携带所述用户设备的永久标识。

20、根据权利要求 16-19 任一所述的用户设备，其特征在于，所述用户设备还包括：

接收单元，用于接收来自所述应用功能设备的加密算法信息；

所述没有开启所述机密性保护的情况，包括：

所述加密算法信息指示加密算法为空算法的情况。

21、根据权利要求 16-20 任一所述的用户设备，其特征在于，所述加密的身份标识为用户隐藏标识 SUCI、通用公共用户标识 GPSI 或者密钥标识 A-KID。

22、根据权利要求 16-21 任一所述的用户设备，其特征在于，所述用户面消息为邻近业务 Prose 流程中的发现请求 Discovery request。

23、一种用户设备，其特征在于，所述用户设备包括：

第一确定单元，用于确定使用具有隐私保护的流程，所述具有隐私保护的流程用于在所述用户设备与应用功能设备之间交互；

第二确定单元，用于基于所述具有隐私保护的流程确定与所述应用功能设备的通信密钥和非空加密算法；

发送单元，用于向所述应用功能设备发送用户面消息，所述用户面消息中包括所述用户设备的标识；其中，所述用户面消息由所述通信密钥和所述非空加密算法进行机密性保护。

24、根据权利要求 23 所述的用户设备，其特征在于，所述第一确定单元具体用于：

在满足如下条件中的一项或多项的情况下，确定使用所述具有隐私保护的流程：

所述用户设备启动的应用程序指示所述用户设备选择所述具有隐私保护的流程，所述应用程序的服务器包括在所述应用功能设备中；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述具有隐私保护的流程；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述所述具有隐私保护的流程，所述具有隐私保护的流程的优先级最高；

或者，所述用户设备接收到优先选择所述所述具有隐私保护的流程的指示；

或者，所述用户设备确定自身使用了 5G 全球用户识别卡；

或者，所述用户设备确定自身中存在有效的公私钥；

或者，所述用户设备确定所述用户面消息中需要携带所述用户设备的永久标识。

25、根据权利要求 23 或 24 所述的设备，其特征在于，所述第二确定单元具体用于：

基于自身存储的锚点密钥生成所述通信密钥；

向所述应用功能设备发送请求消息，所述请求消息包括密钥标识和指示使用所述具有隐私保护的流程的信息，所述密钥标识用于协助所述应用该功能设备获取所述通信密钥；

接收来自所述应用功能设备的响应消息，所述响应消息包括所述非空加密算法的信息。

26、根据权利要求 25 所述的设备，其特征在于，所述请求消息中还包括协商非空加密算法的指示信息。

27、根据权利要求 25 所述的设备，其特征在于，所述请求消息中还包括所述用户设备支持的加密算法的信息，所述用户设备支持的加密算法的信息用于指示所述应用功能设备选择非空加密算法，所述用户设备支持的加密算法为非空加密算法。

28、一种用户设备，其特征在于，所述用户设备包括：

第一确定单元，用于确定使用具有隐私保护的流程，所述具有隐私保护的流程用于在所述用户设备与应用功能设备之间交互；

第二确定单元，用于基于所述具有隐私保护的流程确定与所述应用功能设备的通信密钥；

发送单元，用于向所述应用功能设备发送用户面消息，所述用户面消息中包括所述用户设备加密的身份标识；其中，所述用户面消息由所述通信密钥进行机密性保护。

29、根据权利要求 28 所述的用户设备，其特征在于，所述具有隐私保护的流程包括应用中认证和密钥协商 AKMA 流程。

30、根据权利要求 28 或 29 所述的用户设备，其特征在于，所述用第一确定单元具体用于：在满足如下条件中的一项或多项的情况下，确定使用所述具有隐私保护的流程：

所述用户设备启动的应用程序指示所述用户设备选择所述具有隐私保护的流程，所述应用程序的服务器包括在所述应用功能设备中；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所

述具有隐私保护的流程；

或者，所述应用程序指示能够选择多种交互流程中的一种，所述多种交互流程包括所述所述具有隐私保护的流程，所述具有隐私保护的流程的优先级最高；

或者，所述用户设备接收到优先选择所述所述具有隐私保护的流程的指示；

或者，所述用户设备确定自身使用了 5G 全球用户识别卡；

或者，所述用户设备确定自身中存在有效的公私钥；

或者，所述用户设备确定所述用户面消息中需要携带所述用户设备的永久标识。

31、一种通信装置，其特征在于，所述通信装置包括处理模块和收发模块，所述处理模块和所述收发模块用于所述用户设备执行权利要求 1 至 7 中任一项所述的方法；或者，所述处理模块和所述收发模块用于所述用户设备执行权利要求 8 至 12 中任一项所述的方法；或者，所述处理模块和所述收发模块用于所述用户设备执行权利要求 13 至 15 中任一项所述的方法。

32、一种通信装置，其特征在于，所述通信装置包括：处理器，所述处理器与存储器耦合，所述存储器用于存储计算机程序，当所述计算机程序被所述处理器执行时，使得所述装置执行如权利要求 1 至 7 中任一项所述的方法；或者，当所述计算机程序被所述处理器执行时，使得所述装置执行如权利要求 8 至 12 中任一项所述的方法；或者，当所述计算机程序被所述处理器执行时，使得所述装置执行如权利要求 13 至 15 中任一项所述的方法。

33、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被执行时使得计算机执行如权利要求 1 至 7 中任一项所述的方法；或者，所述计算机程序被执行时使得计算机执行如权利要求 8 至 12 中任一项所述的方法；所述计算机程序被执行时使得计算机执行如权利要求 13 至 15 中任一项所述的方法。

34、一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行如权利要求 1 至 7，8 至 12 或者 13 至 15 中任一项所述的方法。