

说明书

获取安全上下文的方法、装置和通信系统

5       本申请要求于 2019 年 05 月 31 日提交中国专利局、申请号为 201910470895.8、申请名称为“获取安全上下文的方法、装置和通信系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

10       本发明涉及通信领域，并且更具体地，涉及一种获取安全上下文的方法、装置和通信系统。

背景技术

      在第五代（5th generation，5G）通信场景下，由于用户设备的移动，存在为用户设备提供服务的网络设备发生变化的情况。一种可能的切换场景是用户设备由第四代（4th generation，4G）通信系统中切换到了 5G 通信系统中，这种切换场景下对于用户设备来说就是接入网设备部分由 4G 接入网设备切换到了 5G 接入网设备，而核心网设备部分则由 4G 核心网设备切换到了 5G 核心网设备，其中，核心网设备部分的切换包括为用户设备提供移动管理服务的核心网网元之间的切换，也就是从 4G 通信系统中的移动性管理实体（mobility management entity，MME）切换到了 5G 通信系统中的接入和移动管理功能（access and mobility management function，AMF）。

20       现有的用户设备从 4G 通信系统切换至 5G 通信系统的场景下，在 5G 通信系统中除了被 MME 选择的 AMF（第一 AMF）之外还包括保存有用户设备的安全上下文的 AMF（第二 AMF），此时，第一 AMF 如何从第二 AMF 中获取用户设备的安全上下文成为亟待解决的问题。

发明内容

      本申请提供一种获取安全上下文的方法、装置和通信系统，通过基于用户设备与第二 AMF 之间的本地安全上下文对第一 AMF 在向第二 AMF 发送的第二注册请求消息进行完整性保护，以使得第二 AMF 能够基于用户设备与第二 AMF 之间的本地安全上下文校验第二注册请求消息的完整性，从而能够提高第二 AMF 校验第二注册请求消息成功的可能性，若验证成功，则第一 AMF 就能够成功的从第二 AMF 处获取用户设备的安全上下文。

      第一方面，提供了一种获取安全上下文的方法，包括：第一接入和移动管理功能 AMF 接收用户设备发送的第一注册请求消息，所述第一注册请求消息中携带第二注册请求消息，所述第二注册请求消息被第一安全上下文进行过完整性保护，所述第一安全上下文为所述用户设备与第二 AMF 之间的本地安全上下文，其中，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；所述第一 AMF 向所述第二 AMF 发送所述第二注册请求消息；所述第二 AMF 校验

所述第二注册请求消息的完整性；若所述第二 AMF 校验所述第二注册请求消息的完整性成功，则所述第二 AMF 向所述第一 AMF 发送所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法，在用户设备从 4G 通信系统切换至 5G 通信系统时，在切换之前用户设备与第二 AMF 之间保存有用户设备的安全上下文，在用户设备从 4G 通信系统切换至 5G 通信系统之后，为用户设备提供接入和移动管理服务为第一 AMF，该第一 AMF 需要从第二 AMF 处获得上述的用户设备的安全上下文，具体地，用户设备可以在接收到切换命令之后，基于本地保存的与第二 AMF 之间的安全上下文对第四注册请求消息进行完整性保护，生成第二注册请求消息，在向第一 AMF 发送第一注册请求消息，并在第一注册请求消息中携带该第二注册请求消息，使得第一 AMF 可以将该第二注册请求消息转发给第二 AMF，则第二 AMF 可以校验该第二注册请求消息的完整性，第二 AMF 校验第二注册请求消息的完整性成功之后，可以将上述用户设备的安全上下文返回给第一 AMF，能够提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

结合第一方面，在第一方面的某些实现方式中，所述用户设备的安全上下文包括：所述第一安全上下文，或者，基于所述第一安全上下文获取的第二安全上下文。

本申请实施例提供的获取安全上下文的方法，上述用户设备的安全上下文可以是用户设备与第二 AMF 之间的本地安全上下文，或者，当第二 AMF 进行密钥推演之后生成了新的密钥的情况下，上述用户设备的安全上下文还可以是基于所述第一安全上下文进行密钥推演生成的第二安全上下文。

结合第一方面，在第一方面的某些实现方式中，所述第一 AMF 向所述第二 AMF 发送所述第二注册请求消息，包括：所述第一 AMF 向所述第二 AMF 发送用户设备上下文传输服务调用请求，所述用户设备上下文传输服务调用请求中携带所述第二注册请求消息。

本申请实施例提供的获取安全上下文的方法，第一 AMF 向第二 AMF 发送上述的第二注册请求消息可以在第一 AMF 向第二 AMF 发送用户设备上下文传输服务调用请求中携带第二注册请求消息。

结合第一方面，在第一方面的某些实现方式中，所述第二 AMF 向所述第一 AMF 发送所述用户设备的安全上下文，包括：所述第二 AMF 向所述第一 AMF 发送第一响应消息，所述第一响应消息中携带所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法，第二 AMF 向第一 AMF 返回上述的用户设备的安全上下文时，可以是向第一 AMF 发送第一响应消息，并在第一响应消息中携带上述用户设备的安全上下文。

结合第一方面，在第一方面的某些实现方式中，所述方法还包括：当所述第一 AMF 接收到所述第二 AMF 校验所述第二注册请求消息的完整性失败的消息时，所述第一 AMF 继续使用映射的安全上下文或向所述用户设备发起初始认证。

本申请实施例提供的获取安全上下文的方法，当第一 AMF 从第二 AMF 处获取用户设备的安全上下文失败的情况下，第一 AMF 可以继续使用与用户设备之间协商生成的映射的安全上下文，或者，第一 AMF 可以向用户设备发起初始认证生成第一 AMF 与用户设备之间安全上下文。

结合第一方面，在第一方面的某些实现方式中，所述映射的安全上下文是根据移动管理实体 MME 与所述用户设备之间的安全上下文获得的；其中所述 MME 为所述 4G 通信系统的网元。

5 本申请实施例提供的获取安全上下文的方法中涉及到的映射的安全上下文指的是用户设备和第一 AMF 分别基于用户设备与 MME 之间的安全上下文推导生成的安全上下文。

结合第一方面，在第一方面的某些实现方式中，所述第二 AMF 校验所述第二注册请求消息的完整性，包括：所述第二 AMF 根据所述第二 AMF 与所述用户设备之间的本地安全上下文对所述第二注册请求消息的完整性进行校验。

第二方面，提供了一种获取安全上下文的方法，包括：第二接入和移动管理功能 AMF  
10 接收第一 AMF 发送的第二注册请求消息，所述第二注册请求消息被第一安全上下文进行过完整性保护，所述第一安全上下文为用户设备与所述第二 AMF 之间的本地安全上下文，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；所述第二 AMF 校验所述第二注册请求消息的完整性；若所述第二 AMF 校验所述第二注册请求消息的完整性成功，则所述第二 AMF 向所述第一  
15 AMF 发送所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法，在用户设备从 4G 通信系统切换至 5G 通信系统时，在切换之前用户设备与第二 AMF 之间保存有用户设备的安全上下文，在用户设备从 4G 通信系统切换至 5G 通信系统之后，为用户设备提供接入和移动管理服务为第一 AMF，该第一 AMF 需要从第二 AMF 处获得上述的用户设备的安全上下文，具体地，  
20 用户设备可以在接收到切换命令之后，基于本地保存的与第二 AMF 之间的安全上下文对第四注册请求消息进行完整性保护之后，生成第二注册请求消息，UE 在向第一 AMF 发送的第一注册请求消息中携带该第二注册请求消息，使得第一 AMF 可以将该第二注册请求消息转发给第二 AMF，第二 AMF 可以校验第二注册请求消息的完整性，并在校验第二注册请求消息的完整性成功的情况下，向第一 AMF 发送用户设备的安全上下文，能够提  
25 高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

结合第二方面，在第二方面的某些实现方式中，所述用户设备的安全上下文包括：所述第一安全上下文，或者，基于所述第一安全上下文进行密钥推演生成的第二安全上下文。

本申请实施例提供的获取安全上下文的方法，上述用户设备的安全上下文可以是用户设备与第二 AMF 之间的本地安全上下文，或者，当第二 AMF 进行密钥推演之后生成了新的密钥的情况下，上述用户设备的安全上下文还可以是基于所述第一安全上下文进行密钥推演生成的第二安全上下文。  
30

结合第二方面，在第二方面的某些实现方式中，所述第二 AMF 接收所述第一 AMF 发送的所述第二注册请求消息，包括：所述第二 AMF 接收所述第一 AMF 发送的用户设备上下文传输服务调用请求，所述用户设备上下文传输服务调用请求中携带所述第二注册请求消息。  
35

本申请实施例提供的获取安全上下文的方法，第一 AMF 向第二 AMF 发送上述的第二注册请求消息可以是在第一 AMF 向第二 AMF 发送用户设备上下文传输服务调用请求中携带第二注册请求消息。

结合第二方面，在第二方面的某些实现方式中，所述第二 AMF 向所述第一 AMF 发

送所述用户设备的安全上下文，包括：所述第二 AMF 向所述第一 AMF 发送第一响应消息，所述第一响应消息中携带所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法，第二 AMF 向第一 AMF 返回上述的用户设备的安全上下文时，可以是向第一 AMF 发送第一响应消息，并在第一响应消息中携带上述用户设备的安全上下文。

结合第二方面，在第二方面的某些实现方式中，所述第二 AMF 校验所述第二注册请求消息的完整性，包括：所述第二 AMF 根据所述第一安全上下文对所述第二注册请求消息的完整性进行校验。

第三方面，提供了一种获取安全上下文的方法，包括：用户设备确定第二注册请求消息进行完整性保护，所述第二注册请求消息被第一安全上下文进行过完整性保护，其中，所述第一安全上下文为所述用户设备与第二接入和移动管理功能 AMF 之间的本地安全上下文；所述用户设备向第一接入和移动管理功能 AMF 发送第一注册请求消息，所述第一注册请求消息中携带第二注册请求消息，其中，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF。

本申请实施例提供的获取安全上下文的方法，在用户设备从 4G 通信系统切换至 5G 通信系统时，在切换之前用户设备与第二 AMF 之间保存有用户设备的安全上下文，该用户设备的安全上下文，在用户设备从 4G 通信系统切换至 5G 通信系统之后，为用户设备提供接入和移动管理服务为第一 AMF，该第一 AMF 需要从第二 AMF 处获得上述的用户设备的安全上下文，具体地，用户设备可以在接收到切换命令之后，基于本地保存的与第二 AMF 之间的安全上下文对第四注册请求消息进行完整性保护之后，生成第二注册请求消息，UE 在向第一 AMF 发送的第一注册请求消息中携带该第二注册请求消息，使得第一 AMF 可以将该第二注册请求消息转发给第二 AMF，则第二 AMF 可以校验该第二注册请求消息的完整性，第二 AMF 校验该第二注册请求消息的完整性成功之后，可以将上述用户设备的安全上下文返回给第一 AMF，能够提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

结合第三方面，在第三方面的某些实现方式中，所述方法还包括：若接收到所述第一 AMF 发送的非接入层安全模式命令 NAS SMC 消息，则对所述 NAS SMC 进行完整校验；若校验成功，则向所述第一 AMF 发送非接入层安全模式完成消息。

本申请实施例提供的获取安全上下文的方法，如果用户设备接收到第一 AMF 发送的 NAS SMC 消息，并且用户设备校验该 NAS SMC 消息成功，则用户设备向第一 AMF 发送非接入层安全模式完成消息。

第四方面，提供了一种获取安全上下文的方法，包括：第一接入和移动管理功能 AMF 接收用户设备发送的第一注册请求消息，所述第一注册请求消息中携带第二注册请求消息，所述第二注册请求消息被第一安全上下文进行过完整性保护，所述第一安全上下文为所述用户设备与第二 AMF 之间的本地安全上下文，其中，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；所述第一 AMF 向所述第二 AMF 发送所述第二注册请求消息；若所述第二 AMF 校验所述第二注册请求消息的完整性成功，则所述第一 AMF 接收所述第二 AMF 发送的所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法，在用户设备从 4G 通信系统切换至 5G 通信系统时，在切换之前用户设备与第二 AMF 之间保存有用户设备的安全上下文，在用户设备从 4G 通信系统切换至 5G 通信系统之后，为用户设备提供接入和移动管理服务为第一 AMF，该第一 AMF 需要从第二 AMF 处获得上述的用户设备的安全上下文，具体地，

5 用户设备可以在接收到切换命令之后，基于本地保存的与第二 AMF 之间的安全上下文对第四注册请求消息进行完整性保护之后，生成第二注册请求消息，UE 在向第一 AMF 发送的第一注册请求消息中携带第二注册请求消息，使得第一 AMF 可以将该第二注册请求消息转发给第二 AMF，则第二 AMF 可以校验该第二注册请求消息的完整性，第二 AMF 校验第二注册请求消息的完整性成功之后，可以将上述用户设备的安全上下文返回给第一

10 AMF，能够提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

结合第四方面，在第四方面的某些实现方式中，所述用户设备的安全上下文包括：所述第一安全上下文，或者，基于所述第一安全上下文进行密钥推演生成的第二安全上下文。

本申请实施例提供的获取安全上下文的方法，上述用户设备的安全上下文可以是用户设备与第二 AMF 之间的本地安全上下文，或者，当第二 AMF 进行密钥推演之后生成了新的密钥的情况下，上述用户设备的安全上下文还可以是基于所述第一安全上下文进行密钥推演生成的第二安全上下文。

15

结合第四方面，在第四方面的某些实现方式中，所述第一 AMF 向所述第二 AMF 发送所述第二注册请求消息，包括：所述第一 AMF 向所述第二 AMF 发送用户设备上下文传输服务调用请求，所述用户设备上下文传输服务调用请求中携带所述第二注册请求消息。

20

本申请实施例提供的获取安全上下文的方法，第一 AMF 向第二 AMF 发送上述的第二注册请求消息可以在第一 AMF 向第二 AMF 发送用户设备上下文传输服务调用请求中携带第二注册请求消息。

结合第四方面，在第四方面的某些实现方式中，所述第一 AMF 接收所述第二 AMF 发送的所述用户设备的安全上下文，包括：所述第一 AMF 接收所述第二 AMF 发送的第一响应消息，所述第一响应消息中携带所述用户设备的安全上下文。

25

本申请实施例提供的获取安全上下文的方法，第二 AMF 向第一 AMF 返回上述的用户设备的安全上下文时，可以是向第一 AMF 发送第一响应消息，并在第一响应消息中携带上述用户设备的安全上下文。

结合第四方面，在第四方面的某些实现方式中，所述方法还包括：当所述第一 AMF 接收到所述第二 AMF 校验所述第二注册请求消息的完整性失败的消息时，所述第一 AMF 继续使用映射的安全上下文或向所述用户设备发起初始认证。

30

本申请实施例提供的获取安全上下文的方法，当第一 AMF 从第二 AMF 处获取用户设备的安全上下文失败的情况下，第一 AMF 可以继续使用与用户设备之间协商生成的映射的安全上下文，或者，第一 AMF 可以向用户设备发起初始认证生成第一 AMF 与用户设备之间安全上下文。

35

结合第四方面，在第四方面的某些实现方式中，所述映射的安全上下文是根据移动管理实体 MME 与所述用户设备之间的安全上下文获得的，其中，所述 MME 为所述 4G 通信系统中的网元。

本申请实施例提供的获取安全上下文的方法中涉及到的映射的安全上下文指的是用户设备和第一 AMF 分别基于用户设备与 MME 之间的安全上下文推导生成的安全上下文。

第五方面,提供了一种获取安全上下文的方法,包括:第一接入和移动管理功能 AMF 向第二 AMF 发送用户设备上下文传输服务调用请求,所述用户设备上下文传输服务调用请求用于获取用户设备的安全上下文,所述用户设备上下文传输服务调用请求中携带指示信息,所述指示信息用于指示所述用户设备为合法的用户设备,其中,所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后,为所述用户设备提供接入和移动管理服务的 AMF;所述第一 AMF 接收所述第二 AMF 发送的第二响应消息,所述第二响应消息中携带所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法,通过第一 AMF 在向第二 AMF 发送的用户设备上下文传输服务调用请求中携带指示 UE 为合法的 UE 指示信息,可以避免第二 AMF 对 UE 进行验证失败,导致第二 AMF 不向第一 AMF 发送 UE 的安全上下文,提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

结合第五方面,在第五方面的某些实现方式中,所述指示信息用于指示所述用户设备为合法的用户设备包括:所述指示信息用于指示注册请求消息完整性校验通过,其中,所述注册请求消息为所述第一 AMF 从所述用户设备处接收到的。

本申请实施例提供的获取安全上下文的方法,第一 AMF 向第二 AMF 发送的指示 UE 为合法的 UE 的指示信息可以是第一 AMF 通知第二 AMF 该 UE 发送的注册请求消息的完整性校验通过,为指示 UE 为合法 UE 提供灵活可选的方案。

结合第五方面,在第五方面的某些实现方式中,在所述第一 AMF 向第二 AMF 发送用户设备上下文传输服务调用请求之前,所述方法还包括:所述第一 AMF 成功校验注册请求消息的完整性保护,其中,所述注册请求消息为所述第一 AMF 从所述用户设备处接收到的;和/或,所述第一 AMF 确定所述注册请求消息,为所述用户设备从 4G 通信系统切换至 5G 通信系统后发送的注册请求消息。

本申请实施例提供的获取安全上下文的方法,第一 AMF 基于注册请求消息的成功校验的结果,和/或,接收到的注册请求消息,为所述用户设备从 4G 通信系统切换至 5G 通信系统后发送的注册请求消息,判断可以向第二 AMF 发送的用户设备上下文传输服务调用请求。

结合第五方面,在第五方面的某些实现方式中,所述用户设备上下文传输服务调用请求中携带所述用户设备的标识。

本申请实施例提供的获取安全上下文的方法,第一 AMF 为了使得第二 AMF 获知第一 AMF 需要获取的是某个用户设备的用户设备的安全上下文,在该上下文传输服务调用请求中携带该用户设备的标识。

结合第五方面,在第五方面的某些实现方式中,所述用户设备上下文传输服务调用请求中携带所述用户设备的上行非接入层计数器 UL NAS COUNT。

本申请实施例提供的获取安全上下文的方法,第一 AMF 为了使得第二 AMF 获知 UL NAS COUNT,可以在该上下文传输服务调用请求中携带该 UL NAS COUNT。

结合第五方面,在第五方面的某些实现方式中,所述用户设备上下文传输服务调用请求中携带所述 UL NAS COUNT 包括:所述用户设备上下文传输服务调用请求中携带明文

的注册请求消息，所述明文的注册请求消息中包括所述 UL NAS COUNT，其中，所述注册请求消息为所述第一 AMF 从所述用户设备处接收到的。

本申请实施例提供的获取安全上下文的方法，用户设备上下文传输服务调用请求中携带 UL NAS COUNT 可以是通过在用户设备上下文传输服务调用请求中携带明文的注册请求消息，该明文的注册请求消息中包括该 UL NAS COUNT，为第一 AMF 向第二 AMF 发送 UL NAS COUNT 提供灵活可选的方案。

第六方面，提供了一种获取安全上下文的方法，包括：第二接入和移动管理功能 AMF 接收第一 AMF 发送的用户设备上下文传输服务调用请求，所述用户设备上下文传输服务调用请求用于获取用户设备的安全上下文，所述用户设备上下文传输服务调用请求中携带指示信息，所述指示信息用于指示所述用户设备为合法的用户设备，其中，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；所述第二 AMF 向所述第一 AMF 发送第二响应消息，所述第二响应消息中携带所述用户设备的安全上下文。

本申请实施例提供的获取安全上下文的方法，通过在第二 AMF 接收到第一 AMF 发送的用户设备上下文传输服务调用请求中携带指示 UE 为合法的 UE 指示信息，第二 AMF 基于该指示信息无需对 UE 进行验证，可以避免第二 AMF 验证 UE 失败而不向第一 AMF 发送 UE 的安全上下文，提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

结合第六方面，在第六方面的某些实现方式中，所述指示信息用于指示所述用户设备为合法的用户设备包括：所述指示信息用于指示注册请求消息完整性校验通过，其中，所述注册请求消息为所述第一 AMF 从所述用户设备处接收到的。

本申请实施例提供的获取安全上下文的方法，第二 AMF 接收到的第一 AMF 发送的指示 UE 为合法的 UE 的指示信息可以是第一 AMF 通知第二 AMF 该 UE 发送的注册请求消息的完整性校验通过，为指示 UE 为合法 UE 提供灵活可选的方案。

结合第六方面，在第六方面的某些实现方式中，所述用户设备上下文传输服务调用请求中携带所述用户设备的标识。

本申请实施例提供的获取安全上下文的方法，第二 AMF 可以基于该上下文传输服务调用请求中携带该用户设备的标识，确定第一 AMF 需要获取的是该用户设备的用户设备的安全上下文。

结合第六方面，在第六方面的某些实现方式中，所述用户设备上下文传输服务调用请求中携带所述用户设备的上行非接入层计数器 UL NAS COUNT。

本申请实施例提供的获取安全上下文的方法，第二 AMF 可以基于该上下文传输服务调用请求中携带的 UL NAS COUNT，获知 UL NAS COUNT。

结合第六方面，在第六方面的某些实现方式中，所述用户设备上下文传输服务调用请求中携带所述 UL NAS COUNT 包括：所述用户设备上下文传输服务调用请求中携带明文的注册请求消息，所述明文的注册请求消息中包括所述 UL NAS COUNT，其中，所述注册请求消息为所述第一 AMF 从所述用户设备处接收到的。

本申请实施例提供的获取安全上下文的方法，用户设备上下文传输服务调用请求中携带 UL NAS COUNT 可以是通过在用户设备上下文传输服务调用请求中携带明文的注册请

求消息，该明文的注册请求消息中包括该 UL NAS COUNT，为第一 AMF 向第二 AMF 发送 UL NAS COUNT 提供灵活可选的方案。

结合第六方面，在第六方面的某些实现方式中，所述方法还包括：所述第二 AMF 基于所述 UL NAS COUNT 进行密钥推演。

- 5       本申请实施例提供的获取安全上下文的方法，第二 AMF 可以基于接收到的 UL NAS COUNT 进行密钥推演。

第七方面，提供了一种通信系统，该通信系统包括上述的第一 AMF 和第二 AMF 可以用来用于执行第一方面以及第一方面的任意可能的实现方式中的第一 AMF 和第二 AMF 的操作。具体地，该通信系统可以包括用于执行上述第一方面以及第一方面的任意可能的实现方式中所描述的步骤或功能相对应的部件 (means) 可以是第一方面的第一 AMF 和第二 AMF 或第一 AMF 和第二 AMF 内部的芯片或功能模块。步骤或功能可以通过软件实现，或硬件实现，或者通过硬件和软件结合来实现。

第八方面，提供了一种获取安全上下文的装置，该装置可以用来用于执行第五方面和第四方面以及第五方面和第四方面的任意可能的实现方式中的第一 AMF 的操作。具体地，该获取安全上下文的装置可以包括用于执行上述第五方面和第四方面以及第一方面和第四方面的任意可能的实现方式中所描述的步骤或功能相对应的部件 (means) 可以是第五方面和第四方面的第一 AMF 或第一 AMF 内部的芯片或功能模块。步骤或功能可以通过软件实现，或硬件实现，或者通过硬件和软件结合来实现。

第九方面，提供了一种获取安全上下文的装置，该装置可以用来用于执行第二方面和第六方面以及第二方面和第六方面的任意可能的实现方式中的第二 AMF 的操作。具体地，该获取安全上下文的装置可以包括用于执行上述第二方面和第六方面以及第二方面和第六方面的任意可能的实现方式中所描述的步骤或功能相对应的部件 (means) 可以是第二方面和第六方面的第二 AMF 或第二 AMF 内部的芯片或功能模块。步骤或功能可以通过软件实现，或硬件实现，或者通过硬件和软件结合来实现。

第十方面，提供了一种获取安全上下文的装置，该装置可以用来用于执行第三方面中的用户设备的操作。具体地，该获取安全上下文的装置可以包括用于执行上述第三方面中所描述的步骤或功能相对应的部件 (means) 可以是第三方面中的用户设备或用户设备内部的芯片或功能模块。步骤或功能可以通过软件实现，或硬件实现，或者通过硬件和软件结合来实现。

第十一方面，提供了一种通信设备，包括，处理器，收发器，存储器，该存储器用于存储计算机程序，该收发器，用于执行第一至第五方面中任一种可能实现方式中的获取安全上下文的装置方法中的收发步骤，该处理器用于从存储器中调用并运行该计算机程序，使得该通信设备执行第一至第六方面中任一种可能实现方式中的获取安全上下文的装置方法。

35       可选地，处理器为一个或多个，存储器为一个或多个。

可选地，存储器可以与处理器集成在一起，或者存储器与处理器分离设置。

可选的，收发器包括，发射机 (发射器) 和接收机 (接收器)。

第十二方面，提供了一种系统，系统包括第八方面和第九方面提供的获取安全上下文的装置。

第十三方面，提供了一种计算机程序产品，计算机程序产品包括：计算机程序（也可以称为代码，或指令），当计算机程序被运行时，使得计算机执行上述第一至第六方面中任一种可能实现方式中的方法。

第十四方面，提供了一种计算机可读介质，计算机可读介质存储有计算机程序（也可以称为代码，或指令）当其在计算机上运行时，使得计算机执行上述第一至第六方面中任一种可能实现方式中的方法。

第十五方面，提供了一种芯片系统，包括存储器和处理器，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得安装有该芯片系统的通信设备执行上述第一至第六方面中任一种可能实现方式中的方法。

10

#### 附图说明

图 1 是适用于本申请实施例的网络架构。

图 2 是一种通信系统切换的示意性流程图。

图 3 是本申请实施例提供的一种获取安全上下文的方法示意图。

15 图 4 是本申请实施例提供的另一种获取安全上下文的方法示意图。

图 5 为本申请实施例提供的获取安全上下文的装置 50 的示意图。

图 6 是适用于本申请实施例的用户设备 60 的结构示意图。

图 7 为本申请实施例提供的获取安全上下文的装置 70 的示意图。

图 8 是适用于本申请实施例的第一 AMF 80 的结构示意图。

20 图 9 为本申请实施例提供的获取安全上下文的装置 90 的示意图。

图 10 是适用于本申请实施例的第二 AMF 100 的结构示意图。

#### 具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

25 本申请实施例的技术方案可以应用于各种通信系统，例如：全球移动通信（global system for mobile communications, GSM）系统、码分多址（code division multiple access, CDMA）系统、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、未来的第五代（5th generation, 5G）系统或新无线（new radio, NR）等。

30 图 1 是适用于本申请实施例的网络架构。如图 1 所示，下面对该网络架构中涉及各个部分分别进行说明。

35 1、用户设备（user equipment, UE）110：可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备，以及各种形式的终端，移动台（mobile station, MS），终端（terminal），软终端等等。例如，水表、电表、传感器等。

2、（无线）接入网络（radio access network, (R)AN）网元 120：用于为特定区域的

授权用户设备提供入网功能，并能够根据用户设备的级别，业务的需求等使用不同质量的传输隧道。

(R)AN 网元能够管理无线资源，为用户设备提供接入服务，进而完成控制信号和用户设备数据在用户设备和核心网之间的转发，(R)AN 网元也可以理解为传统网络中的基站。

- 5        3、用户面网元 130：用于分组路由和转发以及用户面数据的服务质量（quality of service, QoS）处理等。

在 5G 通信系统中，该用户面网元可以是用户面功能（user plane function, UPF）网元。在未来通信系统中，用户面网元仍可以是 UPF 网元，或者，还可以有其它的名称，本申请不做限定。

- 10       4、数据网络网元 140：用于提供传输数据的网络。

在 5G 通信系统中，该数据网络网元可以是数据网络（data network, DN）网元。在未来通信系统中，数据网络网元仍可以是 DN 网元，或者，还可以有其它的名称，本申请不做限定。

- 15       5、接入和移动管理网元 150：主要用于移动性管理和接入管理等，可以用于实现移动性管理实体（mobility management entity, MME）功能中除会话管理之外的其它功能，例如，合法监听以及接入授权/鉴权等功能。

在 5G 通信系统中，该接入和移动管理网元可以是接入和移动管理功能（access and mobility management function, AMF）。在未来通信系统中，接入和移动管理设备仍可以是 AMF，或者，还可以有其它的名称，本申请不做限定。

- 20       6、会话管理网元 160：主要用于会话管理、用户设备的网络互连协议（internet protocol, IP）地址分配和管理、选择可管理用户平面功能、策略控制和收费功能接口的终结点以及下行数据通知等。

在 5G 通信系统中，该会话管理网元可以是会话管理功能（session management function, SMF）网元。在未来通信系统中，会话管理网元仍可以是 SMF 网元，或者，还可以有其它的名称，本申请不做限定。

- 25       7、策略控制网元 170：用于指导网络行为的统一策略框架，为控制面功能网元（例如 AMF, SMF 网元等）提供策略规则信息等。

在 4G 通信系统中，该策略控制网元可以是策略和计费规则功能（policy and charging rules function, PCRF）网元。在 5G 通信系统中，该策略控制网元可以是策略控制功能（policy control function, PCF）网元。在未来通信系统中，策略控制网元仍可以是 PCF 网元，或者，还可以有其它的名称，本申请不做限定。

- 30       8、认证服务器 180：用于鉴权服务、产生密钥实现对用户设备的双向鉴权，支持统一的鉴权框架。

在 5G 通信系统中，该认证服务器可以是认证服务器功能（authentication server function, AUSF）网元。在未来通信系统中，认证服务器功能网元仍可以是 AUSF 网元，或者，还可以有其它的名称，本申请不做限定。

- 9、数据管理网元 190：用于处理用户设备标识，接入鉴权，注册以及移动性管理等。

在 5G 通信系统中，该数据管理网元可以是统一数据管理（unified data management, UDM）网元；在 4G 通信系统中，该数据管理网元可以是归属用户服务器（home subscriber

server, HSS) 网元在未来通信系统中, 统一数据管理仍可以是 UDM 网元, 或者, 还可以有其它的名称, 本申请不做限定。

10、应用网元 1100: 用于进行应用影响的数据路由, 接入网络开放功能网元, 与策略框架交互进行策略控制等。

- 5 在 5G 通信系统中, 该应用网元可以是应用功能 (application function, AF) 网元。在未来通信系统中, 应用网元仍可以是 AF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

11、网络存储网元: 用于维护网络中所有网络功能服务的实时信息。

- 10 在 5G 通信系统中, 该网络存储网元可以是网络注册功能 (network repository function, NRF) 网元。在未来通信系统中, 网络存储网元仍可以是 NRF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

- 可以理解的是, 上述网元或者功能既可以是硬件设备中的网络元件, 也可以是在专用硬件上运行软件功能, 或者是平台 (例如, 云平台) 上实例化的虚拟化功能。为方便说明, 本申请后续, 以接入和移动管理设备为 AMF, 数据管理网元为 UDM 网元, 会话管理网元为 SMF 网元, 用户面网元为 UPF 网元为例进行说明。

为方便说明, 本申请实施例中以装置为 AMF 实体、UDM 实体为例, 对用于会话建立的方法进行说明, 对于装置为 AMF 实体内的芯片、UDM 实体内的芯片的实现方法, 可参考装置分别为 AMF 实体、UDM 实体的具体说明, 不再重复介绍。

- 20 在图 1 所示的网络架构中, 用户设备通过 N1 接口与 AMF 连接, (R)AN 通过 N2 接口与 AMF 连接, (R)AN 通过 N3 接口与 UPF 连接。UPF 之间通过 N9 接口连接, UPF 通过 N6 接口 DN 互联。SMF 通过 N4 接口控制 UPF。AMF 通过 N11 接口与 SMF 接口。AMF 通过 N8 接口从 UDM 单元获取用户设备签约数据, SMF 通过 N10 接口从 UDM 单元获取用户设备签约数据。

- 25 应理解, 上述应用于本申请实施例的网络架构仅是一种举例说明, 适用本申请实施例的网络架构并不局限于此, 任何能够实现上述各个网元的功能的网络架构都适用于本申请实施例。

- 30 例如, 在某些网络架构中, AMF、SMF 网元、PCF 网元、BSF 网元以及 UDM 网元等网络功能网元实体都称为网络功能 (network function, NF) 网元; 或者, 在另一些网络架构中, AMF, SMF 网元, PCF 网元, BSF 网元, UDM 网元等网元的集合都可以称为控制面功能网元。

- 35 本申请实施例中的用户设备可以指接入终端、用户单元、用户站、移动站、移动台、中继站、远方站、远程终端、移动设备、用户终端 (user terminal)、终端设备 (terminal equipment)、终端 (terminal)、无线通信设备、用户代理或用户装置。用户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 网络中的用户设备或者未来演进的公用陆地移动通信网络 (public land mobile network, PLMN) 中的用户设备等, 本申请实施例对此并不限定。

本申请实施例中的网络设备可以是用于与用户设备通信的任意一种具有无线收发功

能的设备。该设备包括但不限于：演进型节点 B (evolved Node B, eNB)、无线网络控制器 (radio network controller, RNC)、节点 B (Node B, NB)、基站控制器 (base station controller, BSC)、基站收发台 (base transceiver station, BTS)、家庭基站 (home evolved NodeB, 或 home Node B, HNB)、基带单元 (baseBand unit, BBU)、无线保真 (wireless fidelity, WIFI) 系统中的接入点 (access point, AP)、无线中继节点、无线回传节点、传输点 (transmission point, TP) 或者发送接收点 (transmission and reception point, TRP) 等, 还可以为 5G, 如, NR, 系统中的 gNB, 或, 传输点 (TRP 或 TP), 5G 系统中的基站的一个或一组 (包括多个天线面板) 天线面板, 或者, 还可以为构成 gNB 或传输点的网络节点, 如基带单元 (BBU), 或, 分布式单元 (distributed unit, DU) 等。

10 在一些部署中, gNB 可以包括集中式单元 (centralized unit, CU) 和 DU。gNB 还可以包括有源天线单元 (active antenna unit, AAU)。CU 实现 gNB 的部分功能, DU 实现 gNB 的部分功能。比如, CU 负责处理非实时协议和服务, 实现无线资源控制 (radio resource control, RRC), 分组数据汇聚层协议 (packet data convergence protocol, PDCP) 层的功能。DU 负责处理物理层协议和实时服务, 实现无线链路控制 (radio link control, RLC) 15 层、媒体接入控制 (media access control, MAC) 层和物理 (physical, PHY) 层的功能。AAU 实现部分物理层处理功能、射频处理及有源天线的相关功能。由于 RRC 层的信息最终会变成 PHY 层的信息, 或者, 由 PHY 层的信息转变而来, 因而, 在这种架构下, 高层信令, 如 RRC 层信令, 也可以认为是由 DU 发送的, 或者, 由 DU+AAU 发送的。可以理解的是, 网络设备可以为包括 CU 节点、DU 节点、AAU 节点中一项或多项的设备。此外, 20 可以将 CU 划分为接入网 (radio access network, RAN) 中的网络设备, 也可以将 CU 划分为核心网 (core network, CN) 中的网络设备, 本申请对此不做限定。

在本申请实施例中, 用户设备或网络设备包括硬件层、运行在硬件层之上的操作系统层, 以及运行在操作系统层上的应用层。该硬件层包括中央处理器 (central processing unit, CPU)、内存管理单元 (memory management unit, MMU) 和内存 (也称为主存) 等硬件。25 该操作系统可以是任意一种或多种通过进程 (process) 实现业务处理的计算机操作系统, 例如, Linux 操作系统、Unix 操作系统、Android 操作系统、iOS 操作系统或 windows 操作系统等。该应用层包含浏览器、通讯录、文字处理软件、即时通信软件等应用。并且, 本申请实施例并未对本申请实施例提供的方法的执行主体的具体结构特别限定, 只要能够通过运行记录有本申请实施例的提供的方法的代码的程序, 以根据本申请实施例提供的方法 30 进行通信即可, 例如, 本申请实施例提供的方法的执行主体可以是用户设备或网络设备, 或者, 是用户设备或网络设备中能够调用程序并执行程序的功能模块。

另外, 本申请的各个方面或特征可以实现成方法、装置或使用标准编程和/或工程技术的制品。本申请中使用的术语“制品”涵盖可从任何计算机可读器件、载体或介质访问的计算机程序。例如, 计算机可读介质可以包括, 但不限于: 磁存储器件 (例如, 硬盘、软 35 盘或磁带等), 光盘 (例如, 压缩盘 (compact disc, CD)、数字通用盘 (digital versatile disc, DVD) 等), 智能卡和闪存器件 (例如, 可擦写可编程只读存储器 (erasable programmable read-only memory, EPROM)、卡、棒或钥匙驱动器等)。另外, 本文描述的各种存储介质可代表用于存储信息的一个或多个设备和/或其它机器可读介质。术语“机器可读存储介质”可包括但不限于, 无线信道和能够存储、包含和/或承载指令和/或数据的各种其它介质。

本申请实施例中主要涉及到图 1 所示的网络架构为 4G 网络架构时的移动性管理实体 MME 和图 1 所示的网络架构为 5G 网络架构时的接入和移动管理功能 AMF 以及 UE。其中，针对 AMF 本申请中涉及到第一 AMF 和第二 AMF。具体地，本申请中所涉及的第一 AMF 指的是发生用户设备从 4G 通信系统切换到 5G 通信系统的过程中，4G 通信系统中的 MME 为 UE 从 5G 通信系统中选择的为 UE 提供核心网服务的 AMF；本申请中所涉及的第二 AMF 指的是用户设备从 4G 通信系统切换到 5G 通信系统的过程中，5G 通信系统中除了第一 AMF 之外的保存有 UE 的安全上下文的 AMF。

应理解本申请中的“第一”、“第二”仅用于区分说明，而不应对本申请构成任何限定。例如，上述的第一 AMF 和第二 AMF 只是区分不同的 AMF。

10 为了便于理解本申请实施例提供的获取安全上下文的方法，下面结合图 2 简单介绍用户设备从 4G 通信系统切换到 5G 通信系统的过程，图 2 是一种通信系统切换的示意性流程图。包括 UE、MME、第一 AMF 和第二 AMF。

该通信系统切换包括以下步骤：

S210，MME 向第一 AMF 发送转发重分配请求（forward relocation request）消息。

15 具体地，4G 通信系统中的 MME 获知发生用户设备从 4G 通信系统到 5G 通信系统的切换，需要为 UE 在 5G 通信系统中选择第一 AMF 继续为 UE 提供接入和移动管理服务。UE 在 4G 通信系统中接入时，UE 和 MME 会得到一个相同的密钥  $K_{ASME}$ ，当发生 UE 从 4G 通信系统到 5G 通信系统切换时，MME 选择第一 AMF 并将该  $K_{ASME}$  和下一跳参数（next hop parameter，NH）发送给第一 AMF，即上述的转发重分配请求消息中携带有  $K_{ASME}$  和 NH 等参数。

20 本申请实施例中对于 MME 如何获知发生系统切换的并不限制，可以参考现有协议中对于 4G 通信系统切换到 5G 通信系统流程中的规定。例如，可以是 4G 通信系统中的基站向 MME 发送切换请求，使得 MME 获知用户设备需要从 4G 通信系统切换到 5G 通信系统。

25 另外，本申请实施例中对于 MME 如何选择到第一 AMF 也不限制，可以参考现有协议中的规定。例如，MME 中保存有运营商配置有至少一个 AMF，当 MME 获知用户设备需要从 4G 通信系统切换至 5G 通信系统时，MME 从该至少一个 AMF 中选择上述的第一 AMF。

S220，第一 AMF 确定映射的（mapped）安全上下文。

30 具体地，第一 AMF 根据接收到的重分配请求消息中携带的  $K_{ASME}$  和 NH 等参数，推导出映射的安全上下文，映射的安全上下文包括在 UE 的映射的上下文中。应理解，本申请中所涉及的映射的上下文指的是第一 AMF 和 UE 分别基于 4G 通信系统中 UE 和 MME 之间协商生成的上下文，推导得到的 UE 的安全上下文，对于如何基于 4G 上下文推导可以参考现有协议的规定，本申请对此过程并不限制，映射的安全上下文指的是第一 AMF 和 UE 分别根据 MME 与用户设备之间的安全上下文获得的。另外，本申请中所涉及的 4G 通信系统中 UE 和 MME 之间协商的上下文，包括 UE 和 MME 之间的安全上下文，为了区分也可以称之为 UE 的 4G 上下文；同理，本申请中所涉及的 UE 从 4G 通信系统切换至 5G 通信系统之前，UE 和第二 AMF 中保存的 UE 的安全上下文指的是 5G 通信系统中 UE 和第二 AMF 之间协商的上下文，包括 UE 和 AMF 之间的安全上下文，为了区分也可以称

之为 UE 的 5G 上下文。

其中，为了便于描述，下文中将第一 AMF 和 UE 分别根据 MME 与用户设备之间的安全上下文推导获得的安全上下文称为映射的安全上下文、将第二 AMF 和 UE 之间的安全上下文称为本地（native）安全上下文。

5 还应理解，本申请实施例中主要涉及的是第二 AMF 向第一 AMF 发送 UE 的安全上下文，而 UE 的安全上下文作为 UE 的上下文的一部分，可以随着 UE 的上下文的传递而传递，所以为了便于描述，本申请实施例中描述可以为发送 UE 的上下文，或者，本申请实施例中描述可以为发送 UE 的安全上下文，仅仅是描述上的简便，对本申请实施例的保护范围并不构成任何限定。

10 上述第一 AMF 根据接收到的重分配请求消息中携带的  $K_{ASME}$  和 NH 等参数，推导出 UE 的映射的安全上下文包括第一 AMF 基于  $K_{ASME}$  和 NH 推导密钥  $K_{AMF1}$ 。

例如，第一 AMF 接收到上述的  $K_{ASME}$  和 NH 之后，可以利用预设的推导公式，计算得到密钥  $K_{AMF1}$ ，推导公式包括： $K_{AMF1} = \text{HMAC-SHA-256}(\text{Key}, \text{FC} \parallel \text{P0} \parallel \text{L0})$ ，其中， $\text{FC} = 0x76$ 、 $\text{P0} = \text{NH value}$ 、 $\text{L0} = \text{length of NH value (i.e. } 0x00\ 0x20\text{)}$ 、 $\text{KEY} = K_{ASME}$ 。第一 AMF 15 基于该密钥  $K_{AMF1}$  以及与 UE 协商的安全算法计算得到完整性保护密钥  $K_{NASint1}$  和机密性保护密钥  $K_{NASenc1}$ ，其中， $K_{AMF1}$ 、 $K_{NASint1}$  和  $K_{NASenc1}$  包括在 UE 的安全上下文中，而  $K_{AMF1}$ 、 $K_{NASint1}$  和  $K_{NASenc1}$  是基于  $K_{ASME}$  和 NH 推导得到的， $K_{ASME}$  和 NH 为 UE 和 MME 之间的安全上下文，所以  $K_{AMF1}$ 、 $K_{NASint1}$  和  $K_{NASenc1}$  称为 UE 的映射的安全上下文。

S230，第一 AMF 向 MME 发送转发重分配响应（forward relocation response）消息。

20 具体地，第一 AMF 确定映射的安全上下文之后，向 MME 发送转发重分配响应消息，该转发重分配响应消息用于通知 MME 该第一 AMF 可以作为 UE 从 4G 通信系统切换至 5G 通信系统时，在 5G 通信系统中为 UE 提供接入和移动管理服务的 AMF。

S240，MME 向 UE 发送切换命令（handover command）消息。

MME 接收到第一 AMF 发送的转发重分配响应消息之后，获知第一 AMF 可以为 UE 25 提供接入和移动管理服务，则 MME 向 UE 发送切换命令消息，使得 UE 获知可以从 4G 通信系统切换至 5G 通信系统。

S250，UE 确定映射的安全上下文。

UE 接收到切换命令消息之后，对 UE 中保存的密钥  $K_{ASME}$  和 NH 基于预设的推导公式，计算得到密钥  $K_{AMF1}$ ，具体地推导过程如上述的 S220 所示，这里不再赘述。

30 则 S250 之后，UE 和第一 AMF 之间获得了相同的密钥  $K_{AMF1}$ ，该密钥  $K_{AMF1}$  可以用于后续的其他密钥的推导。

例如，UE 和第一 AMF 得到一个相同的密钥  $K_{AMF1}$ ，然后基于  $K_{AMF1}$ ，以及 UE 和第一 AMF 之间协商的非接入层（non-access stratum，NAS）完整性保护算法和机密性保护算法，UE 和第一 AMF 生成用于 NAS 消息（如注册请求消息）保护的完整性保护密钥 35  $K_{NASint1}$  和机密性保护密钥  $K_{NASenc1}$ 。具体地，计算  $K_{NASint1}$  和  $K_{NASenc1}$  如下所示：

$K_{NASint1} = \text{HMAC-SHA-256}(\text{KEY}, \text{S})$ ，其中， $\text{S} = \text{FC} \parallel \text{P0}_1 \parallel \text{L0}_1 \parallel \text{P1}_1 \parallel \text{L1}_1$ ， $\text{FC} = 0x69$ ， $\text{P0}_1 =$  算法类型（algorithm type distinguisher）、 $\text{L0}_1 =$  算法类型长度（length of algorithm type distinguisher）（i.e.  $0x00\ 0x01$ ）、 $\text{P1}_1 =$  算法标识（algorithm identity）、 $\text{L1}_1 =$  算法标识长度（length of algorithm identity）（i.e.  $0x00\ 0x01$ ）， $\text{KEY} = K_{AMF1}$ ；

$K_{NASenc1} = \text{HMAC-SHA-256}(\text{KEY}, S)$ , 其中,  $S = FC || P0 || L0 || P1 || L1$ ,  $FC = 0x69$ ,  $P0 =$  algorithm type distinguisher,  $L0 =$  length of algorithm type distinguisher (i.e.  $0x00\ 0x01$ ),  $P1 =$  algorithm identity,  $L1 =$  length of algorithm identity (i.e.  $0x00\ 0x01$ ),  $\text{KEY} = K_{AMF1}$ 。

其中, 计算  $K_{NASint1}$ 、 $K_{NASenc1}$  的算法类型以及算法标识不一样。

- 5       在切换完成之后, UE 会发起移动性注册, 即执行 S260, UE 向第一 AMF 发送注册请求 (registration request) 消息, 且 UE 会用基于上述生成的  $K_{AMF1}$  推导生成的映射的安全上下文对该注册请求消息进行安全保护, 其中, 安全保护包括加密保护和/或完整性保护。

- 应理解, UE 向核心网设备发送消息可以通过接入网设备转发的, 由于在本申请实施例中对于接入设备的功能并不限定, 接入网设备可以为 UE 为第一 AMF 之间转发消息, 10       为了简便本申请中之间描述为 UE 向第一 AMF 发送注册请求消息、MME 向 UE 发送消息, 其中, UE 发送的注册请求消息中还包括有映射的上下文中的全球唯一临时用户设备标识 (globally unique temporary user equipment identity, GUTI), 该 GUTI 用于接入网设备确定将该注册请求消息转发给第一 AMF, 由于该 GUTI 包括在映射的上下文中, 可以称该 GUTI 为映射的 GUTI。

- 15       可选地, 在 UE 向第一 AMF 发送注册请求消息的时候, UE 中保存有与其他的 AMF (第二 AMF) 之间的 UE 的安全上下文和用户设备的 5G 全球唯一临时用户设备标识 (5th generation globally unique temporary user equipment identity, 5G-GUTI), 则 UE 在上述的注册请求消息中携带该 5G-GUTI。

- 应理解, 本申请实施例中主要涉及第一 AMF 如何从第二 AMF 处成功获得 UE 的安全上下文的过 20       程, 因此, 本申请中主要考虑 UE 在 UE 向第一 AMF 发送注册请求消息的时候, UE 中保存有与第二 AMF 之间协商的 UE 的安全上下文和 5G-GUTI 的情况。

- 还应理解, 本申请实施例中对于 UE 和第二 AMF 之间保存有 UE 的安全上下文和 5G-GUTI 的原因并不限制, 可以是现有协议中规定的情况。例如, 可以是 UE 在从 4G 通信系统切换至 5G 通信系统之前, UE 是从 5G 网络通信系统中切换到了 4G 通信系统; 或者, 支持双连接的 UE 通过非 3GPP 接入 5G 通信系统, 同时通过 3GPP 接入 4G 通信系统, 25       发生 4G 通信系统到 5G 通信系统的连接态切换。

- 应理解, 在第二 AMF 上存在与 UE 之间 UE 的安全上下文的情况下, 第一 AMF 需要从第二 AMF 处获得该 UE 的安全上下文, 具体地, 第一 AMF 从第二 AMF 处获得 UE 的安全上下文, 是基于从 UE 处接收到的注册请求消息中携带的 5G-GUTI 确定的, 该 30       5G-GUTI 是第二 AMF 为 UE 配置, 可以用于标识 UE 和第二 AMF。协议规定 5G 通信系统中存在 UE 的安全上下文时, 优先使用该 UE 的安全上下文, 而不是使用第一 AMF 和 UE 之间协商确定的映射的安全上下文, 因为该映射的安全上下文是基于 4G 通信系统中 UE 和 MME 之间的 UE 的安全上下文映射得到的, 即图 2 所示的流程还包括 S270, 第一 AMF 发起用户设备上下文传输服务调用请求 (Namf\_Communication\_UEContextTransfer)。

- 35       具体地, 第一 AMF 接收到 UE 发送的注册请求消息, 并根据注册请求消息中携带的 5G-GUTI 向第二 AMF 发起用户设备上下文传输服务调用请求, 该用户设备上下文传输服务调用请求中携带上述的注册请求消息。

      应理解, 上述的注册请求消息是基于 UE 和第一 AMF 之间的映射的安全上下文进行安全保护的, 第二 AMF 根据对注册请求消息的校验结果, 决定是否向第一 AMF 返回 UE 的

安全上下文。即执行 S290，第二 AMF 校验注册请求消息。

一种可能的实现方式，第二 AMF 校验该注册请求消息失败，第二 AMF 不会将 UE 的安全上下文返回给第一 AMF，最终导致第一 AMF 从第二 AMF 处获取 UE 的安全上下文失败，则导致第一 AMF 无法优先利用 UE 的安全上下文，不符合协议的规定。

5 另一种可能的实现方式，第二 AMF 校验注册请求消息完整性成功，则第二 AMF 将 UE 的安全上下文传递给第一 AMF，执行 S291，第二 AMF 向第一 AMF 发送 UE 的安全上下文。可选地，可以描述为第二 AMF 向第一 AMF 发送 UE 的上下文，UE 的上下文包括第二 AMF 与 UE 之间协商确定的 UE 的安全上下文，该 UE 的安全上下文中包括密钥  $K_{AMF2}$  和非接入层计数（non-access stratum count，NAS COUNT）等。

10 可选的，第二 AMF 在传递 UE 的安全上下文之前，可能会根据本地策略对密钥  $K_{AMF2}$  进行密钥推演。若第二 AMF 对  $K_{AMF2}$  进行了密钥推演，则向第一 AMF 发送推演之后的密钥  $K_{AMF2}'$  的同时还会携带推演指示信息，用来指示第二 AMF 对  $K_{AMF2}$  进行了密钥推演。

作为一种可能的实现方式，本申请中所述的密钥推演可以为水平密钥推演；

15 例如， $K_{AMF2}$  经过水平密钥推演生成为  $K_{AMF2}'$  的方式为：

$K_{AMF2}' = \text{HMAC-SHA-256}(\text{Key}, S)$ ;

$FC = 0x72$ ;

$P0 = 0x01$ ;

$L0 = \text{length of } P0 \text{ (i.e. } 0x00 \ 0x01)$ ;

20  $P1 = \text{uplink NAS COUNT}$ ;

$L1 = \text{length of } P1 \text{ (i.e. } 0x00 \ 0x04)$ ;

$\text{KEY} = K_{AMF2}$ ;

$S = FC || P0 || L0 || P1 || L1$ 。

25 作为另一种可能的实现方式，本申请中所述的密钥推演可以为不同的网元之间约定的密钥推演方式。例如，第一 AMF 和第二 AMF 之间约定密钥推演方式为预设的密钥推演方式，只要第二 AMF 向第一 AMF 发送的 UE 的安全上下文中包括推演指示信息，第一 AMF 能够确定接收到的 UE 的安全上下文中的密钥是第二 AMF 通过预设的密钥推演方式进行密钥推演得到的。

30 同样地，第一 AMF 收到推演指示信息后，也会向 UE 发送推演指示信息，指示 UE 对密钥  $K_{AMF2}$  进行密钥推演得到密钥  $K_{AMF2}'$ ，使得 UE 和网络侧的密钥达成一致，应理解，UE 能够确定是对密钥  $K_{AMF2}$  进行密钥推演而不是对  $K_{AMF}$  进行密钥推演，因为 UE 接到到指示密钥  $K_{AMF2}$  的密钥标识符，因为本申请对密钥标识符并不涉及改进，这里不对密钥标识符进行详细说明。

35 由图 2 所示的用户设备从 4G 通信系统切换到 5G 通信系统的过程可知，在第二 AMF 校验 UE 失败的情况下，上述的第一 AMF 无法从上述的第二 AMF 中获得 UE 的安全上下文。为了避免上述的无法成功获取 UE 的安全上下文的情况发生，本申请实施例提供一种获取安全上下文的方法，通过第一 AMF 在从第二 AMF 处获得 UE 的安全上下文的时候，携带指示信息，该指示信息表示 UE 已经通过了校验，而第二 AMF 根据指示信息不需要对 UE 进行验证，直接返回 UE 的安全上下文即可，从而可以避免上述的获取 UE 的安全

上下文失败的可能。

应理解，本申请中涉及到的对 UE 进行验证，指的是对 UE 发送的注册请求消息进行完整性校验，例如，解密该注册请求消息和/或验证该注册请求消息的完整性。由于注册请求消息的完整性验证通过的前提是成功解密该注册请求消息，所以本申请中实施例中将

5 UE 通过验证描述为注册请求消息的完整性验证通过。

下面，结合图 3 详细介绍本申请实施例提供的获取安全上下文的方法。图 3 是本申请实施例提供的一种获取安全上下文的方法示意图。该示意图包括 UE、MME、第一 AMF 和第二 AMF。

该获取安全上下文的方法包括以下步骤：

10 S310，第一 AMF 向第二 AMF 发送第二请求消息。

该第二请求消息用于请求获取 UE 的安全上下文，该第二请求消息中携带指示信息，该指示信息用于指示 UE 为合法 UE。

可选地，指示信息可以称为原因值（value）。

具体地，第一 AMF 确定 UE 为合法的 UE 主要是判断从 UE 处接收到的注册请求消息

15 是否满足预设的条件，应理解，第一 AMF 向第二 AMF 发送第二请求消息之前，图 3 所示的方法流程还包括 S311-S316：

S311，MME 向第一 AMF 发送转发重分配请求消息，与图 2 中 S210 类似，这里不再赘述；

S312，第一 AMF 确定映射的安全上下文，与图 2 中 S220 类似，这里不再赘述；

20 S313，第一 AMF 向 MME 发送转发重分配响应消息，与图 2 中 S230 类似，这里不再赘述；

S314，MME 向 UE 发送切换命令消息，与图 2 中 S240 类似，这里不再赘述；

S315，UE 确定映射的安全上下文，与图 2 中 S250 类似，这里不再赘述；

S316，UE 向第一 AMF 发送注册请求消息，与图 2 中 S260 类似，这里不再赘述。

25 进一步地，第一 AMF 确定所述注册请求消息满足预设条件包括：

第一 AMF 成功校验注册请求消息的完整性保护；或者，

第一 AMF 确定注册请求消息，为 UE 从 4G 通信系统切换至 5G 通信系统后发送的注册请求消息。例如，第一 AMF 在接收到 UE 发送的注册请求消息之前，接收到 MME 发送的转发重分配请求消息，则第一 AMF 能够获知当前接收到的注册请求消息，是在切换

30 过程中从 UE 接收到的注册请求消息。

具体地，第一 AMF 成功校验注册请求消息的完整性保护也可以称之为第一 AMF 验证 UE 成功，即图 3 所示的方法流程还包括 S317，第一 AMF 验证 UE。

作为一种可能的实现方式，该第二请求消息为图 2 中所示的第一 AMF 发起用户设备上下文传输服务调用请求（Namf\_Communication\_UEContextTransfer），与图 2 中所示的用户设备上下文传输服务调用请求不同的是，本申请实施例中的用户设备上下文传输服务调用请求中新增信息元素（information element，IE）-指示信息。

35

作为另一种可能的实现方式，第二请求消息为第一 AMF 向第二 AMF 发送的用于获取 UE 的安全上下文的其他可能的第二请求消息。

应理解，本申请中对于第二请求消息的具体形式并不限制，可以是在第一 AMF 和第

二 AMF 之间已有的信令中, 新增上述的指示信息, 还可以是第一 AMF 和第二 AMF 之间新增的信令。

作为另一种可能的实现方式, 本申请实施例中只限定第一 AMF 需要在向第二 AMF 发送用户设备上下文传输服务调用请求之前, 将上述的指示信息发送给第二 AMF, 也就是说第一 AMF 可以直接向第二 AMF 发送指示信息, 无需将该指示信息携带在上述的第二请求消息中, 该可能的实现方式在图 3 中并未示出。

还应理解, 本申请中对于上述指示信息具体如何指示 UE 为合法 UE 并不限制。一种可能的实现方式, 指示信息可以是复用上述 UE 的 5G-GUTI, 则该 5G-GUTI 可以标识该 UE 还可以用于表示该 UE 为合法 UE, 在这种实现方式下, 对现有的 IE 增加了新的指示功能, 可以通过预定义的方式通知第二 AMF 该 5G-GUTI 具有新的功能; 另一种可能的实现方式, 指示信息可以是新增的至少一个比特位, 该比特位值设为 1, 表示 UE 为合法的 UE。上述的可能的实现方式仅仅是举例说明, 对本申请的保护范围不构成任何限定。

作为一种可能的实现方式, 上述的指示信息为显式地指示 UE 为合法的 UE; 或者, 作为另一种可能的实现方式, 上述的指示信息为隐式地指示 UE 为合法的 UE, 例如, 指示信息指示第一 AMF 从 UE 处接收到的注册请求消息完整性校验通过。

进一步地, 为了使得第二 AMF 确定第一 AMF 是需要获得 UE 的安全上下文, 上述第二请求消息中还需要携带 UE 的标识。

作为一种可能的实现方式, UE 的标识可以是上述的 5G-GUTI;

作为另一种可能的实现方式, UE 的标识可以是用户永久标识 (subscriber permanent identity, SUPI)。

应理解, 第一 AMF 从 UE 处接收到 UE 的 5G-GUTI 之后, 确定需要从第二 AMF 处获得 UE 的安全上下文, 则可以选择继续在第二请求消息中携带 UE 的 5G-GUTI, 或者, 携带 UE 的 SUPI, 或者, 携带 UE 的 5G-GUTI 和 UE 的 SUPI。

可选地, 为了使得第二 AMF 能够获得 UE 的上行非接入层计数器 (uplink non-access stratum count, UL NAS COUNT), 一种可能的实现方式是上述第二请求消息中携带明文的注册请求消息, 该明文的注册请求消息中包括 UL NAS COUNT; 或者, 一种可能的实现方式是上述第二请求消息中携带 UL NAS COUNT。

进一步地, 第二 AMF 接收到第一 AMF 发送的第二请求消息之后, 第二 AMF 基于指示信息获知 UE 为合法的 UE, 第二 AMF 无需进行 UE 验证, 即执行 S320, 第二 AMF 确定无需进行验证。

S330, 第二 AMF 向第一 AMF 发送第二响应消息。

该第二响应消息中携带 UE 的安全上下文。

本申请实施例中第二 AMF 无需对 UE 进行验证, 接收到第一 AMF 发送的第二请求消息之后, 直接将 UE 的安全上下文返回给第一 AMF, 则不存在由于第二 AMF 验证 UE 失败而导致的第一 AMF 获取 UE 的安全上下文失败。

可选地, 当第二请求消息中携带明文的注册请求消息, 或者, 第二请求消息中携带 UL NAS COUNT 的情况下, 第二 AMF 能够获得 UL NAS COUNT。例如, 由于明文的注册请求消息为未安全保护的注册请求消息, 第二 AMF 无需验证该明文的注册请求消息, 可以直接从明文的注册请求消息中获得 UL NAS COUNT。

进一步地, 第二 AMF 能够根据该 UL NAS COUNT 对 UE 的安全上下文中的第一密钥进行密钥推演, 在此情况下, 第二 AMF 返回给第一 AMF 的 UE 的安全上下文中的密钥为第一密钥进行密钥推演得到的第二密钥。

具体地, 第二 AMF 发送给第一 AMF 的 UE 的安全上下文中的密钥为上述的第二密钥  
5 时, 第二 AMF 还需要向第一 AMF 发送密钥推演指示信息, 用于指示第二密钥为进行密钥推演得到的密钥。

应理解, 第一 AMF 获得 UE 的安全上下文之后的流程与现有中的 UE 从 4G 通信系统切换至 5G 通信系统流程中第一 AMF 获得 UE 的安全上下文之后的流程类似, 参考现有流程即可, 这里不再赘述。

10 图 3 所示的获取安全上下文的方法, 主要是在第一 AMF 向第二 AMF 发送的第二请求消息中携带指示信息, 该指示信息用于指示 UE 为合法 UE。从而第二 AMF 可以基于该指示信息判断 UE 为合法的 UE, 第二 AMF 无需验证 UE, 第二 AMF 在接收到携带指示信息的第二请求消息之后, 直接将 UE 的安全上下文返回给第一 AMF, 从而避免了第二 AMF 验证 UE 失败导致第一 AMF 获取 UE 的安全上下文失败。本申请还提供另外一种获取安全上下文的方法, 第二 AMF 验证 UE, 但是该方法能够提高第二 AMF 验证 UE 成功的可能性, 从而提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。  
15

下面, 结合图 4 详细介绍该获取安全上下文的方法。图 4 是本申请实施例提供的另一种获取安全上下文的方法示意图。该示意图包括 UE、MME、第一 AMF 和第二 AMF。

该获取安全上下文的方法包括以下步骤:

20 S410, UE 确定第一注册请求消息。

该第一注册请求消息中携带第二注册请求消息, 其中, 所述第二注册请求消息被第一安全上下文进行过完整性保护, 所述第一安全上下文为所述 UE 与第二 AMF 之间的本地 (native) 安全上下文。

具体地, UE 确定第一注册请求消息主要涉及 UE 确定第二注册请求消息, 该第二注册请求消息为 UE 对第四注册请求消息用 native 安全上下文完整性保护之后的消息, 该第四注册请求消息中包括 UE 与第二 AMF 之间的 UE 的上下文中的 GUTI、密钥标识符 (ngKSI) 信息、UL NAS COUNT, 为了便于区分该 GUTI 可以称之为本地 GUTI、该密钥标识符可以称之为本地密钥标识符。  
25

可选地, 第四注册请求消息可以为以下几种可能的情况:

30 情况一:

第四注册请求消息为 UE 基于上述的本地 GUTI、本地密钥标识符和 UL NAS COUNT 生成的一个消息, 在该情况一下第四注册请求消息还可以称之为第四消息或其他可能的名称, 本申请实施例中对于消息的名称并不做限定。

应理解, UE 基于 UE 与第二 AMF 之间的 UE 的上下文生成第四注册请求消息还可以是其他的形式, 例如, UE 生成的第四注册请求消息中除了包括上述的本地 GUTI、本地密钥标识符和 UL NAS COUNT 还包括其他的信息元素 (information element, IE)。  
35

在情况一下, UE 基于第一安全上下文对第四注册请求消息进行完整性保护包括: UE 基于所述第一安全上下文对该第四注册请求消息进行完整性保护, 生成第一 MAC。因此, 在第一注册请求消息中携带第二注册请求消息也可以理解为: 在第一注册请求消息中携带

第一 MAC 以及所述第四注册请求消息。

进一步地，在情况一下，UE 确定第一注册请求消息包括以下步骤：

步骤一：

UE 构造的第四注册请求消息；

5 步骤二：

UE 基于所述 UE 与第二 AMF 之间的安全上下文对第四注册请求消息进行完整性保护，生成第一 MAC；

步骤三：

10 UE 基于所述 UE 与第一 AMF 之间的映射的安全上下文对第三注册请求消息和第二注册请求消息 (RR2)，进行完整性保护，生成第五 MAC，其中，第三注册请求消息为图 2 所示的方法流程 S260 中 UE 向第一 AMF 发送的注册请求消息，具体地，该第三注册请求消息中包括 UE 与第一 AMF 之间的映射的上下文中的 GUTI、密钥标识符信息，为了便于区分该 GUTI 可以称之为映射的 GUTI、该密钥标识符可以称之为映射的密钥标识符。

15 则在该情况下，第一注册请求消息中包括第四注册请求消息 (RR4)、第三注册请求消息 (RR3)，第五 MAC (MAC5) 和第一 MAC (MAC1)，其中，MAC1 为对 RR4 用本地安全上下文进行完整性保护得到的 MAC 值，MAC5 为对 RR3 和 RR2 用映射的安全上下文进行完保得到的 MAC 值 (或者，MAC5 为对 RR3、RR4 和 MAC1 用映射的安全上下文进行完保得到的 MAC 值)；也可以理解为第一注册请求消息为依次基于 native 安全上下文和映射的安全上下文进行完整性保护的消息。

20 情况二：

第四注册请求消息为 UE 基于映射的安全上下文对第三注册请求消息进行完整性保护之后的注册请求消息。

25 在情况二下，UE 基于第一安全上下文对第四注册请求消息进行完整性保护包括：UE 基于所述第一安全上下文对该第四注册请求消息进行完整性保护，生成第一 MAC。因此，在第一注册请求消息中携带第二注册请求消息也可以理解为：在第一注册请求消息中携带第一 MAC 和所述第四注册请求消息。

进一步地，在情况二下，UE 确定第一注册请求消息包括以下步骤：

步骤一：

30 UE 基于 UE 与第一 AMF 之间的映射的安全上下文对第三注册请求消息进行完整性保护，生成第三 MAC；

步骤二：

UE 基于所述 UE 与第二 AMF 之间的 native 安全上下文，对步骤一中的基于映射的安全上下文进行完整性保护之后的第三注册请求消息，再次进行完整性保护，生成第一 MAC；

35 则在该情况下，第一注册请求消息中包括第三注册请求消息 (RR3)、第三 MAC (MAC3) 和第一 MAC (MAC1)，其中，MAC3 为对 RR3 用映射的安全上下文进行完整性保护得到的 MAC 值，MAC1 为对 RR3 和 MAC3 用本地安全上下文进行完整性保护得到的 MAC 值；也可以理解为第一注册请求消息为依次基于映射的安全上下文和 native 安全上下文完整性保护的消息。

情况三:

第四注册请求消息为: 第三注册请求消息, 其中, 第三注册请求消息为图 2 所示的方法流程 S260 中 UE 向第一 AMF 发送的注册请求消息。

在情况二下, UE 基于第一安全上下文对第四注册请求消息进行完整性保护包括: UE 基于所述第一安全上下文对该第四注册请求消息进行完整性保护, 生成第一 MAC。因此, 在第一注册请求消息中携带第二注册请求消息也可以理解为: 在第一注册请求消息中携带第一 MAC 和所述第四注册请求消息。

进一步地, 在情况三下, UE 确定第一注册请求消息包括以下步骤:

步骤一:

10 UE 基于 UE 与第二 AMF 之间的 native 安全上下文对第三注册请求消息进行完整性保护, 生成第一 MAC;

步骤二:

15 UE 基于所述 UE 与第一 AMF 之间的映射的安全上下文, 对步骤一中的基于 native 安全上下文进行完整性保护之后的第三注册请求消息, 再次进行完整性保护, 生成第四 MAC;

20 则在该情况下, 第一注册请求消息中包括第三注册请求消息 (RR3)、第一 MAC (MAC1) 和第四 MAC (MAC4) 其中, MAC1 为对 RR3 用本地安全上下文进行完整性保护得到的 MAC 值, MAC4 为对 RR3 和 MAC1 用映射的安全上下文进行完整性保护得到的 MAC 值; 也可以理解为第一注册请求消息为依次基于 native 安全上下文和映射的安全上下文完整性保护的消息。

应理解, 在情况一下, 第一 AMF 能够根据 UE 发送的第一注册请求消息中同时携带映射的 GUTI 和本地 GUTI 确定将经由 native 安全上下文完整性保护的第三注册请求消息发送给第二 AMF。

25 还应理解, 上述的情况一-情况三只是以举例的形式说明第二注册请求消息可能的情况, 以及 UE 如何确定上述的第一注册请求消息, 其他未列举出的第二注册请求可能的形式也在本申请的保护范围之内, 例如, 上述第四注册请求消息为 UE 基于 native 上下文构成其他的可能的消息。

S420, UE 向第一 AMF 发送第一注册请求消息。

具体地, UE 将 S410 中确定的第一注册请求消息发送给第一 AMF。

30 应理解, UE 向第一 AMF 发送第一注册请求消息可以经由接入网设备的转发, 本申请中对接入网设备的功能并不限定, 因此可以直接描述为 UE 向第一 AMF 发送第一注册请求消息。

35 还应理解, UE 在向第一 AMF 发送第一注册请求消息之前, UE 需要确定映射的安全上下文, 则 UE 向第一 AMF 发送第一注册请求消息之前, 图 4 所示的方法流程还包括 S411-S414:

S411, MME 向第一 AMF 发送转发重分配请求消息, 与图 2 中 S210 类似, 这里不再赘述;

S412, 第一 AMF 确定映射的安全上下文, 与图 2 中 S220 类似, 这里不再赘述;

S413, 第一 AMF 向 MME 发送转发重分配响应消息, 与图 2 中 S230 类似, 这里不再

赘述;

S414, MME 向 UE 发送切换命令消息, 与图 2 中 S240 类似, 这里不再赘述;

具体地, UE 收到切换命令消息后, 推导出映射的安全上下文。进而, UE 利用 native 安全上下文和 mapped 安全上下文对上述的第一注册请求消息进行安全保护。

5 S430, 第一 AMF 验证 UE。

具体地, 第一 AMF 确定 UE 为合法的 UE 主要是判断从 UE 处接收到的第一注册请求消息是否满足预设的条件。第一 AMF 确定所述第一注册请求消息满足预设条件包括:

第一 AMF 基于映射的安全上下文成功校验第一注册请求消息的完整性保护; 或者,

10 第一 AMF 确定第一注册请求消息, 为 UE 从 4G 通信系统切换至 5G 通信系统后发送的注册请求消息。例如, 第一 AMF 在接收到 UE 发送的第一注册请求消息之前, 接收到 MME 发送的转发重分配请求消息, 则第一 AMF 能够获知当前接收到的第一注册请求消息, 是在切换过程中从 UE 接收到的注册请求消息。

第一 AMF 验证 UE 为合法的 UE 之后, 第一 AMF 向第二 AMF 发送第二注册请求消息, 该第二注册请求消息用于第二 AMF 验证 UE。即图 4 所示的方法流程还包括 S440,  
15 第一 AMF 向第二 AMF 发送第二注册请求消息。

可选地, 第二注册请求消息携带在第一请求消息中, 由第一 AMF 发送给第二 AMF。

作为一种可能的实现方式, 该第一请求消息为图 2 中所示的第一 AMF 发起用户设备上下文传输服务调用请求 (Namf\_Communication\_UEContextTransfer), 与图 2 中所示的用户设备上下文传输服务调用请求不同的是, 本申请实施例中的用户设备上下文传输服务调用请求中新增信元-第一 MAC。  
20

作为另一种可能的实现方式, 第一请求消息为第一 AMF 向第二 AMF 发送的用于获取 UE 的安全上下文的其他可能的第一请求消息。

应理解, 本申请中对于第一请求消息的具体形式并不限制, 可以是在第一 AMF 和第二 AMF 之间已有的信令中, 新增上述的第一 MAC, 还可以是第一 AMF 和第二 AMF 之间新增的信令。  
25

进一步地, 为了使得第二 AMF 确定第一 AMF 是需要获得 UE 的安全上下文, 上述第一请求消息中还携带有 UE 的标识。具体地, 该 UE 的标识包括在上述第一 AMF 向第二 AMF 发送的第二注册请求消息中。

作为一种可能的实现方式, UE 的标识可以是上述的映射的 GUTI;

30 作为一种可能的实现方式, UE 的标识可以是上述的本地 GUTI;

作为另一种可能的实现方式, UE 的标识可以是 SUPI。

应理解, 第一 AMF 从 UE 处接收到 UE 的映射的 GUTI 之后, 确定需要从第二 AMF 处获得 UE 的安全上下文, 则可以选择继续在第一请求消息中携带 UE 的映射的 GUTI, 或者, 携带 UE 的 SUPI, 或者, 携带 UE 的映射的 GUTI 和 UE 的 SUPI。

35 还应理解, 当第一 AMF 接收到的第一注册请求消息为 S410 中情况一所示的情况下, 则第一注册请求消息中携带有第二注册请求消息, 而第二注册请求消息中包括有本地 GUTI, 那么在该情况下, 第一 AMF 可以选择在第一请求消息中携带 UE 的本地 GUTI。

进一步地, 上述的第二注册请求消息中还包括 UE 的 UL NAS COUNT, 使得第二 AMF 能够获得 UE 的 UL NAS COUNT。

进一步地,第二 AMF 接收到第一 AMF 发送的第一请求消息之后,第二 AMF 基于第二注册请求消息的完整性校验结果判断 UE 是否为合法的 UE,即执行 S450,第二 AMF 校验第二注册请求消息的完整性。

5 所述第二 AMF 根据所述第二 AMF 与所述用户设备之间的安全上下文对所述第二注册请求消息进行完整性校验。例如,第二 AMF 基于本地保存的安全上下文生成第二 MAC,对比第一 MAC 和第二 MAC,当第一 MAC 和第二 MAC 相等的情况下,第二 AMF 验证 UE 成功,确定 UE 合法的 UE,则第二 AMF 向第一 AMF 发送 UE 的安全上下文。

10 应理解,上述的第一 MAC 为 UE 基于 UE 和第二 AMF 之间协商的 UE 的安全上下文生成的 MAC、第二 MAC 为第二 AMF 基于 UE 和第二 AMF 之间协商的 UE 的安全上下文生成的 MAC,所以大概率下第一 MAC 和第二 MAC 是相等的第二 AMF 能够验证 UE 成功,向第一 AMF 返回 UE 的安全上下文,除非发生传输错误的小概率事件发生,而导致第二 AMF 验证失败。图 4 所示的获取安全上下文的方法与图 2 中所示的方法流程相比提高第一 AMF 成功从第二 AMF 处获取用户设备的安全上下文的可能性。

15 在第二 AMF 校验第二注册请求消息的完整性成功之后,执行 S460,第二 AMF 向第一 AMF 发送 UE 的安全上下文。

可选地,该 UE 的安全上下文携带在第一响应消息中。

进一步地,该 UE 的安全上下文包括在 UE 的上下文中,则第二 AMF 可以向第一 AMF 发送 UE 的上下文。

20 可选地,第二 AMF 能够根据 UL NAS COUNT 对 UE 的安全上下文中的第一密钥进行密钥推演,在此情况下,第二 AMF 返回给第一 AMF 的 UE 的安全上下文中的密钥为第一密钥进行密钥推演得到的第二密钥。其中,本申请实施例中可以将包括该进行密钥推演生成的第二密钥的 UE 的安全上下文称为第二安全上下文,也就是说第二 AMF 向第一 AMF 发送 UE 的安全上下文可以是未经过密钥推演的,第二 AMF 中本地保存的第二 AMF 和 UE 之间的 UE 的安全上下文,或者,当第二 AMF 根据本地策略对本地保存的第二 AMF 和 UE 之间的 UE 的安全上下文中的密钥,进行过密钥推演生成了推演后的密钥的情况下,25 第二 AMF 向第一 AMF 发送 UE 的安全上下文可以是上述的第二安全上下文。

具体地,第二 AMF 发送给第一 AMF 的 UE 的安全上下文中的密钥为上述的第二密钥时,第二 AMF 还需要向第一 AMF 发送密钥推演指示信息,用于指示第二密钥为进行密钥推演得到的密钥。

30 应理解,第一 AMF 获得 UE 的安全上下文之后的流程与现有中的 UE 从 4G 通信系统切换至 5G 通信系统流程中第一 AMF 获得 UE 的安全上下文之后的流程类似,参考现有流程即可,这里不再赘述。

例如,后续 UE 和第一 AMF 之间协商使用上述的 native 安全上下文,具体地,第一 AMF 向 UE 发送非接入层安全模式命令(non-access layer secure mode command, NAS SMC)消息,UE 对 NAS SMC 消息进行完整性校验,当 UE 校验 NAS SMC 成功之后,35 UE 向第一 AMF 发送非接入层安全模式完成(non-access layer security mode complete)消息。

作为一种可能的实现方式,当第二 AMF 校验第二注册请求消息的完整性失败的情况下,第二 AMF 向第一 AMF 发送失败指示信息,用于通知第一 AMF,该第二 AMF 校验

第二注册请求消息的完整性失败。

进一步地，第一 AMF 在接收到指示第二 AMF 校验第二注册请求消息的完整性失败的失败指示信息之后，第一 AMF 基于本地策略确定第一 AMF 可以继续使用上述映射的安全上下文，或者，第一 AMF 基于本地策略确定向 UE 发起初始认证，生成新的第一 AMF 和 UE 之间的安全上下文。

应理解，上述方法实施例中，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。

上面结合图 3 和图 4 详细介绍了本申请实施例提供的获取安全上下文的方法，下面结合图 5-图 10 详细介绍本申请实施例提供的获取安全上下文的装置。

参见图 5，图 5 是本申请提出的获取安全上下文的装置 50 的示意图。如图 5 所示，装置 50 包括发送单元 510、处理单元 520 和接收单元 530。

发送单元 510，用于向第一 AMF 发送第一注册请求消息；

处理单元 520，用于确定第一注册请求消息；

接收单元 530，用于接收 MME 发送的切换命令消息。

装置 50 和方法实施例中的用户设备完全对应，装置 50 可以是方法实施例中的用户设备，或者方法实施例中的用户设备内部的芯片或功能模块。装置 50 的相应单元用于执行图 3 和图 4 所示的方法实施例中由用户设备执行的相应步骤。

其中，装置 50 中的发送单元 510 执行方法实施例中用户设备发送的步骤。例如，执行图 3 中向第一 AMF 发送注册请求消息的步骤 S316 和执行图 4 中向第一 AMF 发送第一注册请求消息的步骤 S420；

处理单元 520 执行方法实施例中用户设备内部实现或处理的步骤。例如，执行图 3 中确定映射的安全上下文的步骤 S315 和执行图 4 中确定第一注册请求消息的步骤 S410；

接收单元 530 执行方法实施例中用户设备接收的步骤。例如，执行图 3 中接收 MME 发送的切换命令消息的步骤 S314 和执行图 4 中接收 MME 发送的切换命令消息的步骤 S414。

装置 50 中所示发送单元 510 和接收单元 530 可以组成收发单元，同时具有接收和发送的功能。其中，处理单元 520 可以是处理器。发送单元 510 可以是发射器，接收单元 530 可以是接收器。接收器和发射器可以集成在一起组成收发器。

参见图 6，图 6 是适用于本申请实施例的用户设备 60 的结构示意图。该用户设备 60 可应用于图 1 所示出的系统中。为了便于说明，图 6 仅示出了用户设备的主要部件。如图 6 所示，用户设备 60 包括处理器（对应于图 5 中所示的处理单元 520）、存储器、控制电路、天线以及输入输出装置（对应于图 5 中所示的发送单元 510 和接收单元 530）。处理器用于控制天线以及输入输出装置收发信号，存储器用于存储计算机程序，处理器用于从存储器中调用并运行该计算机程序，以执行本申请提出的获取安全上下文的方法中由用户设备执行的相应流程和/或操作。此处不再赘述。

本领域技术人员可以理解，为了便于说明，图 6 仅示出了一个存储器和处理器。在实际的用户设备中，可以存在多个处理器和存储器。存储器也可以称为存储介质或者存储设备等，本申请实施例对此不做限制。

参见图 7，图 7 是本申请提出的获取安全上下文的装置 70 的示意图。如图 7 所示，装置 70 包括接收单元 710、处理单元 720 和发送单元 730。

接收单元 710，用于接收用户设备发送的第一注册请求消息，所述第一注册请求消息中携带第二注册请求消息，其中，所述第二注册请求消息被第一安全上下文进行过完整性保护，所述第一安全上下文为所述用户设备与第二 AMF 之间的本地安全上下文，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；

处理单元 720，用于确定映射的安全上下文；

发送单元 730，用于向第二 AMF 发送第二注册请求消息。

10 装置 70 和方法实施例中的第一 AMF 完全对应，装置 70 可以是方法实施例中的第一 AMF，或者方法实施例中的第一 AMF 内部的芯片或功能模块。装置 70 的相应单元用于执行图 3 和图 4 所示的方法实施例中由第一 AMF 执行的相应步骤。

其中，装置 70 中的接收单元 710 执行方法实施例中第一 AMF 接收的步骤。例如，执行图 3 中接收 MME 发送的转发重分配请求消息的步骤 S311、执行图 4 中接收 MME 发送的转发重分配请求消息的步骤 S411、执行图 3 中接收 UE 发送的注册请求消息的步骤 S316、执行图 3 中接收 UE 发送的第一注册请求消息的步骤 S420、执行图 3 中接收第二 AMF 发送的第二响应消息的步骤 S330、执行图 4 中接收第二 AMF 发送的 UE 的安全上下文的步骤 S460。

20 处理单元 720 执行方法实施例中第一 AMF 内部实现或处理的步骤。例如，执行图 3 中确定映射的安全上下文的步骤 S312、执行图 4 中确定映射的安全上下文的步骤 S412、执行图 3 中验证 UE 的步骤 S317、执行图 4 中验证 UE 的步骤 S430。

发送单元 730 执行方法实施例中第一 AMF 发送的步骤。例如，执行图 3 中向 MME 发送转发重分配响应消息的步骤 S313、执行图 4 中向 MME 发送转发重分配响应消息的步骤 S413、执行图 3 中向第二 AMF 发送第二请求消息的步骤 S310、执行图 4 中向第二 AMF 发送第二注册请求消息的步骤 S440。

接收单元 710 和发送单元 730 可以组成收发单元，同时具有接收和发送的功能。其中，处理单元 720 可以是处理器。发送单元 730 可以是发射器。接收单元 710 可以是接收器。接收器和发射器可以集成在一起组成收发器。

30 如图 8 所示，本申请实施例还提供了一种第一 AMF 80，该第一 AMF 80 包括处理器 810，存储器 820 与收发器 830，其中，存储器 820 中存储指令或程序，处理器 830 用于执行存储器 820 中存储的指令或程序。存储器 820 中存储的指令或程序被执行时，收发器 830 用于执行图 7 所示的装置 70 中的接收单元 710 与发送单元 730 执行的操作。

参见图 9，图 9 是本申请提出的获取安全上下文的装置 90 的示意图。如图 9 所示，装置 90 包括接收单元 910、处理单元 920 和发送单元 930。

35 接收单元 910，用于接收第一 AMF 发送的第二注册请求消息，其中，所述第二注册请求消息被第一安全上下文进行过完整性保护，所述第一安全上下文为所述用户设备与第二 AMF 之间的本地安全上下文；

处理单元 920，用于校验所述第二注册请求消息的完整性；

发送单元 930，当处理单元 920 校验所述第二注册请求消息的完整性成功，向所述第

一 AMF 发送所述用户设备的安全上下文。

装置 90 和方法实施例中的第二 AMF 完全对应，装置 90 可以是方法实施例中的第二 AMF，或者方法实施例中的第二 AMF 内部的芯片或功能模块。装置 80 的相应单元用于执行图 3 和图 4 所示的方法实施例中由第二 AMF 执行的相应步骤。

- 5 其中，装置 90 中的接收单元 910 执行方法实施例中第二 AMF 接收的步骤。例如，执行图 3 中接收第一 AMF 发送的第二请求消息的步骤 S310、执行图 4 中接收第一 AMF 发送的第二注册请求消息的步骤 S440。

处理单元 920 执行方法实施例中第二 AMF 内部实现或处理的步骤。例如，执行图 3 中确定无需验证 UE 的步骤 S320、执行图 4 中校验第二注册请求消息的完整性的步骤 S450。

- 10 发送单元 930 执行方法实施例中第二 AMF 发送的步骤。例如，执行图 3 中向第一 AMF 发送第二响应消息的步骤 S330、执行图 4 中向第一 AMF 发送 UE 的安全上下文的步骤 S460。

接收单元 910 和发送单元 930 可以组成收发单元，同时具有接收和发送的功能。其中，处理单元 920 可以是处理器。发送单元 930 可以是发射器，接收单元 910 可以是接收器。

- 15 接收器和发射器可以集成在一起组成收发器。

如图 10 所示，本申请实施例还提供了一种第二 AMF 100，该第二 AMF 100 包括处理器 1010，存储器 1020 与收发器 1030，其中，存储器 1020 中存储指令或程序，处理器 1030 用于执行存储器 1020 中存储的指令或程序。存储器 1020 中存储的指令或程序被执行时，收发器 1030 用于执行图 9 所示的装置 90 中的接收单元 910 与发送单元 930 执行的操作。

- 20 本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当该指令在计算机上运行时，使得计算机执行上述如图 3 和图 4 所示的方法中第一 AMF 执行的各个步骤。

本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当该指令在计算机上运行时，使得计算机执行上述如图 3 和图 4 所示的方法中第二

- 25 AMF 执行的各个步骤。

本申请实施例还提供了一种包含指令的计算机程序产品，当该计算机程序产品在计算机上运行时，使得计算机执行如图 3 和图 4 所示的方法中第一 AMF 执行的各个步骤。

本申请实施例还提供了一种包含指令的计算机程序产品，当该计算机程序产品在计算机上运行时，使得计算机执行如图 3 和图 4 所示的方法中第二 AMF 执行的各个步骤。

- 30 本申请实施例还提供一种芯片，包括处理器。该处理器用于读取并运行存储器中存储的计算机程序，以执行本申请提供的获取安全上下文的方法中由第二 AMF 执行的相应操作和/或流程。可选地，该芯片还包括存储器，该存储器与该处理器通过电路或电线与存储器连接，处理器用于读取并执行该存储器中的计算机程序。进一步可选地，该芯片还包括通信接口，处理器与该通信接口连接。通信接口用于接收需要处理的数据和/或信息，  
35 处理器从该通信接口获取该数据和/或信息，并对该数据和/或信息进行处理。该通信接口可以是输入输出接口。

本申请还提供一种芯片，包括处理器。该处理器用于调用并运行存储器中存储的计算机程序，以执行本申请提供的获取安全上下文的方法中由第一 AMF 执行的相应操作和/或流程。可选地，该芯片还包括存储器，该存储器与该处理器通过电路或电线与存储器连

接，处理器用于读取并执行该存储器中的计算机程序。进一步可选地，该芯片还包括通信接口，处理器与该通信接口连接。通信接口用于接收需要处理的数据和/或信息，处理器从该通信接口获取该数据和/或信息，并对该数据和/或信息进行处理。该通信接口可以是输入输出接口。

5 本领域普通技术人员可以意识到，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，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，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来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

10 所属领域的技术人员可以清楚地了解到，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。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

另外，本申请中术语“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。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系；本申请中术语“至少一个”，可以表示“一个”和“两个或两个以上”，例如，A、B 和 C 中至少一个，可以表示：单独存在 A，单独存在 B，单独存在 C、同时存在 A 和 B，同时存在 A 和 C，同时存在 C 和 B，同时存在 A 和 B 和 C，这七种情况。

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。因此，本申请的保护范围应以所述权利要求的保护范围为准。

# 权 利 要 求 书

1、一种获取安全上下文的方法，其特征在于，包括：

5 第一接入和移动管理功能 AMF 接收用户设备发送的第一注册请求消息，所述第一注册请求消息中携带第二注册请求消息，

其中，所述第二注册请求消息被第一安全上下文进行过完整性保护，所述第一安全上下文为所述用户设备与第二 AMF 之间的本地安全上下文，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；

10 所述第一 AMF 向所述第二 AMF 发送所述第二注册请求消息；

所述第二 AMF 校验所述第二注册请求消息的完整性；

若所述第二 AMF 校验所述第二注册请求消息的完整性成功，则所述第二 AMF 向所述第一 AMF 发送所述用户设备的安全上下文。

2、根据权利要求 1 所述的方法，其特征在于，所述用户设备的安全上下文包括：

15 所述第一安全上下文，或者，基于所述第一安全上下文获得的第二安全上下文。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述第一 AMF 向所述第二 AMF 发送所述第二注册请求消息，包括：

所述第一 AMF 向所述第二 AMF 发送用户设备上下文传输服务调用请求，所述用户设备上下文传输服务调用请求中携带所述第二注册请求消息。

20 4、根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述第二 AMF 向所述第一 AMF 发送所述用户设备的安全上下文，包括：

所述第二 AMF 向所述第一 AMF 发送第一响应消息，所述第一响应消息中携带所述用户设备的安全上下文。

5、根据权利要求 1 至 4 中任一项所述的方法，其特征在于，所述方法还包括：

25 当所述第一 AMF 接收到所述第二 AMF 校验所述第二注册请求消息的完整性失败的消息时，所述第一 AMF 继续使用映射的安全上下文或向所述用户设备发起初始认证。

6、根据权利要求 5 中所述的方法，其特征在于，所述映射的安全上下文是根据移动管理实体 MME 与所述用户设备之间的安全上下文获得的，其中，所述 MME 为所述 4G 通信系统中的网元。

30 7、根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述第二 AMF 校验所述第二注册请求消息的完整性，包括：

所述第二 AMF 根据所述第一安全上下文对所述第二注册请求消息的完整性进行校验。

8、一种获取安全上下文的方法，其特征在于，包括：

35 用户设备确定第二注册请求消息，所述第二注册请求消息被第一安全上下文进行过完整性保护，其中，所述第一安全上下文为所述用户设备与第二接入和移动管理功能 AMF 之间的本地安全上下文；

所述用户设备向第一 AMF 发送第一注册请求消息，所述第一注册请求消息中携带所

述第二注册请求消息，

其中，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF。

9、根据权利要求 8 所述方法，其特征在于，所述方法还包括：

5 若接收到所述第一 AMF 发送的非接入层安全模式命令 NAS SMC 消息，则对所述 NAS SMC 进行完整校验；

若校验成功，则向所述第一 AMF 发送非接入层安全模式完成消息。

10、一种通信系统，其特征在于，所述通信系统中包括第一接入和移动管理功能 AMF 和第一 AMF，

10 所述第一 AMF，用于接收用户设备发送的第一注册请求消息，所述第一注册请求消息中携带第二注册请求消息，其中，所述第二注册请求消息被第一安全上下文进行过完整性保护，其中，所述第一安全上下文为所述用户设备与第二 AMF 之间的本地安全上下文，所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后，为所述用户设备提供接入和移动管理服务的 AMF；

15 所述第一 AMF，还用于向所述第二 AMF 发送所述第二注册请求消息；

所述第二 AMF，用于校验所述第二注册请求消息的完整性；

所述第二 AMF，还用于若校验所述第二注册请求消息的完整性成功，则向所述第一 AMF 发送所述用户设备的安全上下文。

20 11、根据权利要求 10 所述的通信系统，其特征在于，所述用户设备的安全上下文包括：

所述第一安全上下文，或者，基于所述第一安全上下文获得的第二安全上下文。

12、根据权利要求 10 或 11 所述的通信系统，其特征在于，

所述第一 AMF，具体用于向所述第二 AMF 发送用户设备上下文传输服务调用请求，所述用户设备上下文传输服务调用请求中携带所述第二注册请求消息。

25 13、根据权利要求 10 至 12 中任一项所述的通信系统，其特征在于，

所述第二 AMF，具体用于向所述第一 AMF 发送第一响应消息，所述第一响应消息中携带所述用户设备的安全上下文。

14、根据权利要求 10 至 13 中任一项所述的通信系统，其特征在于，

30 所述第一 AMF，还用于当接收到所述第二 AMF 校验所述第二注册请求消息的完整性失败的消息时，继续使用映射的安全上下文或向所述用户设备发起初始认证。

15、根据权利要求 14 所述的通信系统，其特征在于，所述映射的安全上下文是根据移动管理实体 MME 与所述用户设备之间的安全上下文获得的，其中，所述 MME 为所述 4G 通信系统中的网元。

16、根据权利要求 10 至 15 中任一项所述的通信系统，其特征在于，

35 所述第二 AMF，具体用于根据所述第一安全上下文对所述第二注册请求消息进行完整性校验。

17、一种获取安全上下文的装置，其特征在于，包括：

处理单元，用于确定第二注册请求消息，所述第二注册请求消息被第一安全上下文进行过完整性保护，其中，所述第一安全上下文为所述用户设备与第二接入和移动管理功能

AMF 之间的本地安全上下文;

发送单元, 用于向第一 AMF 发送第一注册请求消息, 所述第一注册请求消息中携带所述第二注册请求消息, 其中, 所述第一 AMF 为所述用户设备从 4G 通信系统切换至 5G 通信系统后, 为所述用户设备提供接入和移动管理服务的 AMF。

- 5 18、根据权利要求 17 所述装置, 其特征在于, 所述装置还包括接收单元;

所述处理单元, 用于若所述接收单元接收到所述第一 AMF 发送的非接入层安全模式命令 NAS SMC 消息, 则对所述 NAS SMC 进行完整校验;

所述发送单元, 还用于若所述校验成功, 则向所述第一 AMF 发送非接入层安全模式完成消息。

- 10 19、一种计算机可读存储介质, 其特征在于, 包括: 所述计算机可读介质存储有计算机程序; 所述计算机程序在计算机上运行时, 使得计算机执行权利要求 1-9 中任一项所述的方法。

20、一种获取安全上下文的方法, 其特征在于, 所述方法包括:

第一接入和移动管理功能 AMF 接收用户设备 UE 发送的第一注册请求消息;

- 15 所述第一 AMF 对所述第一注册请求消息进行完整性保护校验;

若所述第一 AMF 成功校验所述第一注册请求消息的完整性保护, 则所述第一 AMF 向第二 AMF 发送第二请求消息;

所述第二 AMF 接收所述第二请求消息;

若所述第二请求消息中携带指示信息且所述指示信息用于指示所述 UE 为合法 UE,

- 20 所述第二 AMF 向所述第一 AMF 发送所述 UE 的安全上下文。

21、根据权利要求 20 所述的方法, 其特征在于, 所述方法还包括:

移动管理网元 MME 向所述第一 AMF 发送转发重分配请求消息, 所述转发重分配请求消息包括所述 UE 和所述 MME 之间的安全上下文;

- 25 所述第一 AMF 根据所述用户设备和所述 MME 之间的安全上下文确定映射的安全上下文;

所述第一 AMF 对所述第一注册请求消息进行完整性保护校验, 包括:

所述第一 AMF 利用所述映射的安全上下文对所述第一注册请求消息进行完整性保护校验。

- 30 22、根据权利要求 20 或 21 所述的方法, 其特征在于, 所述第一注册请求消息中还包括所述用户设备的标识 5G-GUTI。

23、根据权利要求 22 所述的方法, 其特征在于, 所述指示信息为所述 5G-GUTI。

24、根据权利要求 20 至 22 任一所述的方法, 其特征在于, 所述指示信息为原因值。

25、一种获取安全上下文的系统, 其特征在于, 所述系统包括第一接入和移动管理功能 AMF 和第二 AMF;

- 35 所述第一 AMF, 用于接收用户设备 UE 发送的第一注册请求消息; 对所述第一注册请求消息进行完整性保护校验; 若成功校验所述第一注册请求消息的完整性保护, 则向第二 AMF 发送第二请求消息;

所述第二 AMF, 用于接收所述第二请求消息; 若所述第二请求消息中携带指示信息且所述指示信息用于指示所述 UE 为合法 UE, 则向所述第一 AMF 发送 UE 的安全上下文。

- 26、根据权利要求 25 所述的系统，其特征在于，所述系统还包括移动管理网元 MME；  
所述 MME，用于向所述第一 AMF 发送转发重分配请求消息，所述转发重分配请求消息包括所述 UE 和所述 MME 之间的安全上下文；  
所述第一 AMF，还用于根据所述用户设备和所述 MME 之间的安全上下文确定映射的安全上下文；  
5 其中，所述对所述第一注册请求消息进行完整性保护校验，包括：  
利用所述映射的安全上下文对所述第一注册请求消息进行完整性保护校验。
- 27、根据权利要求 25 或 26 所述的系统，其特征在于，所述第一注册请求消息中还包  
括所述用户设备的标识 5G-GUTI。
- 10 28、根据权利要求 27 所述的系统，其特征在于，所述指示信息为所述 5G-GUTI。
- 29、根据权利要求 25 至 27 任一所述的系统，其特征在于，所述指示信息为原因值。
- 30、一种获取安全上下文的方法，其特征在于，所述方法包括：  
第一接入和移动管理功能 AMF 接收用户设备 UE 发送的第一注册请求消息；  
所述第一 AMF 对所述第一注册请求消息进行完整性保护校验；  
15 若所述第一 AMF 成功校验所述第一注册请求消息的完整性保护，则所述第一 AMF  
向第二 AMF 发送第二请求消息；所述第二请求消息中携带指示信息且所述指示信息用于  
指示所述 UE 为合法 UE。
- 31、根据权利要求 30 所述的方法，其特征在于，所述方法还包括：  
所述第一 AMF 接收移动管理网元 MME 发送的转发重分配请求消息，所述转发重分  
20 配请求消息包括所述用户设备和所述 MME 之间的安全上下文；  
所述第一 AMF 根据所述 UE 和所述 MME 之间的安全上下文确定映射的安全上下文；  
所述第一 AMF 对所述第一注册请求消息进行完整性保护校验，包括：  
所述第一 AMF 利用所述映射的安全上下文对所述第一注册请求消息进行完整性  
保护校验。
- 25 32、根据权利要求 30 或 31 所述的方法，其特征在于，所述第一注册请求消息中还包  
括所述用户设备的标识 5G-GUTI。
- 33、根据权利要求 32 所述的方法，其特征在于，所述指示信息为所述 5G-GUTI。
- 34、根据权利要求 30 至 32 任一所述的方法，其特征在于，所述指示信息为原因值。
- 35、一种获取安全上下文的方法，其特征在于，所述方法包括：  
第二接入和移动管理功能 AMF 接收第一 AMF 发送的请求消息；  
若所述请求消息中携带指示信息且所述指示信息用于指示用户设备 UE 为合法 UE，  
所述第二 AMF 向所述第一 AMF 发送所述 UE 的安全上下文。
- 36、根据权利要求 35 所述的方法，其特征在于，所述第二 AMF 向所述第一 AMF 发  
送所述 UE 的安全上下文之前，所述方法还包括：  
35 所述第二 AMF 跳过对所述 UE 的认证。
- 37、根据权利要求 35 或 36 所述的方法，其特征在于，所述指示信息为所述  
5G-GUTI。
- 38、根据权利要求 35 或 36 所述的方法，其特征在于，所述指示信息为原因值。
- 39、一种通信装置，其特征在于，所述装置包括处理器，存储器与收发器；所述存

存储器中存储指令，所述处理器与所述收发器耦合；当所述存储器中存储的指令被执行时，所述处理器执行以下操作：

接收用户设备 UE 发送的第一注册请求消息；

对所述第一注册请求消息进行完整性保护校验；

- 5       若成功校验所述第一注册请求消息的完整性保护，则向第二 AMF 发送第二请求消息；所述第二请求消息中携带指示信息且所述指示信息用于指示所述 UE 为合法 UE。

40、根据权利要求 39 所述的通信装置，其特征在于，所述处理器还执行以下操作：

接收移动管理网元 MME 发送的转发重分配请求消息，所述转发重分配请求消息包括所述用户设备和所述 MME 之间的安全上下文；

- 10       根据所述 UE 和所述 MME 之间的安全上下文确定映射的安全上下文；

所述对所述第一注册请求消息进行完整性保护校验，包括：利用所述映射的安全上下文对所述第一注册请求消息进行完整性保护校验。

41、根据权利要求 39 或 40 所述的通信装置，其特征在于，所述第一注册请求消息中还包括所述用户设备的标识 5G-GUTI。

- 15       42、根据权利要求 41 所述的通信装置，其特征在于，所述指示信息为所述 5G-GUTI。

43、根据权利要求 39 至 41 任一所述的通信装置，其特征在于，所述指示信息为原因值。

- 20       44、一种通信装置，其特征在于，所述装置包括处理器，存储器与收发器；所述存储器中存储指令，所述处理器与所述收发器耦合；当所述存储器中存储的指令被执行时，所述处理器执行以下操作：

接收第一 AMF 发送的请求消息；

若所述请求消息中携带指示信息且所述指示信息用于指示用户设备 UE 为合法 UE，向所述第一 AMF 发送所述 UE 的安全上下文。

- 25       45、根据权利要求 44 所述的通信装置，其特征在于，所述处理器还执行以下操作；跳过对所述 UE 的认证。

46、根据权利要求 44 或 45 所述的通信装置，其特征在于，所述指示信息为所述 5G-GUTI。

- 30       47、根据权利要求 44 或 45 所述的通信装置，其特征在于，所述指示信息为原因值。