

截短参数的保护方法及装置

技术领域

5 本申请涉及通信技术领域，尤其涉及一种截短参数的保护方法及装置。

背景技术

当前，在一些流程（例如重建立流程）中，终端向接入网设备发送携带第五代系统架构演进临时移动台标识符（5th generation-system architecture evolution-temporary mobile subscriber identity, 5G-S-TMSI）的无线资源控制（radio resource control, RRC）
10 消息，以使得接入网设备能够根据 5G-S-TMSI 寻址到特定的接入与移动性管理功能（access and mobility management function, AMF）。

但是，RRC 消息长度有限制，因此 RRC 消息可能无法携带完整的 5G-S-TMSI。这种情况下，终端需要根据截短参数对 5G-S-TMSI 进行截短，再将截短的 5G-S-TMSI 通过 RRC 消息上报给接入网设备。接入网设备接收到截短后的参数（如截短的
15 5G-S-TMSI）之后，将截短后的参数恢复成完整的参数（如完整的 5G-S-TMSI）。

对于其他类似的场景，终端可能也需要对一些其他特定的参数进行截短，并执行上述类似的操作。

终端所使用的截短参数一般为网络侧所配置的。使用控制面蜂窝物联网（cellular internet of things, CIoT）第五代系统（5th generation system, 5GS）优化功能的终端
20 与接入网设备之间不会建立接入层（access stratum, AS）安全上下文，因此接入网设备不能对截短参数进行 AS 安全保护，导致接入网设备只能向终端发送无 AS 安全保护的截短参数。这种情况下，截短参数存在被攻击者篡改的风险。在截短参数被篡改的情况下，终端不能获取到正确的截短参数，导致终端不能正常接入网络。

发明内容

25 本申请提供一种截短参数的保护方法及装置，用于降低截短参数在传输过程中的安全风险。

第一方面，提供一种截短参数的保护方法，包括：移动管理网元判断终端是否符合预设条件，预设条件包括终端使用控制面 CIoT 5GS 优化功能；在终端符合预设条件的情况下，移动管理网元向终端发送经过 NAS 安全上下文进行 NAS 安全保护的下
30 行 NAS 消息，下行 NAS 消息包括截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理。

基于本申请的技术方案，在终端符合预设条件的情况下，该终端是使用控制面 CIoT 5GS 优化功能的终端，因此移动管理网元向终端经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，以使得终端获取到经过 NAS 安全保护的截短参数。这样
35 一来，保证终端接收到的截短参数不被篡改和伪造，从而防止终端被攻击者发起拒绝服务攻击，进而保证终端能够正常接入到网络中。

一种可能的设计中，截短参数是移动管理网元预先存储的。这样一来，移动管理网元无需向其他设备（例如接入网设备）获取截短参数，从而达到简化流程的目的。

一种可能的设计中，该方法还包括：移动管理网元接收接入网设备发送的截短参

数。可以理解的是，移动管理网元从接入网设备获取到截短参数，因此移动管理网元无需预先配置截短参数，从而降低截短参数的配置复杂度。

一种可能的设计中，所述移动管理网元判断终端是否符合预设条件，包括：所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能；若所述终端使用控制面 CIoT 5GS 优化功能，则所述移动管理网元确定所述终端符合预设条件；若所述终端没有使用控制面 CIoT 5GS 优化功能，则所述移动管理网元确定所述终端不符合预设条件。

一种可能的设计中，所述预设条件还包括：所述终端是初始注册到网络的终端。所述移动管理网元判断终端是否符合预设条件，包括：所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能，以及所述终端是否是初始注册到网络的终端；若所述终端使用控制面 CIoT 5GS 优化功能且所述终端是初始注册到网络中的终端，则所述移动管理网元确定所述终端符合预设条件；若所述终端没有使用控制面 CIoT 5GS 优化功能或者所述终端不是初始注册到网络中的终端，则所述移动管理网元确定所述终端不符合预设条件。

一种可能的设计中，移动管理网元判断终端是否是初始注册到网络的终端，包括：移动管理网元根据终端上报的注册类型，确定终端是初始注册到网络的终端。

一种可能的设计中，所述预设条件还包括：所述终端需要更新截短参数。所述移动管理网元判断终端是否符合预设条件，包括：所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能，以及所述终端是否需要更新截短参数；若所述终端使用控制面 CIoT 5GS 优化功能且所述终端是需要更新截短参数的终端，则所述移动管理网元确定所述终端符合预设条件；若所述终端没有使用控制面 CIoT 5GS 优化功能或者所述终端不是需要更新截短参数的终端，则所述移动管理网元确定所述终端不符合预设条件。

一种可能的设计中，移动管理网元判断终端是否需要更新截短参数，包括：当移动管理网元配置的截短参数与终端的上下文中存储的截短参数不相同，移动管理网元确定终端需要更新截短参数。

一种可能的设计中，移动管理网元判断终端是否需要更新截短参数，包括：在所述移动管理网元更新截短参数之后，移动管理网元确定所述终端需要更新截短参数。一种可能的设计中，移动管理网元判断终端是否使用控制面 CIoT 5GS 优化功能，包括：若终端上报的偏好的网络行为用于指示终端偏好使用控制面 CIoT 5GS 优化功能，并且移动管理网元支持控制面 CIoT 5GS 优化功能，则移动管理网元确定终端使用控制面 CIoT 5GS 优化功能。

一种可能的设计中，移动管理网元判断终端是否使用控制面 CIoT 5GS 优化功能，包括：若终端的上下文用于指示终端使用控制面 CIoT 5GS 优化功能，则移动管理网元确定终端使用控制面 CIoT 5GS 优化功能。

一种可能的设计中，移动管理网元判断终端是否符合预设条件，包括：在移动管理网元接收到终端的注册请求消息或者服务请求消息之后，移动管理网元判断终端是否符合预设条件。

一种可能的设计中，下行 NAS 消息为服务接受消息或者注册接受消息。

一种可能的设计中, 5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID, 5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer, 5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数, 所述第一截短参数用于截短 AMF set ID 和 5G-TMSI, 所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

一种可能的设计中, 该方法还包括: 所述移动管理网元根据 AMF set ID 的数目和/或 AMF pointer 的数目, 更新截短参数; 或者, 所述移动管理网元根据网络管理系统的指令, 更新截短参数; 或者, 所述移动管理网元接收接入网设备发送的更新后的截短参数。

第二方面, 提供一种截短参数的保护方法, 包括: 终端接收移动管理网元发送的经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息, 下行 NAS 消息包括截短参数, 截短参数用于对终端的 5G-S-TMSI 进行截短处理; 终端对下行 NAS 消息解安全保护; 在成功对下行 NAS 消息解安全保护之后, 终端存储截短参数。

基于本申请的技术方案, 由于截短参数是承载于经过 NAS 安全保护的下行 NAS 消息中, 因此截短参数也经过 NAS 安全保护, 从而保证截短参数不被篡改和伪造, 从而防止终端被攻击者发起拒绝服务攻击, 进而保证终端能够正常接入到网络中。

一种可能的设计中, 终端存储截短参数, 包括: 终端的 NAS 层存储截短参数。

一种可能的设计中, 该方法还包括: 终端的 NAS 层向终端的 RRC 层发送截短参数; 终端的 RRC 层根据截短参数, 对终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI。

一种可能的设计中, 该方法还包括: 终端的 NAS 层根据截短参数, 对终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI; 终端的 NAS 层向终端的 RRC 层发送截短的 5G-S-TMSI。

一种可能的设计中, 终端存储截短参数, 包括: 终端的 NAS 层向终端的 RRC 层发送截短参数; 终端的 RRC 层存储截短参数。

一种可能的设计中, 该方法还包括: 终端的 RRC 层根据截短参数, 对终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI。

一种可能的设计中, 该方法还包括: 所述终端的 RRC 层向所述终端的 NAS 层发送所述截短参数; 所述终端的 NAS 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI; 所述终端的 NAS 层向所述终端的 RRC 层发送所述截短的 5G-S-TMSI。

一种可能的设计中, 该方法还包括: 所述终端向所述接入网设备发送 RRC 重建请求消息, 所述 RRC 重建请求消息包括所述截短的 5G-S-TMSI。

一种可能的设计中, 下行 NAS 消息为服务接受消息或者注册接受消息。

一种可能的设计中, 5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID, 5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer, 5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数, 所述第一截短参数用于截短 AMF set ID 和 5G-TMSI, 所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第三方面，提供一种截短参数的保护方法，包括：接入网设备判断终端是否支持 CIoT 5GS 优化特性；在终端支持 CIoT 5GS 优化特性的情况下，接入网设备向移动管理网元发送截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理。

5 基于本申请的技术方案，在终端支持 CIoT 5GS 优化特性的情况下，接入网设备向移动管理网元发送截短参数，以便于移动管理网元对该截短参数进行 NAS 安全保护。这样一来，避免接入网设备直接向终端发送未经过安全保护的截短参数，降低截短参数在传输过程中的安全风险。

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：若终端的能力指示信息用于指示终端支持 CIoT 5GS 优化特性，则接入网设备确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：若终端使用的频点与 CIoT 设备使用的频点相同，则接入网设备确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：若终端发送的消息的类型与 CIoT 设备发送的消息的类型相同，则接入网设备确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：在接入网设备接收到终端发送的上行 RRC 消息之后，接入网设备判断终端是否支持 CIoT 5GS 优化特性。

20 一种可能的设计中，上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

一种可能的设计中，接入网设备向移动管理网元发送截短参数，包括：接入网设备向移动管理网元发送初始 UE 消息，初始 UE 消息包括截短参数。

一种可能的设计中，截短参数是预先存储在接入网设备中的。

一种可能的设计中，该方法还包括：所述接入网设备接收所述终端发送的 RRC 重建请求消息，所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

30 第四方面，提供一种截短参数的保护方法，包括：移动管理网元更新截短参数，截短参数用于对 5G-S-TMSI 进行截短处理；移动管理网元查找使用控制面 CIoT 5GS 优化功能的终端；移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，下行 NAS 消息包括更新后的截短参数。

基于本申请的技术方案，在移动管理网元更新截短参数的场景下，移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息。由于更新后的截短参数承载在该下行 NAS 消息中，因此更新后的截短参数不会在空口传输过程中被攻击者篡改或者伪造。这样一来，使用控制面 CIoT

5GS 优化功能的终端能够及时获取到正确的更新后的截短参数,保证,使用控制面 CIoT 5GS 优化功能的终端能够正常接入网络。

一种可能的设计中,移动管理网元更新截短参数,包括:移动管理网元根据 AMF set ID 的数目和/或 AMF pointer 的数目,更新截短参数;或者,移动管理网元根据网络管理系统的指令,更新截短参数;或者,移动管理网元接收接入网设备发送的更新后的截短参数。

一种可能的设计中,移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息,包括:在使用控制面 CIoT 5GS 优化功能的终端处于连接态的情况下,移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送下行 NAS 消息。

一种可能的设计中,移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息,包括:在使用控制面 CIoT 5GS 优化功能的终端处于非连接态的情况下,移动管理网元等待使用控制面 CIoT 5GS 优化功能的终端进入连接态;在使用控制面 CIoT 5GS 优化功能的终端进入连接态,并且移动管理网元与使用控制面 CIoT 5GS 优化功能的终端之间的激活 NAS 安全之后,移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送下行 NAS 消息。

一种可能的设计中,移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息,包括:在使用控制面 CIoT 5GS 优化功能的终端处于非连接态的情况下,移动管理网元以寻呼的方式触发使用控制面 CIoT 5GS 优化功能的终端进入连接态;在使用控制面 CIoT 5GS 优化功能的终端进入连接态,并且移动管理网元与使用控制面 CIoT 5GS 优化功能的终端之间的激活 NAS 安全之后,移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送下行 NAS 消息。

一种可能的设计中,下行 NAS 消息为 UE 配置更新命令消息,或者服务接受消息。

一种可能的设计中,5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID,5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer,5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数,所述第一截短参数用于截短 AMF set ID 和 5G-TMSI,所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第五方面,提供一种截短参数的保护方法,包括:移动管理网元接收接入网设备发送的截短参数,截短参数用于对终端的 5G-S-TMSI 进行截短处理;移动管理网元根据终端的 NAS 安全上下文,对终端的 5G-S-TMSI 进行完整性计算,生成第一 NAS MAC;移动管理网元向接入网设备发送第一 NAS MAC。

基于本申请的技术方案,移动管理网元对截短参数进行完整性计算,得到第一 NAS MAC,并将该第一 NAS MAC 发送给接入网设备。这样一来,接入网设备可以向终端该第一 NAS MAC 和截短参数,以保证截短参数在传输过程中不被攻击者篡改或者伪造,从而降低截短参数在传输过程中的安全风险。

一种可能的设计中,该方法还包括:移动管理网元接收接入网设备发送的保护指示信息和/或新鲜性参数,保护指示信息用于指示移动管理网元对截短参数进行安全保

护，新鲜性参数用于对截短参数的完整性计算。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和
5 第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第六方面，提供一种截短参数的保护方法，包括：接入网设备向移动管理网元发送截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理；接入网设备接收移动管理网元发送的第一 NAS MAC，第一 NAS MAC 是对截短参数进行完整性计算得到
10 的；接入网设备向终端发送第一 NAS MAC 和截短参数。

基于本申请的技术方案，接入网设备可以向终端该第一 NAS MAC 和截短参数，以保证截短参数在传输过程中不被攻击者篡改或者伪造，从而降低截短参数在传输过程中的安全风险。

一种可能的设计中，该方法还包括：接入网设备判断终端是否支持 CIoT 5GS 优化特性。接入网设备向移动管理网元发送截短参数，包括：在终端支持 CIoT 5GS 优化特性的情况下，接入网设备向移动管理网元发送截短参数。
15

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：若终端的能力指示信息用于指示终端支持 CIoT 5GS 优化特性，则接入网设备确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：若终端使用的频点与 CIoT 设备使用的频点相同，则接入网设备确定终端支持 CIoT 5GS 优化特性。
20

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：若终端发送的消息的类型与 CIoT 设备发送的消息的类型相同，则接入网设备确定终端支持 CIoT 5GS 优化特性。
25

一种可能的设计中，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：在接入网设备接收到终端发送的上行 RRC 消息之后，接入网设备判断终端是否支持 CIoT 5GS 优化特性。

一种可能的设计中，上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。
30 一种可能的设计中，该方法还包括：接入网设备向移动管理网元发送保护指示信息和/或新鲜性参数，保护指示信息用于指示移动管理网元对截短参数进行安全保护，新鲜性参数用于对截短参数的完整性计算。

一种可能的设计中，该方法还包括：所述接入网设备接收所述终端发送的 RRC 重建请求消息，所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和
35 第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第七方面，提供一种截短参数的保护方法，包括：终端接收接入网设备发送的第一 NAS MAC 和截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理；终端根据 NAS 安全上下文，对截短参数进行完整性计算，生成第二 NAS MAC；终端根据第二 NAS MAC，校验第一 NAS MAC；在第一 NAS MAC 通过校验的情况下，终端存储截短参数。

5 基于本申请的技术方案，由于终端接收到第一 NAS MAC 和截短参数，因此终端可以通过校验第一 NAS MAC，以验证截短参数的完整性。在确定截短参数未被篡改或者伪造的情况下，终端存储该截短参数，以便于后续过程中根据该截短参数来截短 5G-S-TMSI。

10 一种可能的设计中，终端存储截短参数，包括：终端的 RRC 层存储截短参数。

一种可能的设计中，该方法还包括：终端的 RRC 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

一种可能的设计中，该方法还包括：终端的 RRC 层向终端的 NAS 层发送截短参数；终端的 NAS 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 15 5G-S-TMSI；终端的 NAS 层向终端的 RRC 层发送截短的 5G-S-TMSI。

一种可能的设计中，终端存储截短参数，包括：终端的 RRC 层向终端的 NAS 层发送截短参数；终端的 NAS 层存储截短参数。

一种可能的设计中，该方法还包括：终端的 NAS 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI；终端的 NAS 层向终端的 RRC 层 20 发送截短的 5G-S-TMSI。

一种可能的设计中，该方法还包括：终端的 NAS 层向终端的 RRC 层发送截短参数；终端的 RRC 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

一种可能的设计中，该方法还包括：所述终端向所述接入网设备发送 RRC 重建立 25 请求消息，所述 RRC 重建立请求消息包括截短的 5G-S-TMSI。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数 30 用于截短 AMF pointer 和 5G-TMSI。

第八方面，提供一种通信装置，包括：处理模块，用于判断终端是否符合预设条件，预设条件包括终端使用控制面 ClIoT 5GS 优化功能；通信模块，用于在终端符合预设条件的情况下，向终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，下行 NAS 消息包括截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处 35 理。

一种可能的设计中，通信装置还包括存储模块；存储模块，用于存储截短参数。

一种可能的设计中，通信模块，还用于接收接入网设备发送的截短参数。

一种可能的设计中，所述处理模块，用于判断终端是否符合预设条件，包括：判断所述终端是否使用控制面 ClIoT 5GS 优化功能；若所述终端使用控制面 ClIoT 5GS 优

化功能，则确定所述终端符合预设条件；若所述终端没有使用控制面 ClIoT 5GS 优化功能，则确定所述终端不符合预设条件。

一种可能的设计中，所述预设条件还包括：所述终端是初始注册到网络的终端。所述处理模块，用于判断终端是否符合预设条件，包括：判断所述终端是否使用控制面 ClIoT 5GS 优化功能，以及所述终端是否是初始注册到网络的终端；若所述终端使用控制面 ClIoT 5GS 优化功能且所述终端是初始注册到网络中的终端，则确定所述终端符合预设条件；若所述终端没有使用控制面 ClIoT 5GS 优化功能或者所述终端不是初始注册到网络中的终端，则确定所述终端不符合预设条件。

一种可能的设计中，处理模块，具体用于根据终端上报的注册类型，确定终端是初始注册到网络的终端。

一种可能的设计中，所述预设条件还包括：所述终端需要更新截短参数。所述处理模块，用于判断终端是否符合预设条件，包括：判断所述终端是否使用控制面 ClIoT 5GS 优化功能，以及所述终端是否需要更新截短参数；若所述终端使用控制面 ClIoT 5GS 优化功能且所述终端是需要更新截短参数的终端，则确定所述终端符合预设条件；若所述终端没有使用控制面 ClIoT 5GS 优化功能或者所述终端不是需要更新截短参数的终端，则确定所述终端不符合预设条件。

一种可能的设计中，处理模块，具体用于当移动管理网元配置的截短参数与终端的上下文中存储的截短参数不相同，确定终端需要更新截短参数。

一种可能的设计中，处理模块，具体用于在移动管理网元更新截短参数之后，确定所述终端需要更新截短参数。

一种可能的设计中，处理模块，还用于根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数；或者，根据网络管理系统的指令，更新截短参数；或者，接收接入网设备发送的更新后的截短参数。

一种可能的设计中，处理模块，具体用于若终端上报的偏好的网络行为用于指示终端偏好使用控制面 ClIoT 5GS 优化功能，并且移动管理网元支持控制面 ClIoT 5GS 优化功能，则确定终端使用控制面 ClIoT 5GS 优化功能。

一种可能的设计中，处理模块，具体用于若终端的上下文用于指示终端使用控制面 ClIoT 5GS 优化功能，则确定终端使用控制面 ClIoT 5GS 优化功能。

一种可能的设计中，处理模块，具体用于在通信模块接收到终端的注册请求消息或者服务请求消息之后，判断终端是否符合预设条件。

一种可能的设计中，下行 NAS 消息为服务接受消息或者注册接受消息。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

一种可能的设计中，所述处理模块，用于根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数。

一种可能的设计中，所述处理模块，用于根据网络管理系统的指令，更新截短参

数。

一种可能的设计中，所述通信模块，用于接收接入网设备发送的更新后的截短参数。

5 第九方面，提供一种通信装置，包括：通信模块，用于接收移动管理网元发送的经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，下行 NAS 消息包括截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理；处理模块，用于对下行 NAS 消息解安全保护；存储模块，用于在处理模块成功对下行 NAS 消息解安全保护之后，存储截短参数。

一种可能的设计中，存储模块，用于存储截短参数，包括：NAS 层存储截短参数。

10 一种可能的设计中，处理模块，还用于获取截短的 5G-S-TMSI，包括：NAS 层向 RRC 层发送截短参数；RRC 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

一种可能的设计中，处理模块，还用于获取截短的 5G-S-TMSI，包括：NAS 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI；NAS 层向
15 RRC 层发送截短的 5G-S-TMSI。

一种可能的设计中，存储模块，用于存储截短参数，包括：NAS 层向 RRC 层发送截短参数；RRC 层存储截短参数。

一种可能的设计中，处理模块，还用于获取截短的 5G-S-TMSI，包括：RRC 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

20 一种可能的设计中，所述处理模块，还用于获取截短的 5G-S-TMSI，包括：RRC 层向 NAS 层发送所述截短参数；所述 NAS 层根据所述截短参数，对所述终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI；所述 NAS 层向所述 RRC 层发送所述截短的 5G-S-TMSI。

一种可能的设计中，下行 NAS 消息为服务接受消息或者注册接受消息。

25 一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

30 一种可能的设计中，所述通信模块，还用于向所述接入网设备发送 RRC 重建立请求消息，所述 RRC 重建立请求消息包括所述截短的 5G-S-TMSI。

第十方面，提供一种通信装置，包括：处理模块，用于判断终端是否支持 CIoT 5GS 优化特性；通信模块，用于在终端支持 CIoT 5GS 优化特性的情况下，向移动管理网元发送截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理。

35 一种可能的设计中，处理模块，具体用于若终端的能力指示信息用于指示终端支持 CIoT 5GS 优化特性，则确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，处理模块，具体用于若终端使用的频点与 CIoT 设备使用的频点相同，则确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，处理模块，具体用于若终端发送的消息的类型与 CIoT 设备发

送的消息的类型相同，则确定终端支持 CIoT 5GS 优化特性。

一种可能的设计中，处理模块，具体用于在通信模块接收到终端发送的上行 RRC 消息之后，判断终端是否支持 CIoT 5GS 优化特性。

一种可能的设计中，上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

- 5 一种可能的设计中，通信模块，具体用于向移动管理网元发送初始 UE 消息，初始 UE 消息包括截短参数。

一种可能的设计中，通信装置还包括存储模块；存储模块，用于存储截短参数。

一种可能的设计中，所述通信模块，用于接收所述终端发送的 RRC 重建请求消息，所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

- 10 一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

- 15 第十一方面，提供一种通信装置，包括：处理模块，用于更新截短参数，截短参数用于对 5G-S-TMSI 进行截短处理；查找使用控制面 CIoT 5GS 优化功能的终端；通信模块，用于向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，下行 NAS 消息包括更新后的截短参数。

- 20 一种可能的设计中，处理模块，用于根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数；或者，根据网络管理系统的指令，更新截短参数；或者，接收接入网设备发送的更新后的截短参数。

一种可能的设计中，通信模块，具体用于在使用控制面 CIoT 5GS 优化功能的终端处于连接态的情况下，向使用控制面 CIoT 5GS 优化功能的终端发送下行 NAS 消息。

- 25 一种可能的设计中，通信模块，具体用于在使用控制面 CIoT 5GS 优化功能的终端处于非连接态的情况下，等待使用控制面 CIoT 5GS 优化功能的终端进入连接态；在使用控制面 CIoT 5GS 优化功能的终端进入连接态，并且移动管理网元与使用控制面 CIoT 5GS 优化功能的终端之间的激活 NAS 安全之后，向使用控制面 CIoT 5GS 优化功能的终端发送下行 NAS 消息。

- 30 一种可能的设计中，通信模块，具体用于在使用控制面 CIoT 5GS 优化功能的终端处于非连接态的情况下，以寻呼的方式触发使用控制面 CIoT 5GS 优化功能的终端进入连接态；在使用控制面 CIoT 5GS 优化功能的终端进入连接态，并且移动管理网元与使用控制面 CIoT 5GS 优化功能的终端之间的激活 NAS 安全之后，向使用控制面 CIoT 5GS 优化功能的终端发送下行 NAS 消息。

一种可能的设计中，下行 NAS 消息为 UE 配置更新命令消息，或者服务接受消息。

- 35 一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第十二方面，提供一种通信装置，包括：通信模块，用于接收接入网设备发送的截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理；处理模块，用于根据终端的 NAS 安全上下文，对终端的 5G-S-TMSI 进行完整性计算，生成第一 NAS MAC；通信模块，还用于向接入网设备发送第一 NAS MAC。

5 一种可能的设计中，通信模块，还用于接收接入网设备发送的保护指示信息和/或新鲜性参数，保护指示信息用于指示移动管理网元对截短参数进行安全保护，新鲜性参数用于对截短参数的完整性计算。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和
10 第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第十三方面，提供一种通信装置，包括：通信模块，用于向移动管理网元发送截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理；接收移动管理网元发送的第一 NAS MAC，第一 NAS MAC 是对截短参数进行完整性计算得到的；向终端发送
15 第一 NAS MAC 和截短参数。

一种可能的设计中，通信装置还包括处理模块；处理模块，用于判断终端是否支持 ClIoT 5GS 优化特性；通信模块，具体用于在终端支持 ClIoT 5GS 优化特性的情况下，接入网设备向移动管理网元发送截短参数。

20 一种可能的设计中，处理模块，具体用于若终端的能力指示信息用于指示终端支持 ClIoT 5GS 优化特性，则确定终端支持 ClIoT 5GS 优化特性。

一种可能的设计中，处理模块，具体用于若终端使用的频点与 ClIoT 设备使用的频点相同，则确定终端支持 ClIoT 5GS 优化特性。

25 一种可能的设计中，处理模块，具体用于若终端发送的消息的类型与 ClIoT 设备发送的消息的类型相同，则确定终端支持 ClIoT 5GS 优化特性。

一种可能的设计中，通信模块，还用于接收终端发送的上行 RRC 消息；处理模块，具体用于在通信模块接收到终端发送的上行 RRC 消息之后，判断终端是否支持 ClIoT 5GS 优化特性。

一种可能的设计中，上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

30 一种可能的设计中，通信模块，还用于向移动管理网元发送保护指示信息和/或新鲜性参数，保护指示信息用于指示移动管理网元对截短参数进行安全保护，新鲜性参数用于对截短参数的完整性计算。

一种可能的设计中，所述通信模块，还用于接收所述终端发送的 RRC 重建请求消息，所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

35 一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第十四方面，提供一种通信装置，包括：通信模块，用于接收接入网设备发送的第一 NAS MAC 和截短参数，截短参数用于对终端的 5G-S-TMSI 进行截短处理；处理模块，用于根据 NAS 安全上下文，对截短参数进行完整性计算，生成第二 NAS MAC；根据第二 NAS MAC，校验第一 NAS MAC；存储模块，用于在第一 NAS MAC 通过校验的情况下，存储截短参数。

一种可能的设计中，存储模块，用于存储截短参数，包括：RRC 层存储截短参数。

一种可能的设计中，处理模块，还用于获得截短的 5G-S-TMSI，包括：RRC 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

一种可能的设计中，处理模块，还用于获得截短的 5G-S-TMSI，包括：RRC 层向 NAS 层发送截短参数；NAS 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI；NAS 层向 RRC 层发送截短的 5G-S-TMSI。

一种可能的设计中，存储模块，用于存储截短参数，包括：RRC 层向 NAS 层发送截短参数；NAS 层存储截短参数。

一种可能的设计中，处理模块，还用于获得截短的 5G-S-TMSI，包括：NAS 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI；NAS 层向 RRC 层发送截短的 5G-S-TMSI。

一种可能的设计中，处理模块，还用于获得截短的 5G-S-TMSI，包括：NAS 层向 RRC 层发送截短参数；RRC 层根据截短参数，对终端的 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

一种可能的设计中，所述通信模块，还用于向所述接入网设备发送 RRC 重建立请求消息，所述 RRC 重建立请求消息包括截短的 5G-S-TMSI。

一种可能的设计中，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI。所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

第十五方面，提供一种通信装置，包括处理器和通信接口，处理器用于执行计算机程序指令，使得通信装置实现第一方面至第七方面中任一方面所提供的任一种设计所涉及的截短参数的保护方法。

第十六方面，提供一种计算机可读存储介质，计算机可读存储介质存储有指令，当指令在计算机上运行时，使得计算机实现第一方面至第七方面中任一方面所提供的任一种设计所涉及的截短参数的保护方法。

第十七方面，提供一种计算机程序产品，该计算机程序产品包括指令，当计算机程序产品在计算机上运行时，使得计算机实现第一方面至第七方面中任一方面所提供的任一种设计所涉及的截短参数的保护方法。

第十八方面，提供一种芯片，该芯片包括处理器，当处理器执行计算机程序指令时，使得芯片实现第一方面至第七方面中任一种设计所涉及的截短参数的保护方法。

第十九方面，提供一种通信系统，该通信系统包括：移动管理网元和接入网设备，所述移动管理网元用于执行第一方面中任一种设计所涉及的截短参数的保护方法，所

述接入网设备用于执行第三方面中任一种设计所涉及的截短参数的保护方法。

第二十方面，提供一种通信系统，该通信系统包括移动管理网元和接入网设备，所述移动管理网元用于执行第五方面中任一种设计所涉及的截短参数的保护方法，所述接入网设备用于执行第六方面中任一种设计所涉及的截短参数的保护方法。

5 附图说明

- 图 1 为加密/解密的过程示意图；
- 图 2 为发送发给计算 MAC 的示意图；
- 图 3 为接收方计算 MAC 的示意图；
- 图 4 为现有技术中截短参数的配置流程的示意图；
- 10 图 5 为本申请实施例提供的一种 5G 网络的结构示意图；
- 图 6 为本申请实施例提供的一种协议栈的示意图；
- 图 7 为本申请实施例提供的一种装置的结构示意图；
- 图 8 为本申请实施例提供的一种截短参数的保护方法的流程图；
- 图 9 为本申请实施例提供的另一种截短参数的保护方法的流程图；
- 15 图 10 为本申请实施例提供的另一种截短参数的保护方法的流程图；
- 图 11 为本申请实施例提供的另一种截短参数的保护方法的流程图；
- 图 12 为本申请实施例提供的另一种截短参数的保护方法的流程图；
- 图 13 为本申请实施例提供的一种终端的结构示意图；
- 图 14 为本申请实施例提供的一种接入网设备的结构示意图；
- 20 图 15 为本申请实施例提供的一种移动管理网元的结构示意图。

具体实施方式

- 在本申请的描述中，除非另有说明，“/”表示“或”的意思，例如，A/B 可以表示 A 或 B。本文中的“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
- 25 三种情况。此外，“至少一个”是指一个或多个，“多个”是指两个或两个以上。“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并无限定一定不同。

- 需要说明的是，本申请中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。
- 30

- 在本申请的描述中，“指示”可以包括直接指示和间接指示，也可以包括显式指示和隐式指示。将某一信息（如下文所述的第一指示信息）所指示的信息称为待指示信息，则具体实现过程中，对所述待指示信息进行指示的方式有很多种。例如，可以
- 35 直接指示所述待指示信息，其中所述待指示信息本身或者所述待指示信息的索引等。又例如，也可以通过指示其他信息来间接指示所述待指示信息，其中该其他信息与所述待指示信息之间存在关联关系。又例如，还可以仅仅指示所述待指示信息的一部分，而所述待指示信息的其他部分则是已知的或者提前约定的。另外，还可以借助预先约定（例如协议规定）的各个信息的排列顺序来实现对特定信息的指示，从而在一定程

度上降低指示开销。

为了便于理解本申请的技术方案，下面先对本申请所涉及的术语进行简单介绍。

1、加密/解密

加密/解密：保护数据在传输过程中的机密性（因此又可以被称作机密性保护），
5 机密性是指无法被直接看出真实内容。加密保护一般可以使用密钥和加密算法对数据进行加密来实现。加密保护的具体方法可以参考 3GPP TS 33.401 f50 中 8.2 节或 33.501 f50 中 6.4.4 节标准相关描述，这里不再赘述。

示例性的，如图 1 所示，发送端的加密过程可以为：发送端可以将计数值(count)、
长度(length)、承载(bearer)、以及方向(direction)等参数输入 NEA 中，确定密
10 钥流(keystream)；之后，发送端根据密钥流和明文(plaintext)，确定密文(ciphertext)。

示例性的，如图 1 所示，接收端的解密过程可以为：接收端可以将 count、length、
bearer、以及 direction 等参数输入 NEA 中，确定密钥流；之后，接收端根据密钥流和
密文，确定明文。

2、完整性保护/校验

完整性保护/校验：完整性保护/校验用于判断消息在传递过程中，其内容是否被更
15 改，也可以用于作为身份验证，以确认消息的来源。完整性校验和保护需要使用消息
认证码(message authentication code, MAC)。完整性校验和保护的具体方法可以参考
第三代合作伙伴计划(3rd generation partnership project, 3GPP) TS 33.401 f50 中
8.1 节或 33.501 f50 中 6.4.3 节标准相关描述，这里不再赘述。

20 MAC 可以用于检查消息在传递过程中，其内容是否被更改；以及，MAC 可以用
于作为身份验证，以确认消息的来源。

如图 2 所示，发送端将密钥(key)、计数值(count)、长度(length)、承载(bearer)、
消息(message)、方向(direction)等参数输入演进分组系统完整性算法(evolved packet
system integrity algorithm, EIA)，可以得到完整性的消息认证码(message authentication
25 code integrity, MAC-I) 或者 NAS-MAC。

如图 3 所示，接收端将完整性保护密钥、count、length、bearer、message、direction
等参数输入 EIA，可以得到期望的完整性的消息认证码(excepted message authentication
code integrity, XMAC-I) 或者期望的非接入层消息认证码(excepted non-access stratum
message authentication code, XNAS-MAC)。

30 对于接收端来说，接收端可以将接收到的 MAC-I 与自身生成的 XMAC-I 进行比对，
以验证消息是否完整。若 MAC-I 与 XMAC-I 相同，则接收端确定接收到的 MAC-I 通
过验证，从而接收端能够确定发送端所发送的消息是完整的；若 MAC-I 与 XMAC-I
不相同，则接收端能够确定接收到的 MAC-I 未通过验证，从而接收端能够确定发送端
所发送的消息是不完整的。

35 3、安全上下文

安全上下文是指可以用于实现数据的安全保护（例如，加密/解密，和/或完整性保
护/校验）的信息。

安全上下文可以包括以下一项或者多项：根密钥、加密密钥、完整性保护密钥、
特定参数（比如 NAS Count）、密钥集标识(key set identifier, KSI)、安全算法、安

全指示（例如，是否开启加密的指示，是否开启完整性保护的指示、密钥使用期限的指示，密钥长度）等。

其中，加密密钥为发送端根据加密算法对明文进行加密以生成密文时输入的参数。若使用对称加密的方法，加密密钥和解密密钥是相同的。接收端可以根据相同的加密算法和加密密钥对密文进行解密。换句话说，发送端和接收端可以基于同一个密钥去加密和解密。

完整性保护密钥为发送端根据完整性保护算法对明文或密文进行完整性保护时输入的参数。接收端可以根据相同的完整性保护算法和完整性保护密钥对进行了完整性保护的数据进行完整性验证。

10 特定参数（比如 NAS Count）为发送端根据防重放保护算法对明文或密文进行防重放保护时输入的参数。接收端可以根据相同的防重放保护算法对进行了防重放保护的数据进行防重放验证。

安全算法即对数据进行安全保护时使用的算法。例如，加密算法、解密算法、完整性保护算法等。

15 在本申请实施例中，安全上下文可以分为 NAS 安全上下文和 AS 安全上下文。可以理解的是，NAS 安全上下文用于保护终端与核心网之间传输的信息。AS 安全上下文用于保护终端与基站之间传输的信息。

4、激活 NAS 安全

激活 NAS 安全包含激活 NAS 完整性保护和激活 NAS 加密保护。

20 激活 NAS 完整性保护：一旦激活 NAS 完整性保护，代表后续上行/下行 NAS 消息的完整性保护都需要根据当前的安全上下文的 NAS 完整性密钥和 NAS 完整性保护算法采取一致的处理。所有没有 NAS 完整性保护的消息都不被接受，需要被丢弃，但部分特殊的 NAS 消息可以除外，如附着请求、位置区更新请求、服务请求、控制面服务请求、认证请求、身份请求等。例如，用户设备激活 NAS 完整性保护后，每次发送上行 NAS 消息，都会对上行 NAS 消息根据当前的安全上下文的 NAS 完整性密钥和 NAS 完整性保护算法进行完整性保护；每次接收下行 NAS 消息，都会对下行 NAS 消息根据当前的安全上下文的 NAS 完整性密钥和 NAS 完整性保护算法进行完整性校验。移动管理网元激活 NAS 完整性保护后，每次收到上行 NAS 消息，都会对上行 NAS 消息根据当前的安全上下文的 NAS 完整性密钥和 NAS 完整性保护算法进行完整性校验，每次发送下行 NAS 消息，都会对下行 NAS 消息根据当前的安全上下文的 NAS 完整性密钥和 NAS 完整性保护算法进行完整性保护。

30 激活 NAS 加密保护：一旦激活 NAS 加密保护，代表后续对于上行/下行 NAS 消息的加密保护都需要根据当前的安全上下文的 NAS 加密密钥和 NAS 加密算法采取一致的处理。所有没有 NAS 加密保护的消息都不被接受，需要被丢弃。例如，用户设备激活 NAS 完整性保护后，每次发送上行 NAS 消息，都会对上行 NAS 消息根据当前的安全上下文的 NAS 加密密钥和 NAS 加密算法进行加密保护，每次接受下行 NAS 消息，都会对下行 NAS 消息根据当前的安全上下文的 NAS 加密密钥和 NAS 加密算法进行解密。移动管理网元激活 NAS 完整性保护后，每次收到上行 NAS 消息，都会对上行 NAS 消息根据当前的安全上下文的 NAS 加密密钥和 NAS 加密算法进行解密，每次发送下

行 NAS 消息，都会对下行 NAS 消息根据当前的安全上下文的 NAS 加密密钥和 NAS 加密算法进行加密保护。

5、5G-S-TMSI

第五代全局唯一的临时标识（5th generation-globally unique temporary identity, 5G-GUTI）是 AMF 分配给终端的。

5G-GUTI 的结构为：5G-GUTI=<MCC>+<MNC>+<AMF Region ID>+<AMF set ID>+<AMF Pointer>+<5G-TMSI>。

其中，移动国家码（mobile country code, MCC）为 3 位十进制数字，用于标识一个国家。

移动网络码（mobile network Code）为 2 或 3 位十进制数字，用于标识国家内运营商网络的代码。

AMF region ID 占用 8 个比特，用于标识一组 AMF 集合（set）。

AMF set ID 占用 10 个比特，用于标识一组 AMF，这一组 AMF 支持相同的网络切片。

AMF 指针（pointer）占用 6 个比特，用于标识一个 AMF。

第五代临时移动台标识（5th generation-temporary mobile subscriber identity, 5G-TMSI）占用 32 个比特，用于标识一个 AMF。

5G-S-TMSI 是 5G-GUTI 的低 48 位。5G-S-TMSI 的结构为：5G-S-TMSI=<AMF set ID>+<AMF Pointer>+<5G-TMSI>。

也就是说，5G-S-TMSI 包括 48 个比特，其中第一个比特到第十个比特用于表示 AMF set ID，第十一个比特到第十六个比特用于表示 AMF pointer，第十七个比特到第四十八个比特用于表示 5G-TMSI。

6、截短参数

截短参数用于对 5G-S-TMSI 进行截短处理。

例如，截短参数可以包括第一截短参数和第二截短参数。其中，第一截短参数用于对 AMF set ID 和 5G-TMSI 进行截短处理。第二截短参数用于对 AMF Pointer 和 5G-TMSI 进行截短处理。

为了便于说明，下文中将第一截短参数记为 n，第二截短参数记为 m。

需要说明的是，截短的 5G-S-TMSI=<截短的 AMF set ID>+<截短的 AMF Pointer>+<截短的 5G-TMSI>。

其中，截短的 AMF set ID 由原先的 AMF set ID 中最后 n 个比特组成。

截短的 AMF Pointer 由原先的 AMF Pointer 中最后 m 个比特组成。

截短的 5G-TMSI 由原先的 5G-TMSI 中最后 40-n-m 个比特组成。

举例来说，5G-TMSI=<0000001010(10bit)><000110(6bit)><000100...10(32bit)>。假设 n=5, m=3, 则截短的 5G-TMSI=<01010(5bit)><110(3bit)><000100...10(32bit)>。

需要说明的，接入网设备在接收到截短的 5G-TMSI 之后，可以通过补零的方式，将截短的 5G-TMSI 还原为完整的 5G-TMSI。

以上是对本申请实施例所涉及的术语的介绍，以下不再赘述。

非频繁小包传输的 CIoT 终端（例如电表）具有电池耐用的需求。例如，这一类终端要求电池可以使用 10 年。为满足电池耐用的需求，5G 技术设计了 CIoT 5GS 优化特性。CIoT 5GS 优化特性去掉了终端周期性上报测量报告的特征。因此，源基站无法获取信号数据，以指示终端执行切换流程。这样一来，使用控制面 CIoT 5GS 优化功能的终端在移动时无法像传统终端一样通过切换流程切换到另一个基站上。因此，对于使用控制面 CIoT 5GS 优化功能的终端，引入了重建流程以保障终端在移动过程中的会话连续性。

在重建流程中，终端上报的 RRC 消息需要携带终端的 5G-S-TMSI，以使得接入网设备可以根据 5G-S-TMSI 寻址到特定的 AMF，并使 AMF 根据 5G-S-TMSI 查找到终端的安全上下文。但是，RRC 消息的长度有限制，而 5G-S-TMSI 的长度超过 RRC 消息的最大长度，因此 RRC 消息无法携带完整的 5G-S-TMSI。因此，终端需要使用截短参数对 5G-S-TMSI 进行截短处理，以使得 RRC 消息携带截短的 5G-S-TMSI。

如图 4 所示，现有技术中，接入网设备为终端配置截短参数的流程包括以下步骤：

- S10、接入网设备预先配置 m 和 n。
- S11、终端与网络侧之间执行注册流程。
- S12、接入网设备向终端发送 RRC 重配置消息，该 RRC 重配置消息包括 m 和 n。
- S13、终端存储 m 和 n。
- S14、终端根据 m、n 和 5G-S-TMSI，获得截短的 5G-S-TMSI。
- 可选的，终端执行步骤 S14 的条件可以为：重建流程被触发。
- S15、终端向接入网设备发送 RRC 重建请求消息，RRC 重建请求消息包括截短的 5G-S-TMSI。

需要说明的是，RRC 重建请求消息最多可以承载 67 比特（bit）的信息。其中，RRC 重建请求消息需要预留至少 27bit 的空间给除了 5G-S-TMSI 之外的其他参数，因此 RRC 重建请求携带的截短的 5G-S-TMSI 不能超过 40bit。

- S16、接入网设备根据 m、n 以及截短后的 5G-GUTI，恢复出 5G-S-TMSI。

在图 4 所示的流程中，使用控制面 CIoT 5GS 优化功能的终端和接入网设备之间不会建立 AS 安全上下文。因此，接入网设备发送给使用控制面 CIoT 5GS 优化功能的终端的 RRC 消息未经过 AS 安全保护，因此 RRC 消息携带的截短参数存在被攻击者篡改的安全风险。

- 为了解决截短参数在传输过程中的存在安全风险的问题，本申请实施例提供一种截短参数的保护方法及装置，其具体内容参见下文。

本申请实施例提供的技术方案可以应用于各种通信系统，例如，5G 通信系统，未来演进系统或者多种通信融合系统等等。本申请提供的技术方案可以应用于多种应用场景，例如，机器对机器（machine to machine，M2M）、宏微通信、增强型移动互联网（enhanced mobile broadband，eMBB）、超高可靠超低时延通信（ultra-reliable & low latency communication，uRLLC）以及海量物联网通信（massive machine type communication，mMTC）等场景。这些场景可以包括但不限于：通信设备与通信设备之间的通信场景，网络设备与网络设备之间的通信场景，网络设备与通信设备之间的通信场景等。下文中均是以应用于网络设备和终端之间的通信场景中为例进行说明的。

此外，本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

5 如图 5 所示，为本申请实施例提供的技术方案所适用的 5G 网络的架构。5G 网络可以包括：终端、无线接入通信网络（radio access network, RAN）或者接入通信网络（access network, AN）（下文中将 RAN 和 AN 统称为（R）AN）、核心网（core network, CN）、以及数据网（data network, DN）。

其中，终端可以是一种具有无线收发功能的设备。所述终端可以有不同的名称，
10 例如用户设备（user equipment, UE）、接入终端、终端单元、终端站、移动站、移动台、远方站、远程终端、移动设备、无线通信设备、终端代理或终端装置等。终端可以被部署在陆地上，包括室内或室外、手持或车载；也可以被部署在水面上（如轮船等）；还可以被部署在空中（例如飞机、气球和卫星上等）。终端包括具有无线通信功能的手持式设备、车载设备、可穿戴设备或计算设备。示例性地，终端可以是手机
15 （mobile phone）、平板电脑或带无线收发功能的电脑。终端设备还可以是虚拟现实（virtual reality, VR）终端设备、增强现实（augmented reality, AR）终端设备、工业控制中的无线终端、无人驾驶中的无线终端、远程医疗中的无线终端、智能电网中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端等。本申请实施例中，用于实现终端的功能的装置可以是终端，也可以是能够支持终端实现该功能的装置，例如芯片系统。本申请实施例中，芯片系统可以由芯片构成，也可以包括芯片和其他分立器件。本申请实施例中，以用于实现终端的功能的装置是终端为例，描述本申请实施例提供的技术方案。

在本申请实施例中，终端可以为使用控制面 CIoT 5GS 优化功能的终端。使用 CIoT 5GS 优化功能的终端使用 NAS 消息的载荷（payload）在终端和 SMF 之间传输上行和
25 下行用户数据，而不需要建立 PDU 会话的用户面连接。使用 CIoT 5GS 优化功能的终端和 AMF 之间使用 NAS 安全上下文对用户数据进行完整性保护和加密。

需要说明的是，控制面 CIoT 5GS 优化，也可以记为 CIoT 5GS 控制面优化，本申请实施例不限于此。

接入网设备也可以称为基站。基站可以包括各种形式的基站，例如：宏基站，微
30 基站（也称为小站），中继站，接入点等。具体可以为：是无线局域网（wireless local area network, WLAN）中的接入点（access point, AP），全球移动通信系统（Global System for Mobile Communications, GSM）或码分多址接入（Code Division Multiple Access, CDMA）中的基站（Base Transceiver Station, BTS），也可以是宽带码分多址（Wideband Code Division Multiple Access, WCDMA）中的基站（NodeB, NB），还可以是 LTE
35 中的 eNB，或者中继站或接入点，或者车载设备、可穿戴设备以及未来 5G 网络中的下一代节点 B（the next generation node B, gNB）或者未来演进的公用陆地移动网（public land mobile network, PLMN）网络中的基站等。

基站，通常包括基带单元（baseband unit, BBU）、射频拉远单元（remote radio unit, RRU）、天线、以及用于连接 RRU 和天线的馈线。其中，BBU 用于负责信号调制。

RRU 用于负责射频处理。天线用于负责线缆上导行波和空气中空间波之间的转换。一方面，分布式基站大大缩短了 RRU 和天线之间馈线的长度，可以减少信号损耗，也可以降低馈线的成本。另一方面，RRU 加天线比较小，可以随地安装，让网络规划更加灵活。除了 RRU 拉远之外，还可以把 BBU 全部都集中起来放置在中心机房（central office, CO），通过这种集中化的方式，可以极大减少基站机房数量，减少配套设备，特别是空调的能耗，可以减少大量的碳排放。此外，分散的 BBU 集中起来变成 BBU 基带池之后，可以统一管理和调度，资源调配更加灵活。这种模式下，所有的实体基站演变成了虚拟基站。所有的虚拟基站在 BBU 基带池中共享用户的数据收发、信道质量等信息，相互协作，使得联合调度得以实现。

5 在一些部署中，基站可以包括集中式单元（centralized unit, CU）和分布式单元（distributed unit, DU）。基站还可以包括有源天线单元（active antenna unit, AAU）。CU 实现基站的部分功能，DU 实现基站的部分功能。比如，CU 负责处理非实时协议和服务，实现 RRC 层，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, 15 简称 RLC）、媒体接入控制（media access control, MAC）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 层信令或 PDCP 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，在本申请实施例中，接入网设备可以 20 为包括 CU 节点、DU 节点、AAU 节点中一项或多项的设备。此外，CU 可以划分为 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，在此不做限制。

一种可能的设计中，对于基站来说，还可以将 CU 的控制面（control plane, CP）和用户面（user plane, UP）分离，以不同实体来实现。也即，CU 可以分为 CU-CP 和 25 CU-UP。

核心网包括多个核心网网元（或者称为网络功能网元），例如：接入和移动性管理功能（access and mobility management function, AMF）网元、会话管理功能（session management function, SMF）网元、策略控制功能（policy control function, PCF）网元网元、用户面功能（user plane function, UPF）网元、应用层功能（application function） 30 网元、鉴权功能（authentication server function, AUSF）网元、以及统一数据管理（unified data management, UDM）网元。

此外，核心网还可以包括一些图 5 中未示出的网元，例如：安全锚功能（security anchor function, SEAF）网元、认证凭证库以及处理功能（authentication credential repository and processing function, ARPF），本申请实施例在此不予赘述。

35 AMF 网元主要负责移动性管理处理部分，例如：接入控制、移动性管理、附着与去附着以及 SMF 选择等功能。AMF 网元为终端中的会话提供服务的情况下，会为该会话提供控制面的存储资源，以存储会话标识、与会话标识关联的 SMF 标识等。

其中，终端通过下一代网络（Next generation, N）1 接口（简称 N1）与 AMF 通信，RAN 设备通过 N2 接口（简称 N2）与 AMF 通信，RAN 设备通过 N3 接口（简称

N3) 与 UPF 通信, UPF 通过 N6 接口 (简称 N6) 与 DN 通信。

AMF、SMF、UDM、AUSF、或者 PCF 等控制面网元也可以采用服务化接口进行交互。比如, 如图 5 所示, AMF 对外提供的服务化接口可以为 Namf; SMF 对外提供的服务化接口可以为 Nsmf; UDM 对外提供的服务化接口可以为 Nudm; PCF 对外提供的服务化接口可以为 Npcf, AUSF 对外提供的服务化接口可以为 Nausf; 在此不再一一描述。

如图 6 所示, 为本申请实施例提供的一种协议栈的示意图。如图 6 所示, 终端的协议栈至少包括: 非接入层、RRC 层、分组数据汇聚协议 (packet data convergence protocol, PDCP) 层、无线链路控制 (radio link control, RLC) 层、媒体接入控制 (media access control, MAC) 层、物理层 (PHY layer)。其中, RRC 层、PDCP 层、RLC 层、MAC 层、PHY 层均属于接入层。

其中, 非接入层是终端与核心网之间的功能层, 用于支持终端与核心网的网元 (例如移动管理网元) 之间的信令和数据传输。

RRC 层用于支持无线资源的管理、RRC 连接控制等功能。

对于其他的协议层, 例如 PDCP 层、RLC 层等, 其定义与功能可以参见现有技术的说明, 在此不再赘述。

可选的, 本申请实施例所提及的设备, 例如终端、移动管理网元、接入网设备等, 均可以由图 7 所示的装置来实现。

如图 7 所示, 该装置 100 包括至少一个处理器 101, 通信线路 102, 存储器 103 以及至少一个通信接口 104。

处理器 101 可以是一个通用中央处理器 (central processing unit, CPU), 微处理器, 特定应用集成电路 (application-specific integrated circuit, ASIC), 或一个或多个用于控制本申请方案程序执行的集成电路。

通信线路 102 用于在上述组件之间传送信息。

通信接口 104, 使用任何收发器一类的装置, 用于与其他设备或通信网络通信, 如以太网, 无线接入网 (radio access network, RAN), 无线局域网 (wireless local area networks, WLAN) 等。

存储器 103 可以是只读存储器 (read-only memory, ROM) 或可存储静态信息和指令的其他类型的静态存储设备, 随机存取存储器 (random access memory, RAM) 或者可存储信息和指令的其他类型的动态存储设备, 也可以是电可擦可编程只读存储器 (electrically erasable programmable read-only memory, EEPROM)、只读光盘 (compact disc read-only memory, CD-ROM) 或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式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。存储器可以是独立存在, 通过通信线路 102 与处理器相连接。存储器也可以和处理器集成在一起。

其中, 存储器 103 用于存储执行本申请方案的计算机执行指令, 并由处理器 101 来控制执行。处理器 101 用于执行存储器 103 中存储的计算机执行指令, 从而实现本申请实施例所提供的技术方案。

可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

在具体实现中，作为一种实施例，处理器 101 可以包括一个或多个 CPU，例如图 7 中的 CPU0 和 CPU1。

5 在具体实现中，作为一种实施例，装置 100 可以包括多个处理器，例如图 7 中的处理器 101 和处理器 107。这些处理器中的每一个可以是一个单核（single-CPU）处理器，也可以是一个多核（multi-CPU）处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

10 在具体实现中，作为一种实施例，装置 100 还可以包括输出设备 105 和输入设备 106。输出设备 105 和处理器 101 通信，可以以多种方式来显示信息。例如，输出设备 105 可以是液晶显示器（liquid crystal display, LCD），发光二极管（light emitting diode, LED）显示设备，阴极射线管（cathode ray tube, CRT）显示设备，或投影仪（projector）等。输入设备 106 和处理器 101 通信，可以以多种方式接收用户的输入。例如，输入设备 106 可以是鼠标、键盘、触摸屏设备或传感设备等。

15 下面结合说明书附图对本申请所提供的技术方案进行具体阐述。

为了降低截短参数在传输过程中的安全风险，本申请提供如下三个实施例。

其中，实施例一和实施例三可以应用于某个终端接入网络的场景下，实施例二应用于 AMF 对自身服务的终端进行截短参数更新的场景下。需要说明书的是，如下三个实施例所涉及的技术特征，可以互相参考，互相结合。例如，一个使用控制面 ClIoT 5GS 优化功能的终端 X 注册到网络中时，可以触发执行实施例一所述的方案，从而安全的获取截短参数。后续，网络侧的 AMF 也会根据实施例二所述的方法，主动对该终端 X 进行截短参数更新。

实施例一

25 如图 8 所示，为本申请实施例提供的一种截短参数的保护方法，该方法包括以下步骤：

S101、移动管理网元判断接入网络的终端是否符合预设条件。

其中，在 5G 网络中，移动管理网元可以为 AMF；在未来的演进系统中，移动管理网元可以为类似 AMF 的 NAS 安全终结点。在此统一说明，以下不再赘述。

30 在本申请实施例中，所述预设条件至少包括：终端使用控制面 ClIoT 5GS 优化功能。

可选的，预设条件包括以下情形：

情形一、预设条件为：终端使用控制面 ClIoT 5GS 优化功能。

35 基于情形一，步骤 S101 可以具体实现为：移动管理网元判断终端是否使用控制面 ClIoT 5GS 优化功能。若终端使用控制面 ClIoT 5GS 优化功能，则移动管理网元确定终端符合预设条件；若终端没有使用控制面 ClIoT 5GS 优化功能，则移动管理网元确定终端不符合预设条件。

在本申请实施例中，移动管理网元判断终端是否使用控制面 ClIoT 5GS 优化功能，包括以下实现方式：

实现方式一、移动管理网元根据终端上报的偏好的网络行为（preferred network

behaviour)，判断终端是否使用控制面 CIoT 5GS 优化功能。

其中，偏好的网络行为可以承载于终端发送的注册请求消息中。偏好的网络行为用于指示终端支持的网络功能。或者说，偏好的网络行为用于指示终端偏好使用的网络功能。例如，偏好的网络行为可以指示终端是否支持控制面 CIoT 5GS 优化功能，

5 是否支持用户面 CIoT 5GS 优化功能，是否支持 N3 数据传输，是否支持头压缩等。

也就是说，若终端上报的偏好的网络行为用于指示终端偏好使用控制面 CIoT 5GS 优化功能，且移动管理网元支持控制面 CIoT 5GS 优化功能，则移动管理网元可以确定终端使用控制面 CIoT 5GS 优化功能。

或者，若终端上报的偏好的网络行为用于指示终端偏好使用控制面 CIoT 5GS 优化功能，但移动管理网元不支持控制面 CIoT 5GS 优化功能，则移动管理网元可以确定终端不使用控制面 CIoT 5GS 优化功能。

或者，若终端上报的偏好的网络行为用于指示终端不偏好使用控制面 CIoT 5GS 优化功能，则移动管理网元确定终端不使用控制面 CIoT 5GS 优化功能。

实现方式二、移动管理网元根据终端的上下文，判断终端是否使用控制面 CIoT
15 5GS 优化功能。

也就是说，当终端的上下文指示终端使用控制面 CIoT 5GS 优化功能时，移动管理网元确定终端使用控制面 CIoT 5GS 优化功能。或者，当终端的上下文指示终端不使用控制面 CIoT 5GS 优化功能时，移动管理网元确定终端不使用控制面 CIoT 5GS 优化功能。

20 需要说明的是，若终端使用控制面 CIoT 5GS 优化功能，则终端与接入网设备之间不会建立 AS 安全上下文，因此截短参数不能按照现有技术的方式来传输，以避免被攻击者篡改。基于此，移动管理网元需要执行下述步骤 S102。

情形二、预设条件为：终端使用控制面 CIoT 5GS 优化功能，以及终端是初始注册到网络的终端。

25 基于情形二，步骤 S101 可以具体实现为：移动管理网元判断终端是否使用控制面 CIoT 5GS 优化功能，以及终端是否是初始注册到网络的终端。若终端使用控制面 CIoT 5GS 优化功能，且终端是初始注册到网络的终端，则移动管理网元确定终端符合预设条件。若终端不使用控制面 CIoT 5GS 优化功能，或者终端不是初始注册到网络的终端，则移动管理网元确定终端不符合预设条件。

30 在本申请实施例中，移动管理网元根据终端上报的注册类型，确定终端是否是初始注册到网络的终端。

其中，终端的注册类型可以承载于终端发送的注册请求消息中。终端的注册类型包括：初始注册、移动更新注册、周期性注册更新或者紧急注册。

35 也就是说，当终端的注册类型为初始注册时，移动管理网元可以确定终端是初始注册到网络的终端。或者，当终端的注册类型为移动更新注册、周期性注册更新或者紧急注册时，移动管理网元可以确定终端不是初始注册到网络的终端。

可选的，在注册流程中，预设条件可以采用情形二。

需要说明的是，截短参数不常变化，因此网络侧无需在终端的每一次注册流程中，均向终端发送截短参数。因此，对于使用控制面 CIoT 5GS 优化功能的终端来说，若

该终端是初始注册到网络的，移动管理网元执行下述步骤 S102，以保证该终端接收到正确的截短参数；若该终端不是初始注册到网络的，则说明该终端存储有截短参数，因此移动管理网元可以选择不执行下述步骤 S102，以节省信令开销。

情形三、预设条件为：终端使用控制面 ClIoT 5GS 优化功能，以及终端需要更新截短参数。

基于情形三，步骤 S101 可以具体实现为：移动管理网元判断终端是否使用控制面 ClIoT 5GS 优化功能，以及终端是否需要更新截短参数。若终端使用控制面 ClIoT 5GS 优化功能，且终端需要更新截短参数，则移动管理网元确定终端符合预设条件。若终端不使用控制面 ClIoT 5GS 优化功能，或者终端不需要更新截短参数，则移动管理网元确定终端不符合预设条件。

在本申请实施例中，移动管理网元判断终端是否需要更新截短参数，包括以下实现方式之一：

实现方式一、移动管理网元通过判断自身配置的截短参数以及终端的上下文中存储的截短参数是否相同，以判断终端是否需要更新截短参数。

需要说明的是，移动管理网元会在终端的上下文中存储终端当前使用的截短参数。也即，终端的上下文所存储的截短参数即为终端当前使用的截短参数。

也就是说，当移动管理网元配置的截短参数与终端的上下文中存储的截短参数不相同，移动管理网元可以确定终端需要更新截短参数。或者，当移动管理网元配置的截短参数与终端的上下文中存储的截短参数相同时，移动管理网元可以确定终端不需要更新截短参数。

实现方式二、移动管理网元通过判断当前时间是否在预设时间段内，以判断终端是否需要更新截短参数。

其中，预设时间段的起始时刻为移动管理网元确定截短参数发生更新的时刻，预设时间段的时长为预设时长。示例性的，预设时长可以为 1 分钟，也可以为 10 分钟。可选的，所述预设时长大于周期性注册更新的时间间隔。

例如，预设时长可以大于周期性注册更新的时间间隔的 2 倍。

需要说明的，网络侧可以为终端配置周期性注册更新的时间间隔，例如 10 分钟。在终端的等待时间超过该时间间隔后，终端会主动发起注册请求，以使网络侧获知终端仍在线。因此，网络侧将预设时长设置为大于周期性注册更新的时间间隔的 2 倍，则在预设时间内，移动管理网元可以保证所有在线的终端都可以更新截短参数。

也就是说，在当前时间位于预设时间段内的情况下，移动管理网元确定终端需要更新截短参数；在当前时间不位于预设时间段内的情况下，移动管理网元确定终端不需要更新截短参数。

可选的，在截短参数发生更新的场景下，预设条件可以采用情形三。

需要说明的是，移动管理网元更新截短参数的方式可以参考下文中步骤 S401 的描述，在此不予赘述。

需要说明的是，无论终端是否存储有截短参数，在网络侧更新截短参数的情况下，网络侧均需要向终端发送更新后的截短参数，以避免终端使用未更新的截短参数，获得错误的截短的 5G-S-TMSI。因此，对于使用控制面 ClIoT 5GS 优化功能的终端来说，

在移动管理网元确定终端需要更新截短参数的情况下，移动管理网元执行下述步骤 S102，以保证终端可以获取到最新的截短参数，进而保证终端可以正常接入网络；在移动管理网元确定终端不需要更新截短参数的情况下，移动管理网元可以不执行下述步骤 S102，以节省信令开销。

- 5 需要说明的是，上述情形一至情形三仅是对预设条件的示例，本申请实施例不限于此。

S102、在终端符合预设条件的情况下，移动管理网元向终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，所述下行 NAS 消息包括截短参数。

- 10 可选的，移动管理网元可以预先存储截短参数；或者，移动管理网元从接入网设备获取到截短参数。

其中，上述 NAS 安全保护至少包括完整性保护。可选的，NAS 安全保护还包括加密保护。

可以理解的是，由于该下行 NAS 消息经过 NAS 安全保护，因此下行 NAS 消息中的截短参数也经过 NAS 安全保护，从而可以保证截短参数的安全性。

- 15 需要说明的是，下行 NAS 消息可以为新增的信令，也可以复用现有流程中信令。例如，在注册流程中，下行 NAS 消息可以为注册接受（registration accept）消息。又例如，在服务请求流程中，下行 NAS 消息可以为服务接受（servers accept）消息。

S103、终端对下行 NAS 进行解安全保护。

- 20 其中，当下行 NAS 消息经过的 NAS 安全保护为完整性保护时，上述解安全保护为：完整性校验。或者，当下行 NAS 消息经过完整性保护和加密保护时，上述解安全保护为完整性校验和解密。

S104、终端在成功对下行 NAS 消息解安全保护之后，存储截短参数。

- 25 作为一种可能的实现方式，终端的 NAS 层在成功对下行 NAS 消息解安全保护之后，终端的 NAS 层存储截短参数。

作为另一种可能的实现方式，终端的 NAS 层在成功对下行 NAS 消息解安全保护之后，终端的 NAS 层向终端的 RRC 层发送截短参数，终端的 RRC 层存储截短参数。

- 30 基于图 8 所示的技术方案，由于预设条件至少包括：终端使用控制面 CIoT 5GS 优化功能，因此终端符合预设条件，说明终端使用控制面 CIoT 5GS 优化功能。移动管理网元在确定终端使用控制面 CIoT 5GS 优化功能的情况下，移动管理网元通过向终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，以保证截短参数在传输过程中接受过 NAS 安全保护。这样一来，保证截短参数不被篡改和伪造，从而防止终端被攻击者发起拒绝服务攻击，进而保证终端能够正常接入到网络中。

下面结合具体应用场景来说明图 8 所示的技术方案。

- 35 场景一、移动管理网元预先存储截短参数。

基于场景一，如图 9 所示，为本申请实施例提供的一种截短参数的保护方法，该方法包括以下步骤：

S200、移动管理网元预先存储截短参数。

可选的，工作人员可以通过网管系统向移动管理网元配置截短参数，以使得移动

管理网元可以预先存储截短参数。

一种可能的设计中，截短参数可以是 PLMN 粒度的，也可以是区域粒度的。也就是说，网管系统所配置的截短参数可以适用于整个 PLMN，或者仅适用于某个区域。

本申请实施例对移动管理网元如何预先配置截短参数的具体实现方式不作限定。

- 5 S201、终端向移动管理网元发送上行 NAS 消息，以使得移动管理网元接收终端发送的上行 NAS 消息。

示例性的，该上行 NAS 消息可以为注册请求消息、服务请求消息等，本申请实施例不限于此。

- 10 需要说明的是，注册请求消息可以包括注册类型（5GS registration type）和偏好的网络行为。

S202、终端和移动管理网元之间激活 NAS 安全。

- 示例性的，以上行 NAS 消息为注册请求消息为例，在移动管理网元接收到注册请求消息之后，移动管理网元对终端进行认证和密钥协商（authentication and key agreement, AKA）流程。之后，在认证成功之后，移动管理网元和终端之间通过 NAS 安全模式命令（security mode command, SMC）流程激活终端和移动管理网元之间的 NAS 安全上下文。
- 15

示例性的，以上行 NAS 消息为服务请求消息为例，在移动管理网元接收到服务请求消息之后，移动管理网元对服务请求消息进行完整性校验；在服务请求消息通过完整性校验之后，移动管理网元激活终端和移动管理网元之间的 NAS 安全上下文。

- 20 S203-S206、与步骤 S101-S104 相似，其具体描述可参见图 8 所示的实施例，在此不再赘述。

可选的，当上行 NAS 消息为注册请求消息时，下行 NAS 消息为注册接受消息。

可选的，当上行 NAS 消息为服务请求消息时，下行 NAS 消息为服务接受消息。

- 基于图 9 所示的实施例，在一些流程中，例如注册流程或者服务请求流程，移动管理网元可以主动判断终端是否符合预设条件；在终端符合预设条件的情况下，移动管理网元向终端发送经过 NAS 安全保护的截短参数，以便于终端在后续流程中可以使用到截短参数。
- 25

场景二、接入网设备预先存储截短参数。

- 基于场景二，如图 10 所示，为本申请实施例提供的一种截短参数的保护方法，该方法包括以下步骤：
- 30

S300、接入网设备预先存储截短参数。

需要说明的是，接入网设备一般会预先配置截短参数，以便于接入网设备根据截短参数以及截短的 5G-S-TMSI 恢复出完整的 5G-S-TMSI。

- 可选的，工作人员可以通过网管系统向接入网设备配置截短参数，以使得接入网设备可以预先存储截短参数。
- 35

一种可能的设计中，截短参数可以是 PLMN 粒度的，也可以是区域粒度的。也就是说，网管系统所配置的截短参数可以适用于整个 PLMN，或者仅适用于某个区域。

本申请实施例对接入网设备如何预先配置截短参数的具体实现方式不作限定。

S301、终端向接入网设备发送上行 RRC 消息。

示例性的,上行RRC消息可以为RRC建立请求消息,或者RRC建立完成消息,本申请实施例不限于此。

可选的,除了上行RRC消息之外,终端还可以向接入网设备发送上行NAS消息,以便于接入网设备将该上行NAS消息转发给移动管理网元。示例性的,上行NAS消息可以为注册请求消息,或者服务请求消息,本申请实施例不限于此。

一种可能的设计中,上行NAS消息可以作为上行RRC消息的载荷。例如,上行RRC消息包括NAS容器(container),该NAS container包含上行NAS消息。这样一来,终端通过向接入网设备发送上行RRC消息,从而实现将上行RRC消息和上行NAS消息一同传输给网络侧的目的。

另一种可能的设计中,终端向接入网设备分别发送上行NAS消息和上行RRC消息。

S302、接入网设备判断终端是否支持CIoT 5GS优化特性。

其中,CIoT 5GS优化特性包括用户面CIoT 5GS优化功能,和/或控制面CIoT 5GS优化功能。

也即,终端支持CIoT 5GS优化特性,说明终端可能支持用户面CIoT 5GS优化功能,和/或控制面CIoT 5GS优化功能。

可选的,步骤S302至少采用以下实现方式之一:

实现方式一、在上行RRC消息包括能力指示的情况下,接入网设备根据能力指示,判断终端是否支持CIoT 5GS优化特性。也就是说,若能力指示用于指示终端支持CIoT 5GS优化特性,则接入网设备确定终端支持CIoT 5GS优化特性。

可选的,若能力指示未指示终端支持CIoT 5GS优化特性,则接入网设备确定终端不支持CIoT 5GS优化特性。

实现方式二、接入网设备根据终端接入频点,判断终端是否支持CIoT 5GS优化特性。也就是说,若终端接入CIoT设备使用的频点,则接入网设备确定终端支持CIoT 5GS优化特性。

可选的,若终端未接入CIoT设备使用的频点,则接入网设备确定终端不支持CIoT 5GS优化特性。

实现方式三、接入网设备根据终端发送的消息的类型,判断终端是否支持CIoT 5GS优化特性。也就是说,若终端发送的消息的类型与CIoT设备专用的消息的类型相同,则接入网设备确定终端支持CIoT 5GS优化特性。

可选的,若终端发送的消息的类型与CIoT设备专用的消息的类型不相同,则接入网设备确定终端不支持CIoT 5GS优化特性。

可以理解的是,上述实现方式一至实现方式三仅是步骤S302的具体实现方式的示例。在实际应用中,上述实现方式一、实现方式二和/或实现方式三可以相互结合使用。

需要说明的是,若接入网设备确定终端支持CIoT 5GS优化特性,则接入网设备执行下述步骤S303。

S303、接入网设备向移动管理网元发送N2消息,以使得移动管理网元接收接入网设备发送的N2消息。

其中,N2消息包括截短参数。

可选的，N2 消息可以是初始 UE 消息（Initial UE message）。

可选的，在终端还向接入网设备发送上行 NAS 消息的情况下，N2 消息携带上行 NAS 消息。

5 S304-S307、与步骤 S101-S04 相似，其具体描述可参见图 8 所示的实施例，在此不再赘述。

基于图 10 所示的实施例，在接入网设备存储截短参数的情况下，接入网设备会判断接入的终端是否支持 CIoT 5GS 优化特性；之后，在终端支持 CIoT 5GS 优化特性的情况下，接入网设备会向移动管理网元发送截短参数，以便于在后续的流程中，移动管理网元可以向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全保护的截短参数。在上述过程中，移动管理网元可以从接入网设备获取截短参数，因此移动管理网元无需预先配置截短参数，从而降低截短参数的配置复杂度。

实施例二

如图 11 所示，为本申请实施例提供的一种截短参数的保护方法，该方法包括以下步骤：

15 S401、移动管理网元更新截短参数。

可选的，步骤 S401 可以包括以下实现方式之一：

实现方式一、移动管理网元根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数。

例如，若根据当前的截短参数进行截短的 AMF set ID 和/或 AMF pointer 无法表示所有已分配的移动管理网元，则移动管理网元需要调整截短参数。

举例来说，对于当前的截短参数来说，n 设置为 5，m 设置为 3，则截短的 AMF set ID 仅有 5 个比特，截短的 AMF set ID 可以指示的 AMF set 的总数为 32；截短的 AMF pointer 仅有 3 个比特，截短的 AMF pointer 可以指示的 pointer 的总数为 8。若当前 AMF set 的数目为 14，pointer 的数目为 9，则移动管理网元需要更新截短参数。可选的，对于更新后的截短参数来说，n 可以调整为 4，m 可以调整为 4。这样一来，截短后的 AMF set ID 可以指示的 AMF set 的总数为 16，截短后的 AMF pointer 可以指示的 pointer 的总数为 16。

实现方式二、移动管理网元根据网络管理系统的指令，更新截短参数。

30 可选的，上述网络管理系统可以为操作维护管理（operation administration and maintenance, OAM）系统。

实现方式三、移动管理网元接收接入网设备发送的更新后的截短参数。

需要说明的是，接入网设备可以根据网络管理系统的指令，更新截短参数。

S402、移动管理网元查找到使用控制面 CIoT 5GS 优化功能的终端。

35 作为一种可能的实现方式，移动管理网元存储有终端的上下文，终端的上下文中包括对应的终端是否是使用控制面 CIoT 5GS 优化功能的终端的指示信息。移动管理网元根据其存储的多个终端的上下文中，确定使用控制面 CIoT 5GS 优化功能的终端。

可以理解的是，使用控制面 CIoT 5GS 优化功能的终端的数量可能为一个或者多个。

S403、移动管理网元向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全

上下文进行 NAS 安全保护的下行 NAS 消息。

其中，所述下行 NAS 消息包括更新后的截短参数。

对于任意一个使用控制面 CIoT 5GS 优化功能的终端来说，移动管理网元向该终端发送下行 NAS 消息，包括以下实现方式之一：

- 5 实现方式一、若使用控制面 CIoT 5GS 优化功能的终端处于连接（CONNECTED）态，则移动管理网元可以直接向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息。

可选的，基于实现方式一，下行 NAS 消息可以为 UE 配置更新命令（UE Configuration Update Command）消息。

- 10 实现方式二、若使用控制面 CIoT 5GS 优化功能的终端处于非连接态，则移动管理网元等待该终端进入连接态；在终端进入连接态并且激活 NAS 安全之后，移动管理网元向该终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息。

在本申请实施例中，非连接态可以为空闲（idle）态或者 RRC 不活跃（inactive）态。

- 15 需要说明的是，处于非连接态的终端可以通过主动发起服务请求消息，以进入连接态。

可选的，基于实现方式二，下行 NAS 消息可以为服务接受消息，或者 UE 配置更新命令消息。

- 20 实现方式三、若使用控制面 CIoT 5GS 优化功能的终端处于非连接态，则移动管理网元主动寻呼该终端，以触发该终端进入连接态；在终端进入连接态并且激活 NAS 安全之后，移动管理网元向该终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息。

可选的，基于实现方式三，下行 NAS 消息可以为服务接受消息，或者 UE 配置更新命令（UE Configuration Update Command）消息。

- 25 需要说明的是，当终端处于非连接态时，终端并不需要截短 5G-S-TMSI，因此非连接态下的终端并不需要立即更新截短参数。这种情况下，移动管理网元在等待终端恢复到连接态后，为终端更新截短参数，可以防止移动管理网元在同一时间内大量向终端发送 NAS 信令，从而造成信令拥塞。

- 30 另外，基于实现方式三，移动管理网元不主动唤醒处于非连接态的终端，有利于节省终端的功耗。

S404-S405、与步骤 S103-S104 相似，其具体描述可参考图 8 所示的实施例，在此不再赘述。

- 35 基于图 11 所示的技术方案，移动管理网元在更新截短参数之后，移动管理网元主动向使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全保护的更新后的截短参数，以使得该终端能够获取到更新后的截短参数，避免该终端因使用错误的截短参数而导致终端不能正常接入网络的情况发生。

实施例三

如图 12 所示，为本申请实施例提供的一种截短参数的保护方法，该方法包括以下步骤：

S500-S503、与步骤 S300-S303 相似，其具体描述可以参考图 10 所示的实施例，在此不再赘述。

可选的，除了截短参数之外，接入网设备还可以向移动管理网元发送新鲜性参数和/或保护指示信息。

- 5 其中，新鲜性参数用于截短参数的完整性计算，新鲜性参数用于保证两次生成的 NAS MAC 不同。示例性的，新鲜性参数可以为下行 PDCP 计数值（count）。

保护指示信息用于指示移动管理网元对截短参数进行安全保护。

S504、移动管理网元根据 NAS 安全上下文，对截短参数进行完整性计算，生成第一 NAS MAC。

- 10 作为一种可能的实现方式，当移动管理网元接收到截短参数，则移动管理网元对截短参数进行完整性计算，生成第一 NAS MAC。

作为另一种可能的实现方式，当移动管理网元接收到截短参数和保护指示信息时，移动管理网元对截短参数进行完整性计算，生成第一 NAS MAC。当移动管理网元接收到截短参数，未接收到保护指示信息时，移动管理网元不对截短参数进行完整性计算。

- 15 可选的，移动管理网元根据完整性保护密钥、截短参数、以及完整性保护算法，生成第一 NAS MAC。

- 20 可选的，在接入网设备向移动管理网元发送新鲜性参数的情况下，移动管理网元根据完整性保护密钥、截短参数、完整性保护算法、以及新鲜性参数，生成第一 NAS MAC。

S505、移动管理网元向接入网设备发送第一 NAS MAC，以使得接入网设备接收移动管理网元发送的第一 NAS MAC。

S506、接入网设备向终端发送截短参数以及第一 NAS MAC，以使得终端接收接入网设备发送的截短参数以及第一 NAS MAC。

- 25 其中，截短参数以及第一 NAS MAC 可以承载于下行 RRC 消息中。

可选的，下行 RRC 消息中还携带新鲜性参数指示，新鲜性参数指示可以是下行 PDCP COUNT 的部分比特位。

示例性的，下行 RRC 消息可以为 RRC 重配置消息，本申请实施例不限于此。

- 30 S507、终端根据 NAS 安全上下文，对截短参数进行完整性计算，生成第二 NAS MAC。

可选的，终端根据完整性保护密钥、截短参数、以及完整性保护算法，生成第二 NAS MAC。

可选的，在终端还接收到接入网设备发送的新鲜性参数指示的情况下，终端根据完整性保护密钥、截短参数、新鲜性参数、以及完整性保护算法，生成第二 NAS MAC。

- 35 需要说明的是，在终端接收到新鲜性参数指示之后，终端可以根据新鲜性参数指示，获得新鲜性参数。例如，终端根据下行 PDCP COUNT 的部分比特位，恢复出完整的下行 PDCP COUNT。

S508、终端根据第二 NAS MAC，对第一 NAS MAC 进行校验。

作为一种可能的实现方式，终端判断第二 NAS MAC 与第一 NAS MAC 是否相同。

若第一 NAS MAC 和第二 NAS MAC 相同，则终端确定第一 NAS MAC 通过校验。若第一 NAS MAC 和第二 NAS MAC 不相同，则终端确定第一 NAS MAC 未通过校验。

S509、在第一 NAS MAC 通过校验之后，终端存储截短参数。

作为一种可能的实现方式，在第一 NAS MAC 通过校验之后，终端的 RRC 层存储截短参数。

作为另一种可能的实现方式，在第一 NAS MAC 通过校验之后，终端的 RRC 层向终端的 NAS 层发送截短参数；之后，终端的 NAS 层存储截短参数。

基于图 12 所示的技术方案，接入网设备在需要向终端发送截短参数的情况下，先向移动管理网元发送截短参数，以获取截短参数对应的第一 NAS MAC；之后，接入网设备向终端发送截短参数以及第一 NAS MAC。这样一来，终端能够通过第一 NAS MAC，验证截短参数是否被攻击者篡改，从而保证截短参数的完整性。在终端获取到正确的截短参数的情况下，终端可以正常接入网络。

对于使用控制面 CIoT 5GS 优化功能的终端来说，终端在发生无线链路失败（radio link failure, RLF）的情况下，终端可能会触发 RRC 连接重建立流程。在 RRC 连接重建立流程中，终端需要向目标接入网设备发送 RRC 重建立请求（RRC Reestablishment Request）消息，该 RRC 重建立请求消息携带截短的 5G-S-TMSI。

因此，在 RRC 连接重建立流程中，终端需要获得截短的 5G-S-TMSI。

可选的，终端获得截短的 5G-S-TMSI，包括以下实现方式之一：

实现方式一、在终端的 RRC 层负责存储截短参数的情况下，当终端需要使用截短的 5G-S-TMSI 时，终端的 RRC 层根据截短参数，对 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

实现方式二、在终端的 RRC 层负责存储截短参数的情况下，当终端需要使用截短的 5G-S-TMSI 时，终端的 RRC 层向终端的 NAS 层发送截短参数；终端的 NAS 层根据截短参数，对 5G-S-TMSI 进行截短处理，得到截短的 5G-S-TMSI；终端的 NAS 层向终端的 RRC 层发送截短的 5G-S-TMSI。

实现方式三、在终端的 NAS 层负责存储截短参数的情况下，当终端需要使用截短的 5G-S-TMSI 时，终端的 NAS 层根据截短参数，对 5G-S-TMSI 进行截短处理，得到截短的 5G-S-TMSI；终端的 NAS 层向终端的 RRC 层发送截短的 5G-S-TMSI。

实现方式四、在终端的 NAS 层负责存储截短参数的情况下，当终端需要使用截短的 5G-S-TMSI 时，终端的 NAS 层向终端的 RRC 层发送截短参数；之后，终端的 RRC 层根据截短参数，对 5G-S-TMSI 进行截短处理，获得截短的 5G-S-TMSI。

可以理解的是，终端所存储的截短参数是终端通过上述图 8 至图 12 中任意一图所示的技术方案来获得的。

下面具体说明使用控制面 CIoT 5GS 优化功能的终端的 RRC 连接重建立流程。

由于使用控制面 CIoT 5GS 优化功能的终端没有可用的 AS 安全上下文，因此，为了保护重建立流程，终端的 AS 层触发 NAS 层提供 UL_NAS_MAC 和 XDL_NAS_MAC。UL_NAS_MAC 表示终端请求重新建立 RRC 连接，XDL_NAS_MAC 用于表示终端正在与真实网络通话。

需要说明的是，终端将 key 设置为完整性密钥（KNASint），将 count 设置为上行

NAS count, 将 DIRECTION 设置为 0, 将 message 设置为目标小区标识 (cell ID) 和除了 NAS count 的 LSB 以及 UL_NAS_MAC 之外的整个 RRC 重建请求消息;之后, 终端将这些参数(例如 key、message 等)输入当前使用的完整性算法,生成 NAS MAC。

其中, NAS MAC 的前 16 位比特构成 UL_NAS_MAC, NAS MAC 的后 16 位比特
5 构成 XDL_NAS_MAC。

之后, 终端向目标接入网设备发送 RRC 重建请求消息, 该 RRC 重建请求消息包括截短的 5G-S-TMSI, 和 NAS count 的 5 个最低有效位。NAS count 的最低有效位用于计算 NAS MAC。

目标接入网设备基于 RRC 重建请求消息中的截短的 5G-S-TMSI, 以及本地配置的截短参数 (m 和 n), 恢复出完整的 5G-S-TMSI。目标接入网设备可以基于完整的 5G-S-TMSI, 确定出为终端服务的移动管理网元。并且, 目标接入网设备向该移动管理网元发送 5G-S-TMSI、目标 cell-ID 以及除了截短的 5G-S-TMSI 之外的整个 RRC 重建请求消息。
10

移动管理网元使用与 NAS 连接标识符 “0x01” 相关联的 NAS count 的 LSB, 来估计完整的上行 NAS count。之后, 移动管理网元使用该估计出的上行 NAS count, 来计算 XNAS-MAC。
15

移动管理网元比较 UL_NAS_MAC 与 XNAS-MAC 的前 16 位比特是否相同。在 UL_NAS_MAC 与 XNAS-MAC 的前 16 位比特相同的情况下, 移动管理网元确定真正的终端发送了 RRC 重建请求消息。

之后, 移动管理网元向目标接入网设备发送连接建立指示 (connection establishment indication) 消息, 该连接建立指示消息包括 DL_NAS_MAC。需要说明的是, DL_NAS_MAC 是 XNAS-MAC 的后 16 位比特。
20

接入网设备向终端发送 RRC 重建 (RRC Reestablishment) 消息, 该 RRC 重建消息包括 DL_NAS_MAC。

25 终端检查接收到的 DL_NAS_MAC 与 XDL_NAS_MAC 是否相同。如果 DL_NAS_MAC 与 XDL_NAS_MAC 相同, 则终端完成 RRC 连接重建过程。

上述主要从每一个网元之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是, 每一个网元, 例如终端、接入网设备、以及移动管理网元, 为了实现上述功能, 其包含了执行每一个功能相应的硬件结构或软件模块, 或两者结合。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。
30

35 本申请实施例可以根据上述方法示例对接入网设备、移动管理网元和终端进行功能模块的划分, 例如, 可以对应每一个功能划分每一个功能模块, 也可以将两个或两个以上的功能集成在一个处理模块中。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, 本申请实施例中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。下面以

采用对应每一个功能划分每一个功能模块为例进行说明：

图 13 为本申请实施例提供的一种终端的结构示意图。如图 13 所示，该终端包括：通信模块 201、处理模块 202 和存储模块 203。通信模块 201 用于支持终端执行图 8 中的步骤 S102，图 9 中的步骤 S201 和 S204，图 10 中的步骤 S301 和 S305，图 11 中的步骤 S403，图 12 中的步骤 S501 和 S506，和/或本申请实施例中终端需要执行的其他通信操作。处理模块 202 用于支持终端执行图 8 中的步骤 S103，图 9 中的步骤 S202 和 S205，图 10 中的步骤 S306，图 11 中的步骤 S404，图 12 中的步骤 S507 和 S208，和/或本申请实施例中终端需要执行的其他处理操作。存储模块 203 用于支持终端执行图 8 中的步骤 S104，图 9 中的步骤 S206，图 10 中的步骤 S307，图 11 中的步骤 S405，图 12 中的步骤 S509，和/或本申请实施例中终端需要执行的其他存储操作。

作为一个示例，结合图 7 所示的装置，图 13 中的处理模块 202 可以由图 7 中的处理器 101 来实现，图 13 中的通信模块 201 可以由图 7 中的通信接口 104 来实现，图 13 中的存储模块 203 可以由图 7 中的存储器 103 来实现，本申请实施例对此不作任何限制。

图 14 为本申请实施例提供的一种接入网设备的结构示意图。如图 14 所示，该接入网设备包括通信模块 301、处理模块 302 和存储模块 303。通信模块 301 用于支持接入网设备执行图 10 中的步骤 S301 和 S303，图 12 中的步骤 S501、S503、S505 以及 S506，和/或本申请实施例中接入网设备需要执行的其他通信操作。处理模块 302 用于支持接入网设备执行图 10 中的步骤 S302，图 12 中的步骤 S502，和/或本申请实施例中接入网设备需要执行的其他处理操作。存储模块 303 用于支持接入网设备执行图 10 中的步骤 S300，图 12 中的步骤 S500，和/或本申请实施例中接入网设备需要执行的其他存储操作。

作为一个示例，结合图 7 所示的装置，图 14 中的处理模块 302 可以由图 7 中的处理器 101 来实现，图 14 中的通信模块 301 可以由图 7 中的通信接口 104 来实现，图 14 中的存储模块 303 可以由图 7 中的存储器 103 来实现，本申请实施例对此不作任何限制。

图 15 为本申请实施例提供的一种移动管理网元的结构示意图。如图 15 所示，该移动管理网元包括通信模块 401、处理模块 402 和存储模块 403。通信模块 401 用于支持移动管理网元执行图 8 中的步骤 S102，图 9 中的步骤 S201 和 S204，图 10 中的步骤 S303 和 S305，图 11 中的步骤 S403，图 12 中的步骤 S503 和 S505，和/或本申请实施例中移动管理网元需要执行的其他通信操作。处理模块 402 用于支持移动管理网元执行图 8 中的步骤 S101，图 9 中的步骤 S202 和 S203，图 10 中的步骤 S304，图 11 中的步骤 S401 和 S402，图 12 中的步骤 S504，和/或本申请实施例中移动管理网元需要执行的其他处理操作。存储模块 403 用于支持移动管理网元执行图 9 中的步骤 S200，和/或本申请实施例中移动管理网元需要执行的其他存储操作。

作为一个示例，结合图 7 所示的装置，图 15 中的处理模块 402 可以由图 7 中的处理器 101 来实现，图 15 中的通信模块 401 可以由图 7 中的通信接口 104 来实现，图 15 中的存储模块 403 可以由图 7 中的存储器 103 来实现，本申请实施例对此不作任何限制。

本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机指令；当所述计算机可读存储介质在计算机上运行时，使得该计算机执行本申请实施例所提供的截短参数的保护方法。

5 本申请实施例还提供了一种包含计算机指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行本申请实施例提供的截短参数的保护方法。

本申请实施例提供一种芯片，该芯片包括处理器，该处理器执行指令时，使得该芯片可以执行本申请实施例提供的截短参数的保护方法。

应理解，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、服务器或者数据中心通过有线（例如同轴电缆、光纤、数字用户线）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以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、或者半导体介质（例如固态硬盘）等。

15 通过以上的实施方式的描述，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，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。

20 应该理解到，在本申请所提供的几个实施例中，所揭露的装置和方法，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，所述模块或单元的划分，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装置，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。

25 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一个物理单元或多个物理单元，即可以位于一个地方，或者也可以分布到多个不同地方。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。

30 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。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

35 所述集成的单元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，可以存储在一个可读存储介质中。基于这样的理解，本申请实施例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全部或部分可以以软件产品的形式体现出来，该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个设备（可以是单片机，芯片等）或处理器（processor）执行本申请各个实施例所述方法的全部或部分步骤。

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

何在本申请揭露的技术范围内的变化或替换，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、一种截短参数的保护方法，其特征在于，所述方法包括：
移动管理网元判断终端是否符合预设条件，所述预设条件包括所述终端使用控制面蜂窝物联网 CIoT 第五代系统 5GS 优化功能；
- 5 在所述终端符合预设条件的情况下，所述移动管理网元向所述终端发送经过非接入层 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，所述下行 NAS 消息包括截短参数，所述截短参数用于对所述终端的第五代系统架构演进临时移动台标识符 5G-S-TMSI 进行截短处理。
- 2、根据权利要求 1 所述的方法，其特征在于，所述截短参数是所述移动管理网元
10 预先存储的。
- 3、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：
所述移动管理网元接收接入网设备发送的所述截短参数。
- 4、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述移动管理网元判断终端是否符合预设条件，包括：
- 15 所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能；
若所述终端使用控制面 CIoT 5GS 优化功能，则所述移动管理网元确定所述终端符合预设条件；
若所述终端没有使用控制面 CIoT 5GS 优化功能，则所述移动管理网元确定所述终端不符合预设条件。
- 20 5、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述预设条件还包括：所述终端是初始注册到网络的终端；
所述移动管理网元判断终端是否符合预设条件，包括：
所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能，以及所述终端是否是初始注册到网络的终端；
- 25 若所述终端使用控制面 CIoT 5GS 优化功能且所述终端是初始注册到网络中的终端，则所述移动管理网元确定所述终端符合预设条件；
若所述终端没有使用控制面 CIoT 5GS 优化功能或者所述终端不是初始注册到网络中的终端，则所述移动管理网元确定所述终端不符合预设条件。
- 6、根据权利要求 5 所述的方法，其特征在于，所述移动管理网元判断所述终端是否
30 是初始注册到网络的终端，包括：
所述移动管理网元根据所述终端上报的注册类型，确定所述终端是初始注册到网络的终端。
- 7、根据权利要求 1 至 3 任一项所述的方法，其特征在于，所述预设条件还包括：所述终端需要更新截短参数；
- 35 所述移动管理网元判断终端是否符合预设条件，包括：
所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能，以及所述终端是否需要更新截短参数；
若所述终端使用控制面 CIoT 5GS 优化功能且所述终端是需要更新截短参数的终端，则所述移动管理网元确定所述终端符合预设条件；

若所述终端没有使用控制面 CIoT 5GS 优化功能或者所述终端不是需要更新截短参数的终端，则所述移动管理网元确定所述终端不符合预设条件。

8、根据权利要求 7 所述的方法，其特征在于，所述移动管理网元判断所述终端是否需要更新截短参数，包括：

5 当所述移动管理网元配置的截短参数与所述终端的上下文中存储的截短参数不相同，所述移动管理网元确定所述终端需要更新截短参数。

9、根据权利要求 7 所述的方法，其特征在于，所述移动管理网元判断所述终端是否需要更新截短参数，包括：

10 在所述移动管理网元更新截短参数之后，移动管理网元确定所述终端需要更新截短参数。

10、根据权利要求 4 至 9 任一项所述的方法，其特征在于，所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能，包括：

15 若所述终端上报的偏好的网络行为用于指示终端偏好使用控制面 CIoT 5GS 优化功能，并且所述移动管理网元支持控制面 CIoT 5GS 优化功能，则所述移动管理网元确定所述终端使用控制面 CIoT 5GS 优化功能。

11、根据权利要求 4 至 9 任一项所述的方法，其特征在于，所述移动管理网元判断所述终端是否使用控制面 CIoT 5GS 优化功能，包括：

若所述终端的上下文用于指示所述终端使用控制面 CIoT 5GS 优化功能，则所述移动管理网元确定所述终端使用控制面 CIoT 5GS 优化功能。

20 12、根据权利要求 1 至 11 任一项所述的方法，其特征在于，所述移动管理网元判断所述终端是否符合预设条件，包括：

在所述移动管理网元接收到终端的注册请求消息或者服务请求消息之后，所述移动管理网元判断所述终端是否符合预设条件。

25 13、根据权利要求 1 至 12 任一项所述的方法，其特征在于，所述下行 NAS 消息为服务接受消息或者注册接受消息。

14、根据权利要求 1 至 13 任一项所述的方法，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

30 所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

15、根据权利要求 14 所述的方法，其特征在于，所述方法还包括：

所述移动管理网元根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数；或者，

35 所述移动管理网元根据网络管理系统的指令，更新截短参数；或者，

所述移动管理网元接收接入网设备发送的更新后的截短参数。

16、一种截短参数的保护方法，其特征在于，所述方法包括：

终端接收移动管理网元发送的经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，所述下行 NAS 消息包括截短参数，所述截短参数用于对所述终端的

5G-S-TMSI 进行截短处理;

所述终端对所述下行 NAS 消息解安全保护;

在成功对所述下行 NAS 消息解安全保护之后, 所述终端存储所述截短参数。

17、根据权利要求 16 所述的方法, 其特征在于, 所述终端存储所述截短参数, 包
5 括:

所述终端的 NAS 层存储所述截短参数。

18、根据权利要求 17 所述的方法, 其特征在于, 所述方法还包括:

所述终端的 NAS 层向所述终端的无线资源控制 RRC 层发送截短参数;

所述终端的 RRC 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理,
10 获得截短的 5G-S-TMSI。

19、根据权利要求 17 所述的方法, 其特征在于, 所述方法还包括:

所述终端的 NAS 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理,
获得截短的 5G-S-TMSI;

所述终端的 NAS 层向所述终端的 RRC 层发送所述截短的 5G-S-TMSI。

20、根据权利要求 16 所述的方法, 其特征在于, 所述终端存储所述截短参数, 包
15 括:

所述终端的 NAS 层向所述终端的 RRC 层发送所述截短参数;

所述终端的 RRC 层存储所述截短参数。

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:

所述终端的 RRC 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理,
20 获得截短的 5G-S-TMSI。

22、根据权利要求 20 所述的方法, 其特征在于, 所述方法还包括:

所述终端的 RRC 层向所述终端的 NAS 层发送所述截短参数;

所述终端的 NAS 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理,

25 获得截短的 5G-S-TMSI;

所述终端的 NAS 层向所述终端的 RRC 层发送所述截短的 5G-S-TMSI。

23、根据权利要求 18、19、21 或者 22 所述的方法, 其特征在于, 所述方法还包
括:

所述终端向接入网设备发送 RRC 重建立请求消息, 所述 RRC 重建立请求消息包
30 括所述截短的 5G-S-TMSI。

24、根据权利要求 16 至 23 任一项所述的方法, 其特征在于, 所述下行 NAS 消息
为服务接受消息或者注册接受消息。

25、根据权利要求 16 至 24 任一项所述的方法, 其特征在于, 5G-S-TMSI 的第一
一个比特到第十个比特用于表示 AMF set ID, 5G-S-TMSI 的第十一个比特到第十六个比
35 特用于表示 AMF pointer, 5G-S-TMSI 的第十七个比特到第四十八个比特用于表示
5G-TMSI;

所述截短参数包括第一截短参数和第二截短参数, 所述第一截短参数用于截短
AMF set ID 和 5G-TMSI, 所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

26、一种截短参数的保护方法, 其特征在于, 所述方法包括:

接入网设备判断终端是否支持 CIoT 5GS 优化特性;

在所述终端支持 CIoT 5GS 优化特性的情况下,所述接入网设备向移动管理网元发送截短参数,所述截短参数用于对所述终端的 5G-S-TMSI 进行截短处理。

27、根据权利要求 26 所述的方法,其特征在于,所述接入网设备判断终端是否支持 CIoT 5GS 优化特性,包括:

若所述终端的能力指示信息用于指示所述终端支持 CIoT 5GS 优化特性,则所述接入网设备确定所述终端支持 CIoT 5GS 优化特性。

28、根据权利要求 26 所述的方法,其特征在于,所述接入网设备判断终端是否支持 CIoT 5GS 优化特性,包括:

10 若所述终端使用的频点与 CIoT 设备使用的频点相同,则所述接入网设备确定所述终端支持 CIoT 5GS 优化特性。

29、根据权利要求 26 所述的方法,其特征在于,所述接入网设备判断终端是否支持 CIoT 5GS 优化特性,包括:

15 若所述终端发送的消息的类型与 CIoT 设备发送的消息的类型相同,则所述接入网设备确定所述终端支持 CIoT 5GS 优化特性。

30、根据权利要求 26 至 29 任一项所述的方法,其特征在于,所述接入网设备判断终端是否支持 CIoT 5GS 优化特性,包括:

在所述接入网设备接收到所述终端发送的上行 RRC 消息之后,所述接入网设备判断终端是否支持 CIoT 5GS 优化特性。

20 31、根据权利要求 30 所述的方法,其特征在于,所述上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

32、根据权利要求 26 至 31 任一项所述的方法,其特征在于,所述接入网设备向移动管理网元发送截短参数,包括:

25 所述接入网设备向所述移动管理网元发送初始 UE 消息,所述初始 UE 消息包括所述截短参数。

33、根据权利要求 26 至 32 任一项所述的方法,其特征在于,所述截短参数是预先存储在所述接入网设备中的。

34、根据权利要求 26 至 33 任一项所述的方法,其特征在于,所述方法还包括:

30 所述接入网设备接收所述终端发送的 RRC 重建请求消息,所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

35、根据权利要求 26 至 34 任一项所述的方法,其特征在于,5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID,5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer,5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI;

35 所述截短参数包括第一截短参数和第二截短参数,所述第一截短参数用于截短 AMF set ID 和 5G-TMSI,所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

36、一种截短参数的保护方法,其特征在于,所述方法包括:

移动管理网元更新截短参数,所述截短参数用于对 5G-S-TMSI 进行截短处理;

所述移动管理网元查找使用控制面 CIoT 5GS 优化功能的终端;

所述移动管理网元分别向所述使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，所述下行 NAS 消息包括更新后的截短参数。

- 37、根据权利要求 36 所述的方法，其特征在于，所述移动管理网元更新截短参数，
5 包括：

所述移动管理网元根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数；或者，

所述移动管理网元根据网络管理系统的指令，更新截短参数；或者，

所述移动管理网元接收接入网设备发送的更新后的截短参数。

- 10 38、根据权利要求 36 或 37 所述的方法，其特征在于，所述移动管理网元向所述使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，包括：

在所述使用控制面 CIoT 5GS 优化功能的终端处于连接态的情况下，所述移动管理网元向所述使用控制面 CIoT 5GS 优化功能的终端发送所述下行 NAS 消息。

- 15 39、根据权利要求 36 或 37 所述的方法，其特征在于，所述移动管理网元向所述使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，包括：

在所述使用控制面 CIoT 5GS 优化功能的终端处于非连接态的情况下，所述移动管理网元等待所述使用控制面 CIoT 5GS 优化功能的终端进入连接态；

- 20 在所述使用控制面 CIoT 5GS 优化功能的终端进入连接态，并且所述移动管理网元与所述使用控制面 CIoT 5GS 优化功能的终端之间的激活 NAS 安全之后，所述移动管理网元向所述使用控制面 CIoT 5GS 优化功能的终端发送所述下行 NAS 消息。

- 40、根据权利要求 36 或 37 所述的方法，其特征在于，所述移动管理网元向所述使用控制面 CIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，包括：

在所述使用控制面 CIoT 5GS 优化功能的终端处于非连接态的情况下，所述移动管理网元以寻呼的方式触发所述使用控制面 CIoT 5GS 优化功能的终端进入连接态；

- 30 在所述使用控制面 CIoT 5GS 优化功能的终端进入连接态，并且所述移动管理网元与所述使用控制面 CIoT 5GS 优化功能的终端之间的激活 NAS 安全之后，所述移动管理网元向所述使用控制面 CIoT 5GS 优化功能的终端发送所述下行 NAS 消息。

41、根据权利要求 36 至 40 任一项所述的方法，其特征在于，所述下行 NAS 消息为 UE 配置更新命令消息，或者服务接受消息。

- 42、根据权利要求 36 至 41 任一项所述的方法，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

43、一种截短参数的保护方法，其特征在于，所述方法包括：

移动管理网元接收接入网设备发送的截短参数，所述截短参数用于对终端的 5G-S-TMSI 进行截短处理；

所述移动管理网元根据所述终端的 NAS 安全上下文，对所述终端的 5G-S-TMSI 进行完整性计算，生成第一 NAS MAC；

5 所述移动管理网元向所述接入网设备发送所述第一 NAS MAC。

44、根据权利要求 43 所述的方法，其特征在于，所述方法还包括：

所述移动管理网元接收所述接入网设备发送的保护指示信息和/或新鲜性参数，所述保护指示信息用于指示所述移动管理网元对所述截短参数进行安全保护，所述新鲜性参数用于对所述截短参数的完整性计算。

10 45、根据权利要求 43 或 44 所述的方法，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

15 46、一种截短参数的保护方法，其特征在于，所述方法包括：

接入网设备向移动管理网元发送截短参数，所述截短参数用于对终端的 5G-S-TMSI 进行截短处理；

所述接入网设备接收所述移动管理网元发送的第一 NAS MAC，所述第一 NAS MAC 是对所述截短参数进行完整性计算得到的；

20 所述接入网设备向所述终端发送所述第一 NAS MAC 和所述截短参数。

47、根据权利要求 46 所述的截短参数的保护方法，其特征在于，所述方法还包括：

所述接入网设备判断所述终端是否支持 CIoT 5GS 优化特性；

所述接入网设备向移动管理网元发送截短参数，包括：

25 在所述终端支持 CIoT 5GS 优化特性的情况下，所述接入网设备向所述移动管理网元发送截短参数。

48、根据权利要求 47 所述的方法，其特征在于，所述接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：

若所述终端的能力指示信息用于指示所述终端支持 CIoT 5GS 优化特性，则所述接入网设备确定所述终端支持 CIoT 5GS 优化特性。

30 49、根据权利要求 47 所述的方法，其特征在于，所述接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：

若所述终端使用的频点与 CIoT 设备使用的频点相同，则所述接入网设备确定所述终端支持 CIoT 5GS 优化特性。

35 50、根据权利要求 47 所述的方法，其特征在于，所述接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：

若所述终端发送的消息的类型与 CIoT 设备发送的消息的类型相同，则所述接入网设备确定所述终端支持 CIoT 5GS 优化特性。

51、根据权利要求 47 至 50 任一项所述的方法，其特征在于，接入网设备判断终端是否支持 CIoT 5GS 优化特性，包括：

在所述接入网设备接收到所述终端发送的上行 RRC 消息之后,所述接入网设备判断终端是否支持 CIoT 5GS 优化特性。

52、根据权利要求 51 所述的方法,其特征在于,所述上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

5 53、根据权利要求 46 至 52 任一项所述的方法,其特征在于,所述方法还包括:

所述接入网设备向所述移动管理网元发送保护指示信息和/或新鲜性参数,所述保护指示信息用于指示所述移动管理网元对所述截短参数进行安全保护,所述新鲜性参数用于对所述截短参数的完整性计算。

54、根据权利要求 46 至 53 任一项所述的方法,其特征在于,所述方法还包括:

10 所述接入网设备接收所述终端发送的 RRC 重建立请求消息,所述 RRC 重建立请求消息包括截短的 5G-S-TMSI。

55、根据权利要求 46 至 54 任一项所述的方法,其特征在于,5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID,5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer,5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI;

15 所述截短参数包括第一截短参数和第二截短参数,所述第一截短参数用于截短 AMF set ID 和 5G-TMSI,所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

56、一种截短参数的保护方法,其特征在于,所述方法包括:

20 终端接收接入网设备发送的第一 NAS MAC 和截短参数,所述截短参数用于对所述终端的 5G-S-TMSI 进行截短处理;

所述终端根据 NAS 安全上下文,对所述截短参数进行完整性计算,生成第二 NAS MAC;

所述终端根据所述第二 NAS MAC,校验所述第一 NAS MAC;

在所述第一 NAS MAC 通过校验的情况下,所述终端存储所述截短参数。

25 57、根据权利要求 56 所述的方法,其特征在于,所述终端存储所述截短参数,包括:

所述终端的 RRC 层存储所述截短参数。

58、根据权利要求 57 所述的方法,其特征在于,所述方法还包括:

30 所述终端的 RRC 层根据所述截短参数,对所述终端的 5G-S-TMSI 进行截短处理,获得截短的 5G-S-TMSI。

59、根据权利要求 57 所述的方法,其特征在于,所述方法还包括:

所述终端的 RRC 层向所述终端的 NAS 层发送所述截短参数;

所述终端的 NAS 层根据所述截短参数,对所述终端的 5G-S-TMSI 进行截短处理,获得截短的 5G-S-TMSI;

35 所述终端的 NAS 层向所述终端的 RRC 层发送所述截短的 5G-S-TMSI。

60、根据权利要求 56 所述的方法,其特征在于,所述终端存储所述截短参数,包括:

所述终端的 RRC 层向所述终端的 NAS 层发送所述截短参数;

所述终端的 NAS 层存储所述截短参数。

- 61、根据权利要求 60 所述的方法，其特征在于，所述方法还包括：
所述终端的 NAS 层根据所述截短参数，对所述终端的 5G-S-TMSI 进行截短处理，
获得截短的 5G-S-TMSI；
所述终端的 NAS 层向所述终端的 RRC 层发送所述截短的 5G-S-TMSI。
- 5 62、根据权利要求 60 所述的方法，其特征在于，所述方法还包括：
所述终端的 NAS 层向所述终端的 RRC 层发送所述截短参数；
所述终端的 RRC 层根据所述截短参数，对所述终端的 5G-S-TMSI 进行截短处理，
获得截短的 5G-S-TMSI。
- 10 63、根据权利要求 56 至 62 任一项所述的方法，其特征在于，所述方法还包括：
所述终端向所述接入网设备发送 RRC 重建立请求消息，所述 RRC 重建立请求消息
包括截短的 5G-S-TMSI。
- 15 64、根据权利要求 56 至 63 任一项所述的方法，其特征在于，5G-S-TMSI 的第一个
比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比
特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示
5G-S-TMSI；
所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短
AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。
- 20 65、一种通信装置，其特征在于，包括：
处理模块，用于判断终端是否符合预设条件，所述预设条件包括所述终端使用控
制面 CIoT 5GS 优化功能；
通信模块，用于在所述终端符合预设条件的情况下，向所述终端发送经过 NAS 安全
上下文进行 NAS 安全保护的下行 NAS 消息，所述下行 NAS 消息包括截短参数，所
述截短参数用于对所述终端的 5G-S-TMSI 进行截短处理。
- 25 66、根据权利要求 65 所述的通信装置，其特征在于，所述通信装置还包括存储模
块；
所述存储模块，用于存储所述截短参数。
- 67、根据权利要求 65 所述的通信装置，其特征在于，
所述通信模块，还用于接收接入网设备发送的所述截短参数。
- 68、根据权利要求 65 至 67 任一项所述的通信装置，其特征在于，所述处理模块，
30 用于判断终端是否符合预设条件，包括：
判断所述终端是否使用控制面 CIoT 5GS 优化功能；
若所述终端使用控制面 CIoT 5GS 优化功能，则确定所述终端符合预设条件；
若所述终端没有使用控制面 CIoT 5GS 优化功能，则确定所述终端不符合预设条
件。
- 35 69、根据权利要求 65 至 67 任一项所述的通信装置，其特征在于，所述预设条件
还包括：所述终端是初始注册到网络的终端；
所述处理模块，用于判断终端是否符合预设条件，包括：
判断所述终端是否使用控制面 CIoT 5GS 优化功能，以及所述终端是否是初始注
册到网络的终端；

若所述终端使用控制面 CIoT 5GS 优化功能且所述终端是初始注册到网络中的终端，则确定所述终端符合预设条件；

若所述终端没有使用控制面 CIoT 5GS 优化功能或者所述终端不是初始注册到网络中的终端，则确定所述终端不符合预设条件。

5 70、根据权利要求 69 所述的通信装置，其特征在于，

所述处理模块，具体用于根据所述终端上报的注册类型，确定所述终端是初始注册到网络的终端。

71、根据权利要求 65 至 67 任一项所述的通信装置，其特征在于，所述预设条件还包括：所述终端需要更新截短参数；

10 所述处理模块，用于判断终端是否符合预设条件，包括：

判断所述终端是否使用控制面 CIoT 5GS 优化功能，以及所述终端是否需要更新截短参数；

若所述终端使用控制面 CIoT 5GS 优化功能且所述终端是需要更新截短参数的终端，则确定所述终端符合预设条件；

15 若所述终端没有使用控制面 CIoT 5GS 优化功能或者所述终端不是需要更新截短参数的终端，则确定所述终端不符合预设条件。

72、根据权利要求 71 所述的通信装置，其特征在于，

所述处理模块，具体用于当移动管理网元配置的截短参数与所述终端的上下文存储的截短参数不相同，确定所述终端需要更新截短参数。

20 73、根据权利要求 71 所述的通信装置，其特征在于，

所述处理模块，具体用于在移动管理网元更新截短参数之后，确定所述终端需要更新截短参数。

74、根据权利要求 68 至 73 任一项所述的通信装置，其特征在于，

25 所述处理模块，具体用于若所述终端上报的偏好的网络行为用于指示终端偏好使用控制面 CIoT 5GS 优化功能，并且移动管理网元支持控制面 CIoT 5GS 优化功能，则确定所述终端使用控制面 CIoT 5GS 优化功能。

75、根据权利要求 68 至 73 任一项所述的通信装置，其特征在于，

所述处理模块，具体用于若所述终端的上下文用于指示所述终端使用控制面 CIoT 5GS 优化功能，则确定所述终端使用控制面 CIoT 5GS 优化功能。

30 76、根据权利要求 68 至 75 任一项所述的通信装置，其特征在于，

所述处理模块，具体用于在所述通信模块接收到终端的注册请求消息或者服务请求消息之后，判断所述终端是否符合预设条件。

77、根据权利要求 65 至 76 任一项所述的通信装置，其特征在于，所述下行 NAS 消息为服务接受消息或者注册接受消息。

35 78、根据权利要求 65 至 77 任一项所述的通信装置，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短

AMF set ID 和 5G-TMSI, 所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

79、根据权利要求 78 所述的通信装置, 其特征在于,

所述处理模块, 用于根据 AMF set ID 的数目和/或 AMF pointer 的数目, 更新截短参数; 或者,

5 所述处理模块, 用于根据网络管理系统的指令, 更新截短参数; 或者,

所述通信模块, 用于接收接入网设备发送的更新后的截短参数。

80、一种通信装置, 其特征在于, 包括:

通信模块, 用于接收移动管理网元发送的经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息, 所述下行 NAS 消息包括截短参数, 所述截短参数用于对终端的

10 5G-S-TMSI 进行截短处理;

处理模块, 用于对所述下行 NAS 消息解安全保护;

存储模块, 用于在所述处理模块成功对所述下行 NAS 消息解安全保护之后, 存储所述截短参数。

81、根据权利要求 80 所述的通信装置, 其特征在于, 所述存储模块, 用于存储所述截短参数, 包括:

NAS 层存储所述截短参数。

82、根据权利要求 81 所述的通信装置, 其特征在于, 所述处理模块, 还用于获取截短的 5G-S-TMSI, 包括:

NAS 层向 RRC 层发送截短参数;

20 RRC 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI。

83、根据权利要求 81 所述的通信装置, 其特征在于, 所述处理模块, 还用于获取截短的 5G-S-TMSI, 包括:

25 NAS 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI;

NAS 层向 RRC 层发送所述截短的 5G-S-TMSI。

84、根据权利要求 80 所述的通信装置, 其特征在于, 所述存储模块, 用于存储所述截短参数, 包括:

NAS 层向 RRC 层发送所述截短参数;

30 RRC 层存储所述截短参数。

85、根据权利要求 84 所述的通信装置, 其特征在于, 所述处理模块, 还用于获取截短的 5G-S-TMSI, 包括:

RRC 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI。

35 86、根据权利要求 84 所述的通信装置, 其特征在于, 所述处理模块, 还用于获取截短的 5G-S-TMSI, 包括:

RRC 层向 NAS 层发送所述截短参数;

所述 NAS 层根据所述截短参数, 对所述终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI;

所述 NAS 层向所述 RRC 层发送所述截短的 5G-S-TMSI。

87、根据权利要求 82、83、85 或者 86 所述的通信装置，其特征在于，

所述通信模块，还用于向接入网设备发送 RRC 重建立请求消息，所述 RRC 重建立请求消息包括所述截短的 5G-S-TMSI。

5 88、根据权利要求 80 至 87 任一项所述的通信装置，其特征在于，所述下行 NAS 消息为服务接受消息或者注册接受消息。

89、根据权利要求 80 至 88 任一项所述的通信装置，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示
10 5G-TMSI；

所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

90、一种通信装置，其特征在于，包括：

处理模块，用于判断终端是否支持 CIoT 5GS 优化特性；

15 通信模块，用于在所述终端支持 CIoT 5GS 优化特性的情况下，向移动管理网元发送截短参数，所述截短参数用于对所述终端的 5G-S-TMSI 进行截短处理。

91、根据权利要求 90 所述的通信装置，其特征在于，

所述处理模块，具体用于若所述终端的能力指示信息用于指示所述终端支持 CIoT 5GS 优化特性，则确定所述终端支持 CIoT 5GS 优化特性。

20 92、根据权利要求 90 所述的通信装置，其特征在于，

所述处理模块，具体用于若所述终端使用的频点与 CIoT 设备使用的频点相同，则确定所述终端支持 CIoT 5GS 优化特性。

93、根据权利要求 90 所述的通信装置，其特征在于，

25 所述处理模块，具体用于若所述终端发送的消息的类型与 CIoT 设备发送的消息的类型相同，则确定所述终端支持 CIoT 5GS 优化特性。

94、根据权利要求 90 至 93 任一项所述的通信装置，其特征在于，

所述处理模块，具体用于在所述通信模块接收到所述终端发送的上行 RRC 消息之后，判断终端是否支持 CIoT 5GS 优化特性。

30 95、根据权利要求 94 所述的通信装置，其特征在于，所述上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

96、根据权利要求 90 至 95 任一项所述的通信装置，其特征在于，

所述通信模块，具体用于向所述移动管理网元发送初始 UE 消息，所述初始 UE 消息包括所述截短参数。

35 97、根据权利要求 90 至 96 任一项所述的通信装置，其特征在于，所述通信装置还包括存储模块；

所述存储模块，用于存储所述截短参数。

98、根据权利要求 90 至 97 任一项所述的通信装置，其特征在于，

所述通信模块，用于接收所述终端发送的 RRC 重建立请求消息，所述 RRC 重建立请求消息包括截短的 5G-S-TMSI。

99、根据权利要求 90 至 98 任一项所述的通信装置，其特征在于，

5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

5 所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

100、一种通信装置，其特征在于，包括：

处理模块，用于更新截短参数，所述截短参数用于对 5G-S-TMSI 进行截短处理；
查找使用控制面 ClIoT 5GS 优化功能的终端；

10 通信模块，用于向所述使用控制面 ClIoT 5GS 优化功能的终端发送经过 NAS 安全上下文进行 NAS 安全保护的下行 NAS 消息，所述下行 NAS 消息包括更新后的截短参数。

101、根据权利要求 100 所述的通信装置，其特征在于，

所述处理模块，用于根据 AMF set ID 的数目和/或 AMF pointer 的数目，更新截短参数；或者，根据网络管理系统的指令，更新截短参数；或者，接收接入网设备发送的更新后的截短参数。

102、根据权利要求 100 或 101 所述的通信装置，其特征在于，

所述通信模块，具体用于在所述使用控制面 ClIoT 5GS 优化功能的终端处于连接态的情况下，向所述使用控制面 ClIoT 5GS 优化功能的终端发送所述下行 NAS 消息。

20 103、根据权利要求 100 或 101 所述的通信装置，其特征在于，

所述通信模块，具体用于在所述使用控制面 ClIoT 5GS 优化功能的终端处于非连接态的情况下，等待所述使用控制面 ClIoT 5GS 优化功能的终端进入连接态；在所述使用控制面 ClIoT 5GS 优化功能的终端进入连接态，并且移动管理网元与所述使用控制面 ClIoT 5GS 优化功能的终端之间的激活 NAS 安全之后，向所述使用控制面 ClIoT 5GS 优化功能的终端发送所述下行 NAS 消息。

25 104、根据权利要求 100 或 101 所述的通信装置，其特征在于，

所述通信模块，具体用于在所述使用控制面 ClIoT 5GS 优化功能的终端处于非连接态的情况下，以寻呼的方式触发所述使用控制面 ClIoT 5GS 优化功能的终端进入连接态；在所述使用控制面 ClIoT 5GS 优化功能的终端进入连接态，并且移动管理网元与所述使用控制面 ClIoT 5GS 优化功能的终端之间的激活 NAS 安全之后，向所述使用控制面 ClIoT 5GS 优化功能的终端发送所述下行 NAS 消息。

105、根据权利要求 100 至 104 任一项所述的通信装置，其特征在于，所述下行 NAS 消息为 UE 配置更新命令消息，或者服务接受消息。

106、根据权利要求 100 至 105 任一项所述的通信装置，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

107、一种通信装置，其特征在于，包括：

通信模块，用于接收接入网设备发送的截短参数，所述截短参数用于对终端的 5G-S-TMSI 进行截短处理；

5 处理模块，用于根据所述终端的 NAS 安全上下文，对所述终端的 5G-S-TMSI 进行完整性计算，生成第一 NAS MAC；

通信模块，还用于向所述接入网设备发送所述第一 NAS MAC。

108、根据权利要求 107 所述的通信装置，其特征在于，

10 所述通信模块，还用于接收所述接入网设备发送的保护指示信息和/或新鲜性参数，所述保护指示信息用于指示移动管理网元对所述截短参数进行安全保护，所述新鲜性参数用于对所述截短参数的完整性计算。

109、根据权利要求 107 或 108 所述的通信装置，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

15 所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

110、一种通信装置，其特征在于，包括：

20 通信模块，用于向移动管理网元发送截短参数，所述截短参数用于对终端的 5G-S-TMSI 进行截短处理；接收所述移动管理网元发送的第一 NAS MAC，所述第一 NAS MAC 是对所述截短参数进行完整性计算得到的；向所述终端发送所述第一 NAS MAC 和所述截短参数。

111、根据权利要求 110 所述的通信装置，其特征在于，所述通信装置还包括处理模块；

所述处理模块，用于判断所述终端是否支持 CIoT 5GS 优化特性；

25 所述通信模块，具体用于在所述终端支持 CIoT 5GS 优化特性的情况下，向所述移动管理网元发送截短参数。

112、根据权利要求 111 所述的通信装置，其特征在于，

所述处理模块，具体用于若所述终端的能力指示信息用于指示所述终端支持 CIoT 5GS 优化特性，则确定所述终端支持 CIoT 5GS 优化特性。

30 113、根据权利要求 111 所述的通信装置，其特征在于，

所述处理模块，具体用于若所述终端使用的频点与 CIoT 设备使用的频点相同，则确定所述终端支持 CIoT 5GS 优化特性。

114、根据权利要求 111 所述的通信装置，其特征在于，

35 所述处理模块，具体用于若所述终端发送的消息的类型与 CIoT 设备发送的消息的类型相同，则确定所述终端支持 CIoT 5GS 优化特性。

115、根据权利要求 111 至 114 任一项所述的通信装置，其特征在于，

所述通信模块，还用于接收所述终端发送的上行 RRC 消息；

所述处理模块，具体用于在所述通信模块接收到所述终端发送的上行 RRC 消息之后，判断终端是否支持 CIoT 5GS 优化特性。

116、根据权利要求 115 所述的通信装置，其特征在于，所述上行 RRC 消息为 RRC 建立请求消息或者 RRC 建立完成消息。

117、根据权利要求 110 至 116 任一项所述的通信装置，其特征在于，

5 所述通信模块，还用于向所述移动管理网元发送保护指示信息和/或新鲜性参数，
所述保护指示信息用于指示所述移动管理网元对所述截短参数进行安全保护，所述新鲜性参数用于对所述截短参数的完整性计算。

118、根据权利要求 110 至 117 任一项所述的通信装置，其特征在于，

所述通信模块，还用于接收所述终端发送的 RRC 重建请求消息，所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

10 119、根据权利要求 110 至 118 任一项所述的通信装置，其特征在于，5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID，5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer，5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI；

15 所述截短参数包括第一截短参数和第二截短参数，所述第一截短参数用于截短 AMF set ID 和 5G-TMSI，所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

120、一种通信装置，其特征在于，包括：

通信模块，用于接收接入网设备发送的第一 NAS MAC 和截短参数，所述截短参数用于对 5G-S-TMSI 进行截短处理；

20 处理模块，用于根据 NAS 安全上下文，对所述截短参数进行完整性计算，生成第二 NAS MAC；根据所述第二 NAS MAC，校验所述第一 NAS MAC；

存储模块，用于在所述第一 NAS MAC 通过校验的情况下，存储所述截短参数。

121、根据权利要求 120 所述的通信装置，其特征在于，所述存储模块，用于存储所述截短参数，包括：

RRC 层存储所述截短参数。

25 122、根据权利要求 121 所述的通信装置，其特征在于，所述处理模块，还用于获得截短的 5G-S-TMSI，包括：

RRC 层根据所述截短参数，对终端的 5G-S-TMSI 进行截短处理，获得所述截短的 5G-S-TMSI。

30 123、根据权利要求 121 所述的通信装置，其特征在于，所述处理模块，还用于获得截短的 5G-S-TMSI，包括：

RRC 层向 NAS 层发送所述截短参数；

所述 NAS 层根据所述截短参数，对终端的 5G-S-TMSI 进行截短处理，获得所述截短的 5G-S-TMSI；

所述 NAS 层向所述 RRC 层发送所述截短的 5G-S-TMSI。

35 124、根据权利要求 120 所述的通信装置，其特征在于，所述存储模块，用于存储所述截短参数，包括：

RRC 层向 NAS 层发送所述截短参数；

所述 NAS 层存储所述截短参数。

125、根据权利要求 124 所述的通信装置，其特征在于，所述处理模块，还用于获

得截短的 5G-S-TMSI, 包括:

NAS 层根据所述截短参数, 对终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI;

所述 NAS 层向 RRC 层发送所述截短的 5G-S-TMSI。

- 5 126、根据权利要求 124 所述的通信装置, 其特征在于, 所述处理模块, 还用于获得截短的 5G-S-TMSI, 包括:

NAS 层向 RRC 层发送所述截短参数;

所述 RRC 层根据所述截短参数, 对终端的 5G-S-TMSI 进行截短处理, 获得截短的 5G-S-TMSI。

- 10 127、根据权利要求 120 至 126 任一项所述的通信装置, 其特征在于,

所述通信模块, 还用于向所述接入网设备发送 RRC 重建请求消息, 所述 RRC 重建请求消息包括截短的 5G-S-TMSI。

- 128、根据权利要求 120 至 127 任一项所述的通信装置, 其特征在于, 5G-S-TMSI 的第一个比特到第十个比特用于表示 AMF set ID, 5G-S-TMSI 的第十一个比特到第十六个比特用于表示 AMF pointer, 5G-S-TMSI 的第十七个比特到第四十八个比特用于表示 5G-TMSI;

所述截短参数包括第一截短参数和第二截短参数, 所述第一截短参数用于截短 AMF set ID 和 5G-TMSI, 所述第二截短参数用于截短 AMF pointer 和 5G-TMSI。

- 20 129、一种通信装置, 其特征在于, 包括处理器和通信接口, 所述处理器用于执行计算机程序指令, 使得所述通信装置实现权利要求 1 至 64 任一项所述的截短参数的保护方法。

130、一种计算机可读存储介质, 其特征在于, 所述计算机可读存储介质存储有指令, 当所述指令在计算机上运行时, 使得所述计算机执行权利要求 1 至 64 任一项所述的截短参数的保护方法。

- 25 131、一种计算机程序产品, 其特征在于, 所述计算机程序产品包括指令, 当所述计算机程序产品在计算机上运行时, 使得所述计算机执行权利要求 1 至 64 任一项所述的截短参数的保护方法。

132、一种芯片, 其特征在于, 所述芯片包括处理器, 当所述处理器执行计算机程序指令时, 使得所述芯片执行权利要求 1 至 64 任一项所述的截短参数的保护方法。