

权 利 要 求 书

1、一种安全保护的方法，其特征在于，包括：

5 终端确定第一参数，所述第一参数用于表示传输非接入层 NAS 消息所使用的接入技术，其中，所述终端能够支持至少两种接入技术，且能够分别为所述至少两种接入技术中的每种接入技术维护对应的 NAS 序列号；

所述终端根据所述第一参数、NAS 密钥以及传输所述 NAS 消息所使用的接入技术对应的 NAS 序列号对所述 NAS 消息进行安全保护。

2、根据权利要求 1 所述的方法，其特征在于，所述第一参数为对所述 NAS 消息进行安全保护时使用的输入参数中的 BEARER 的全部或部分比特位。

10 3、根据权利要求 1 或 2 所述的方法，其特征在于，所述至少两种接入技术包括：第三代合作伙伴计划 3GPP 接入技术和非 3GPP 接入技术。

4、根据权利要求 1-3 任一所述的方法，其特征在于，在传输所述 NAS 消息所使用的接入技术为 3GPP 接入技术的情况下，所述第一参数的值为 0；在传输 NAS 消息所使用的接入技术为非 3GPP 接入技术的情况下，所述第一参数的值为 1。

15 5、根据权利要求 1-4 任一所述的方法，其特征在于，所述终端对 NAS 消息进行安全保护包括对待传输至核心网设备的 NAS 消息进行加密，对接收到的 NAS 消息进行解密，对待传输至核心网设备的 NAS 消息进行完整性保护或者对接收到的 NAS 消息进行完整性保护验证。

20 6、根据权利要求 1-5 任一所述的方法，其特征在于，所述至少两种接入技术包括第一接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术，所述终端确定第一参数之前，所述方法还包括：

所述终端确定所述第一接入技术对应的第一上行 NAS 序列号；

25 所述终端向核心网设备发送第一消息，所述第一消息通过所述第一上行 NAS 序列号和所述 NAS 密钥进行安全保护，所述第一消息携带所述第一上行 NAS 序列号的部分或全部。

7、根据权利要求 6 所述的方法，其特征在于，

所述第一上行 NAS 序列号为 0；或者，

所述第一上行 NAS 序列号为随机数；或者，

30 所述至少两种接入技术还包括第二接入技术，所述第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的上行 NAS 序列号；或者，

所述至少两种接入技术还包括第二接入技术，所述第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的上行 NAS 序列号加 1；或者，

所述第一上行 NAS 序列号为所述终端保存的所述第一接入技术对应的上行 NAS 序列号；或者，

35 所述第一上行 NAS 序列号为所述终端保存的所述第一接入技术对应的上行 NAS 序列号加 1。

8、根据权利要求 1-5 任一所述的方法，其特征在于，所述至少两种接入技术包括第一接入技术和第二接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术，所述终端确定第一参数之前，所述方法还包括：

所述终端向核心网设备发送第一消息,所述第一消息通过所述 NAS 密钥和所述第二接入技术对应的上行 NAS 序列号进行安全保护,所述第一消息携带所述第二接入技术对应的上行 NAS 序列号的部分或全部。

- 5 9、根据权利要求 6 至 8 中任一项所述的方法,其特征在于,所述第一消息携带第一指示信息,所述第一指示信息用于指示所述第一消息中携带的上行 NAS 序列号的部分或全部对应的接入技术。

10、根据权利要求 9 所述的方法,其特征在于,所述方法还包括:

所述终端接收来自所述核心网设备的第二消息,所述第二消息包括所述第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

- 10 11、根据权利要求 10 所述的方法,其特征在于,

所述第二上行 NAS 序列号为 0;或者,

所述第二上行 NAS 序列号为随机数;或者,

所述第二上行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号;或者,

- 15 所述第二上行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1;或者,

所述第二上行 NAS 序列号为所述核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1;或者,

所述第二上行 NAS 序列号为所述第一上行 NAS 序列号;或者,

- 20 所述第二上行 NAS 序列号为所述第一上行 NAS 序列号加 1。

12、根据权利要求 10 或 11 所述的方法,其特征在于,

所述第一下行 NAS 序列号为 0;或者,

所述第一下行 NAS 序列号为随机数;或者,

- 25 所述第一下行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号;或者,

所述第一下行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1;或者,

所述第一下行 NAS 序列号为所述核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1。

- 30 13、根据权利要求 10 至 12 中任一项所述的方法,其特征在于,所述第二消息携带第二指示信息,所述第二指示信息用于指示所述第二消息中携带的所述第一下行 NAS 序列号对应的接入技术。

14、一种安全保护的方法,其特征在于,包括:

- 35 核心网设备确定第一参数,所述第一参数用于表示传输非接入层 NAS 消息所使用的接入技术,其中,所述核心网设备能够分别为终端支持的至少两种接入技术中的每种接入技术维护对应的 NAS 序列号;

所述核心网设备根据所述第一参数、NAS 密钥以及传输所述 NAS 消息所使用的接入技术对应的 NAS 序列号对所述 NAS 消息进行安全保护。

15、根据权利要求 14 所述的方法,其特征在于,所述第一参数为对所述 NAS 消息

进安全保护时使用的输入参数中的 BEARER 的全部或部分比特位。

16、根据权利要求 14 或 15 所述的方法，其特征在于，所述至少两种接入技术包括：第三代合作伙伴计划 3GPP 接入技术和非 3GPP 接入

17、根据权利要求 14-16 任一所述的方法，其特征在于，在传输所述 NAS 消息所
5 使用的接入技术为 3GPP 接入技术的情况下，所述第一参数的值为 0；在传输 NAS 消息所使用的接入技术为非 3GPP 接入技术的情况下，所述第一参数的值为 1。

18、根据权利要求 14-17 任一所述的方法，其特征在于，所述至少两种接入技术包括第一接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术，所述核心网设备确定第一参数之前，所述方法还包括：

10 所述核心网设备接收第一消息，所述第一消息通过所述 NAS 密钥和所述第一接入技术对应的第一上行 NAS 序列号进行安全保护，所述第一消息携带所述第一上行 NAS 序列号。

19、根据权利要求 14-17 任一所述的方法，其特征在于，所述至少两种接入技术包括第一接入技术和第二接入技术，传输所述 NAS 消息所使用的接入技术为所述第一
15 接入技术，所述核心网设备确定第一参数之前，所述方法还包括：

所述核心网设备接收第一消息，所述第一消息通过所述 NAS 密钥和所述第二接入技术对应的上行 NAS 序列号进行安全保护，所述第一消息携带所述第二接入技术对应的上行 NAS 序列号的部分或全部。

20、根据权利要求 18 或 19 所述的方法，其特征在于，所述第一消息携带第一指示信息，所述第一指示信息用于指示所述第一消息携带的上行 NAS 序列号的部分或全部对应的接入技术。

21、根据权利要求 20 所述的方法，其特征在于，在所述核心网设备接收第一消息之后，所述方法还包括：

25 所述核心网设备根据所述第一指示信息指示的接入技术对应的上行 NAS 序列号，对所述第一消息携带的 NAS 序列号的部分或全部进行验证。

22、根据权利要求 21 所述的方法，其特征在于，所述方法还包括：

所述核心网设备确定所述第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部；

30 所述核心网设备向所述终端发送第二消息，所述第二消息包括所述第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

23、一种装置，其特征在于，包括：

35 处理单元，用于确定第一参数，所述第一参数用于表示传输非接入层 NAS 消息所使用的接入技术，其中，所述装置能够支持至少两种接入技术，且能够分别为所述至少两种接入技术中的每种接入技术维护对应的 NAS 序列号；还用于根据所述第一参数、NAS 密钥以及传输所述 NAS 消息所使用的接入技术对应的 NAS 序列号对所述 NAS 消息进行安全保护。

24、根据权利要求 23 所述的装置，其特征在于，所述第一参数为对所述 NAS 消息进安全保护时使用的输入参数中的 BEARER 的全部或部分比特位。

25、根据权利要求 23 或 24 所述的装置，其特征在于，所述至少两种接入技术包

括：第三代合作伙伴计划 3GPP 接入技术和非 3GPP 接入技术。

26、根据权利要求 23-25 任一所述的装置，其特征在于，在传输所述 NAS 消息所使用的接入技术为 3GPP 接入技术的情况下，所述第一参数的值为 0；在传输 NAS 消息所使用的接入技术为非 3GPP 接入技术的情况下，所述第一参数的值为 1。

- 5 27、根据权利要求 23-26 任一所述的装置，其特征在于，所述处理单元，用于对 NAS 消息进行安全保护，具体为：对待传输至核心网设备的 NAS 消息进行加密，对接收到的 NAS 消息进行解密，对待传输至核心网设备的 NAS 消息进行完整性保护或者对接收到的 NAS 消息进行完整性保护验证。

- 10 28、根据权利要求 23-27 任一所述的装置，其特征在于，所述至少两种接入技术包括第一接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术；所述装置还包括通信单元；

所述处理单元，还用于确定所述第一接入技术对应的第一上行 NAS 序列号；

- 15 所述通信单元，用于向核心网设备发送第一消息，所述第一消息通过所述第一上行 NAS 序列号和所述 NAS 密钥进行安全保护，所述第一消息携带所述第一上行 NAS 序列号的部分或全部。

29、根据权利要求 28 所述的装置，其特征在于，

所述第一上行 NAS 序列号为 0；或者，

所述第一上行 NAS 序列号为随机数；或者，

- 20 所述至少两种接入技术还包括第二接入技术，所述第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的上行 NAS 序列号；或者，

所述至少两种接入技术还包括第二接入技术，所述第一上行 NAS 序列号为所述终端保存的所述第二接入技术对应的上行 NAS 序列号加 1；或者，

所述第一上行 NAS 序列号为所述终端保存的所述第一接入技术对应的上行 NAS 序列号；或者，

- 25 所述第一上行 NAS 序列号为所述终端保存的所述第一接入技术对应的上行 NAS 序列号加 1。

30、根据权利要求 23-27 任一所述的装置，其特征在于，所述至少两种接入技术包括第一接入技术和第二接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术；所述装置还包括通信单元；

- 30 所述通信单元，用于向核心网设备发送第一消息，所述第一消息通过所述 NAS 密钥和所述第二接入技术对应的上行 NAS 序列号进行安全保护，所述第一消息携带所述第二接入技术对应的上行 NAS 序列号的部分或全部。

- 35 31、根据权利要求 28 至 30 中任一项所述的装置，其特征在于，所述第一消息携带第一指示信息，所述第一指示信息用于指示所述第一消息中携带的上行 NAS 序列号的部分或全部对应的接入技术。

32、根据权利要求 31 所述的装置，其特征在于，

所述通信单元，还用于接收来自所述核心网设备的第二消息，所述第二消息包括所述第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

33、根据权利要求 32 所述的装置，其特征在于，

- 所述第二上行 NAS 序列号为 0；或者，
所述第二上行 NAS 序列号为随机数；或者，
所述第二上行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号；或者，
- 5 所述第二上行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1；或者，
所述第二上行 NAS 序列号为所述核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1；或者，
所述第二上行 NAS 序列号为所述第一上行 NAS 序列号；或者，
- 10 所述第二上行 NAS 序列号为所述第一上行 NAS 序列号加 1。
34、根据权利要求 32 或 33 所述的装置，其特征在于，
所述第一下行 NAS 序列号为 0；或者，
所述第一下行 NAS 序列号为随机数；或者，
所述第一下行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行
- 15 NAS 序列号；或者，
所述第一下行 NAS 序列号为所述核心网设备保存的第二接入技术对应的下行 NAS 序列号加 1；或者，
所述第一下行 NAS 序列号为所述核心网设备保存的第一接入技术对应的下行 NAS 序列号加 1。
- 20 35、根据权利要求 32 至 34 中任一项所述的装置，其特征在于，所述第二消息携带第二指示信息，所述第二指示信息用于指示所述第二消息中携带的所述第一下行 NAS 序列号对应的接入技术。
36、一种装置，其特征在于，包括：
处理单元，用于确定第一参数，所述第一参数用于表示传输非接入层 NAS 消息所
- 25 使用的接入技术，其中，所述装置能够分别为终端支持的至少两种接入技术中的每种接入技术维护对应的 NAS 序列号；还用于根据所述第一参数、NAS 密钥以及传输所述 NAS 消息所使用的接入技术对应的 NAS 序列号对所述 NAS 消息进行安全保护。
37、根据权利要求 36 所述的装置，其特征在于，所述第一参数为对所述 NAS 消息进安全保护时使用的输入参数中的 BEARER 的全部或部分比特位。
- 30 38、根据权利要求 36 或 37 所述的装置，其特征在于，所述至少两种接入技术包括：第三代合作伙伴计划 3GPP 接入技术和非 3GPP 接入
39、根据权利要求 36-38 任一所述的装置，其特征在于，在传输所述 NAS 消息所使用的接入技术为 3GPP 接入技术的情况下，所述第一参数的值为 0；在传输 NAS 消息所使用的接入技术为非 3GPP 接入技术的情况下，所述第一参数的值为 1。
- 35 40、根据权利要求 36-39 任一所述的装置，其特征在于，所述至少两种接入技术包括第一接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术；所述装置还包括通信单元；
所述通信单元，用于接收第一消息，所述第一消息通过所述 NAS 密钥和所述第一接入技术对应的第一上行 NAS 序列号进行安全保护，所述第一消息携带所述第一上行

NAS 序列号。

41、根据权利要求 36-40 任一所述的装置，其特征在于，所述至少两种接入技术包括第一接入技术和第二接入技术，传输所述 NAS 消息所使用的接入技术为所述第一接入技术；所述装置还包括通信单元；

- 5 所述通信单元，用于接收第一消息，所述第一消息通过所述 NAS 密钥和所述第二接入技术对应的上行 NAS 序列号进行安全保护，所述第一消息携带所述第二接入技术对应的上行 NAS 序列号的部分或全部。

- 10 42、根据权利要求 40 或 41 所述的装置，其特征在于，所述第一消息携带第一指示信息，所述第一指示信息用于指示所述第一消息携带的上行 NAS 序列号的部分或全部对应的接入技术。

43、根据权利要求 42 所述的装置，其特征在于，

所述处理单元，还用于根据所述第一指示信息指示的接入技术对应的上行 NAS 序列号，对所述第一消息携带的 NAS 序列号的部分或全部进行验证。

44、根据权利要求 43 所述的装置，其特征在于，

- 15 所述处理单元，还用于确定所述第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部；

所述通信单元，还用于向所述终端发送第二消息，所述第二消息包括所述处理单元确定的所述第一接入技术对应的第二上行 NAS 序列号和第一下行 NAS 序列号之一或全部。

- 20 45、一种计算机存储介质，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行所述权利要求 1-13 中任意一项所述的方法。

46、一种计算机存储介质，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行所述权利要求 14-22 中任意一项所述的方法。

47、一种装置，其特征在于，包括：包括存储器以及与该存储器耦合的处理器；

- 25 所述存储器中保存有程序指令，当所述处理器执行所述程序指令时，使得所述装置执行上述权利要求 1-13 所述的方法。

48、一种装置，其特征在于，包括：包括存储器以及与该存储器耦合的处理器；

所述存储器中保存有程序指令，当所述处理器执行所述程序指令时，使得所述装置执行上述权利要求 14-22 所述的方法。

30