

权 利 要 求 书

1. 一种密钥管理方法，其特征在于，包括：

终端设备执行主鉴权流程并生成第一应用的认证和密钥管理 AKMA 密钥和第一 AKMA 密钥的标识，所述第一 AKMA 密钥的标识用于标识所述第一 AKMA 密钥；

所述终端设备向应用功能网元发送第一应用会话建立请求消息，所述第一应用会话建立请求消息包括所述第一 AKMA 密钥的标识；

所述终端设备接收来自所述应用功能网元的所述第一应用会话建立请求消息的响应消息，所述第一应用会话建立请求消息的响应消息包括第一失败指示，所述第一失败指示用于指示应用会话建立失败；

所述终端设备向所述应用功能网元发送第二应用会话建立请求消息，所述第二应用会话建立请求消息包括第二 AKMA 密钥的标识，所述第二 AKMA 密钥的标识为重鉴权后生成的，所述第二 AKMA 密钥的标识用于标识所述第二 AKMA 密钥。

2. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

终端设备执行重鉴权流程。

3. 根据权利要求 2 所述的方法，其特征在于，所述重鉴权流程包括：

所述终端设备接收来自安全锚点功能网元的鉴权请求消息，所述鉴权请求消息包括第一鉴权参数；

所述终端设备使用本地保存的根密钥计算第二鉴权参数并校验所述安全锚点功能网元的所述第一鉴权参数；

校验通过后，所述终端设备向所述安全锚点功能网元发送所述重鉴权流程中的所述鉴权请求消息的响应消息，所述鉴权请求消息的响应消息包括第三鉴权参数。

4. 根据权利要求 3 所述的方法，其特征在于，所述鉴权请求消息为非接入层 NAS message authentication request，所述鉴权请求消息的响应消息为 NAS message authentication response。

5. 根据权利要求 3 或 4 所述的方法，其特征在于，所述终端设备向所述安全锚点功能网元发送所述重鉴权流程中的所述鉴权请求消息的响应消息后，所述方法还包括：

所述终端设备生成所述第二 AKMA 密钥和所述第二 AKMA 密钥的标识。

6. 根据权利要求 1-5 任一项所述的方法，其特征在于，所述第一应用会话建立请求消息为 application session establishment request message，所述第一应用会话建立请求消息的响应消息为 application session establishment response。

7. 一种密钥管理方法，其特征在于，包括：

应用功能网元接收来自终端设备的第一应用会话建立请求消息，所述第一应用会话建立请求消息包括第一应用的认证和密钥管理 AKMA 密钥的标识，所述第一 AKMA 密钥的标识用于标识所述第一 AKMA 密钥；

所述应用功能网元向 AKMA 锚点功能网元发送第一请求消息，所述第一请求消息用于请求终端设备和所述应用功能网元之间的通信密钥；

所述应用功能网元接收来自所述 AKMA 锚点功能网元的第二失败指示，所述第二失败指示用于指示请求所述通信密钥失败；

所述应用功能网元根据所述第二失败指示，向所述终端设备发送所述第一应用会话建立请求消息的响应消息，所述响应消息包括第一失败指示，所述第一失败指示用于指示应用会话建立失败；

所述应用功能网元接收来自所述终端设备的第二应用会话建立请求消息，所述第二应用

会话建立请求消息包括第二 AKMA 密钥的标识, 所述第二 AKMA 密钥的标识为重鉴权后生成的, 所述第二 AKMA 密钥的标识用于标识所述第二 AKMA 密钥。

8. 根据权利要求 7 所述的方法, 其特征在于, 还包括:

所述 AKMA 锚点功能网元接收所述第一请求消息;

所述 AKMA 锚点功能网元向所述应用功能网元发送所述第二失败指示。

9. 根据权利要求 7 或 8 所述的方法, 其特征在于, 所述第一应用会话建立请求消息为 application session establishment request message, 所述第一应用会话建立请求消息的响应消息为 application session establishment response。

10. 一种密钥管理方法, 其特征在于, 所述方法包括:

终端设备向第一应用功能网元发送第一应用会话的建立请求消息, 所述建立请求消息携带第一密钥的标识信息, 所述第一密钥为应用的认证和密钥管理 AKMA 密钥;

所述终端设备接收重鉴权流程中的第一鉴权请求消息;

所述终端设备发送所述重鉴权流程中的所述第一鉴权请求消息的响应消息;

所述终端设备接收来自所述第一应用功能网元的所述建立请求消息的响应消息;

所述终端设备使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

11. 根据权利要求 10 所述的方法, 其特征在于, 所述方法还包括:

所述终端设备发送所述第一鉴权请求消息的响应消息后, 不删除所述第一密钥和所述第一密钥的标识信息。

12. 根据权利要求 11 所述的方法, 其特征在于, 所述不删除所述第一密钥和所述第一密钥的标识信息, 包括:

若所述重鉴权流程成功, 所述终端设备不删除所述第一密钥和所述第一密钥的标识信息。

13. 根据权利要求 11 所述的方法, 其特征在于, 所述不删除所述第一密钥和所述第一密钥的标识信息, 包括:

若所述重鉴权流程之前发送了所述建立请求消息, 且未收到所述建立请求消息的响应消息, 所述终端设备不删除所述第一密钥和所述第一密钥的标识信息。

14. 根据权利要求 11 所述的方法, 其特征在于, 所述不删除所述第一密钥和所述第一密钥的标识信息, 包括:

若所述重鉴权流程之前所述终端设备发送了所述建立请求消息, 且已收到所述建立请求消息的响应消息但未推演所述终端设备和所述第一应用功能网元之间的通信密钥, 所述终端设备不删除所述第一密钥和所述第一密钥的标识信息。

15. 根据权利要求 11-14 任一项所述的方法, 其特征在于所述不删除所述第一密钥和所述第一密钥的标识信息, 包括:

若未推演所述终端设备和所述第一应用功能网元之间的通信密钥, 所述终端设备不删除所述第一密钥和所述第一密钥的标识信息。

16. 根据权利要求 10-15 任一项所述的方法, 其特征在于, 所述方法还包括:

所述终端设备接收来自所述建立请求消息的响应消息后, 确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

17. 根据权利要求 16 所述的方法, 其特征在于, 所述方法还包括:

所述终端设备发送所述第一鉴权请求消息的响应消息后, 生成第二密钥, 所述第二密钥为 AKMA 密钥。

18. 根据权利要求 16 所述的方法，其特征在于，所述确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥包括：

当所述终端设备确定所述建立请求消息为所述重鉴权流程前发送的，则所述终端设备确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

19. 根据权利要求 16 所述的方法，其特征在于，所述终端设备确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥包括：

当所述终端设备确定所述建立请求消息携带的是所述第一密钥的标识信息，则所述终端设备确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

20. 根据权利要求 19 所述的方法，其特征在于，所述终端设备确定所述建立请求消息携带的是所述第一密钥的标识信息，包括：

所述终端设备根据第一应用会话上下文中的第一密钥的标识信息确定所述建立请求消息携带的是所述第一密钥的标识信息。

21. 根据权利要求 10-20 任一所述的方法，其特征在于，所述方法还包括：

所述终端设备发送所述第一鉴权请求消息的响应消息后，保存发送所述建立请求消息和所述重鉴权流程的先后关系。

22. 根据权利要求 10-21 中任一项所述的方法，其特征在于，所述方法还包括：

当携带所述第一密钥的标识信息的应用会话请求消息都得到了响应，所述终端设备删除所述第一密钥和所述第一密钥的标识信息。

23. 根据权利要求 10-21 中任一项所述的方法，其特征在于，所述方法还包括：

当所述终端设备未得到响应消息的应用会话请求消息都为所述重鉴权流程之后发送的，所述终端设备删除所述第一密钥和所述第一密钥的标识信息。

24. 根据权利要求 10-23 中任一项所述的方法，其特征在于，所述方法还包括：

所述终端设备发送所述第一鉴权请求消息的响应消息后，所述终端设备向第二应用功能网元发送第二应用会话建立请求消息，所述第二应用会话建立请求消息携带第二密钥的标识信息，所述第二密钥为 AKMA 密钥。

25. 一种通信装置，其特征在于，包括处理单元，发送单元和接收单元：

所述处理单元用于执行主鉴权流程并生成第一应用的认证和密钥管理 AKMA 密钥和第一 AKMA 密钥的标识，所述第一 AKMA 密钥的标识用于标识所述第一 AKMA 密钥；

所述发送单元用于向应用功能网元发送第一应用会话建立请求消息，所述第一应用会话建立请求消息包括所述第一 AKMA 密钥的标识；

所述接收单元用于接收来自所述应用功能网元的所述第一应用会话建立请求消息的响应消息，所述第一应用会话建立请求消息的响应消息包括第一失败指示，所述第一失败指示用于指示应用会话建立失败；

所述发送单元还用于向所述应用功能网元发送第二应用会话建立请求消息，所述第二应用会话建立请求消息包括第二 AKMA 密钥的标识，所述第二 AKMA 密钥的标识为重鉴权后生成的，所述第二 AKMA 密钥的标识用于标识所述第二 AKMA 密钥。

26. 根据权利要求 25 所述的装置，其特征在于，

所述处理单元还用于执行重鉴权流程。

27. 根据权利要求 26 所述的装置，其特征在于，所述重鉴权流程包括：

接收来自安全锚点功能网元的鉴权请求消息，所述鉴权请求消息包括第一鉴权参数；

使用本地保存的根密钥计算第二鉴权参数并校验所述安全锚点功能网元的所述第一鉴权

参数;

校验通过后,向所述安全锚点功能网元发送所述重鉴权流程中的所述鉴权请求消息的响应消息,所述鉴权请求消息的响应消息包括第三鉴权参数。

28. 根据权利要求 27 所述的装置,其特征在于,所述鉴权请求消息为非接入层 NAS message authentication request,所述鉴权请求消息的响应消息为 NAS message authentication response。

29. 根据权利要求 25-28 任一项所述的装置,其特征在于,所述处理单元还用于生成所述第二 AKMA 密钥和所述第二 AKMA 密钥的标识。

30. 根据权利要求 25-29 任一项所述的装置,其特征在于,所述第一应用会话建立请求消息为 application session establishment request message,所述第一应用会话建立请求消息的响应消息为 application session establishment response。

31. 根据权利要求 25-30 任一项所述的装置,其特征在于,所述装置为终端设备。

32. 一种通信装置,其特征在于,包括接收单元,发送单元和处理单元:

所述接收单元用于接收来自终端设备的第一应用会话建立请求消息,所述第一应用会话建立请求消息包括第一应用的认证和密钥管理 AKMA 密钥的标识,所述第一 AKMA 密钥的标识用于标识所述第一 AKMA 密钥;

所述发送单元用于向 AKMA 锚点功能网元发送第一请求消息,所述第一请求消息用于请求终端设备和所述应用功能网元之间的通信密钥;

所述接收单元还用于接收来自所述 AKMA 锚点功能网元的第二失败指示,所述第二失败指示用于指示请求所述通信密钥失败;

所述处理单元用于根据所述第二失败指示,通过所述发送单元向所述终端设备发送所述第一应用会话建立请求消息的响应消息,所述响应消息包括第一失败指示,所述第一失败指示用于指示应用会话建立失败;

所述接收单元还用于接收来自所述终端设备的第二应用会话建立请求消息,所述第二应用会话建立请求消息包括第二 AKMA 密钥的标识,所述第二 AKMA 密钥的标识为重鉴权后生成的,所述第二 AKMA 密钥的标识用于标识所述第二 AKMA 密钥。

33. 一种通信系统,其特征在于,包括应用功能网元和应用的认证和密钥管理 AKMA 锚点功能网元,其中,

所述应用功能网元用于:接收来自终端的第一应用会话建立请求消息,所述第一应用会话建立请求消息包括第一应用的认证和密钥管理 AKMA 密钥的标识,所述第一 AKMA 密钥的标识用于标识所述第一 AKMA 密钥;向 AKMA 锚点功能网元发送第一请求消息,所述第一请求消息用于请求终端设备和所述应用功能网元之间的通信密钥;接收来自所述 AKMA 锚点功能网元的第二失败指示,所述第二失败指示用于指示请求所述通信密钥失败;根据所述第二失败指示,向所述终端设备发送所述第一应用会话建立请求消息的响应消息,所述响应消息包括第一失败指示,所述第一失败指示用于指示应用会话建立失败;以及用于接收来自所述终端设备的第二应用会话建立请求消息,所述第二应用会话建立请求消息包括第二 AKMA 密钥的标识,所述第二 AKMA 密钥的标识为重鉴权后生成的,所述第二 AKMA 密钥的标识用于标识所述第二 AKMA 密钥;

所述 AKMA 锚点功能网元用于接收所述第一请求消息;以及用于向所述应用功能网元发送所述第二失败指示。

34. 根据权利要求 33 所述的系统,其特征在于,所述第一应用会话建立请求消息为

application session establishment request message, 所述第一应用会话建立请求消息的响应消息为 application session establishment response。

35. 一种通信装置, 其特征在于, 所述通信装置包括发送单元、接收单元和处理单元;
所述发送单元, 用于向第一应用功能网元发送第一应用会话的建立请求消息, 所述建立请求消息携带第一密钥的标识信息, 所述第一密钥为应用的认证和密钥管理 AKMA 密钥;
所述接收单元, 用于接收所述重鉴权流程中的第一鉴权请求;
所述发送单元, 用于发送所述重鉴权流程中的所述第一鉴权请求消息的响应消息;
所述处理单元, 用于使用所述第一密钥推演终端设备和所述第一应用功能网元之间的通信密钥。

36. 根据权利要求 35 所述的通信装置, 其特征在于,
所述发送单元用于发送所述第一鉴权请求消息的响应消息后, 所述处理单元用于不删除所述第一密钥和所述第一密钥的标识信息。

37. 根据权利要求 36 所述的通信装置, 其特征在于,
若所述重鉴权流程成功, 所述处理单元用于不删除所述第一密钥和所述第一密钥的标识信息。

38. 根据权利要求 36 所述的通信装置, 其特征在于,
若所述重鉴权流程之前发送了所述建立请求消息, 且未收到所述建立请求消息的响应消息, 所述处理单元用于不删除所述第一密钥和所述第一密钥的标识信息。

39. 根据权利要求 36 所述的通信装置, 其特征在于,
若所述重鉴权流程之前所述终端设备发送了所述建立请求消息, 且已收到所述建立请求消息的响应消息但未推演所述终端设备和所述第一应用功能网元之间的通信密钥, 所述处理单元用于不删除所述第一密钥和所述第一密钥的标识信息。

40. 根据权利要求 36-39 任一项所述的通信装置, 其特征在于,
若未推演所述终端设备和所述第一应用功能网元之间的通信密钥, 所述处理单元用于不删除所述第一密钥和所述第一密钥的标识信息。

41. 根据权利要求 35-40 任一所述的通信装置, 其特征在于,
所述接收单元用于接收来自所述建立请求消息的响应消息后, 所述处理单元用于确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

42. 根据权利要求 41 所述的通信装置, 其特征在于,
所述发送单元用于发送所述第一鉴权请求消息的响应消息后, 所述处理单元用于生成第二密钥, 所述第二密钥为 AKMA 密钥。

43. 根据权利要求 42 所述的通信装置, 其特征在于,
当确定所述建立请求消息为所述重鉴权流程前发送的, 则所述处理单元用于确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

44. 根据权利要求 42 所述的通信装置, 其特征在于,
当确定所述建立请求消息携带的是所述第一密钥的标识信息, 则所述处理单元用于确定使用所述第一密钥推演所述终端设备和所述第一应用功能网元之间的通信密钥。

45. 根据权利要求 44 所述的通信装置, 其特征在于,
所述处理单元用于根据第一应用会话上下文中的第一密钥的标识信息确定所述建立请求消息携带的是所述第一密钥的标识信息。

46. 根据权利要求 35-45 任一所述的通信装置, 其特征在于,

所述发送单元用于发送所述第一鉴权请求消息的响应消息后，所述处理单元用于保存发送所述建立请求消息和所述重鉴权流程的先后关系。

47. 根据权利要求 35-46 中任一项所述的通信装置，其特征在于，
当携带所述第一密钥的标识信息的应用会话请求消息都得到了响应，所述处理单元用于删除所述第一密钥和所述第一密钥的标识信息。

48. 根据权利要求 35-46 中任一项所述的通信装置，其特征在于，
当未得到响应消息的应用会话请求消息都为所述重鉴权流程之后发送的，所述处理单元用于删除所述第一密钥和所述第一密钥的标识信息。

49. 根据权利要求 35-48 中任一项所述的通信装置，其特征在于，
所述发送单元用于发送所述第一鉴权请求消息的响应消息后，还用于向第二应用功能网元发送第二应用会话建立请求消息，所述第二应用会话建立请求消息携带第二密钥的标识信息，所述第二密钥为 AKMA 密钥。

50. 一种计算机可读存储介质，其特征在于，包括指令，当其在计算机上运行时，使得计算机执行如权利要求 1-24 任意一项所述的方法。

51. 一种包含指令的计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1-24 任意一项所述的方法。