(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112492590 A
(43)申请公布日 2021.03.12

(21)申请号 202011443633.1

(22)申请日 2017.11.14

(62)分案原申请数据
201711123039.2 2017.11.14

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 潘凯 陈璟

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 宋正伟

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/06(2021.01)
H04W 12/122(2021.01)

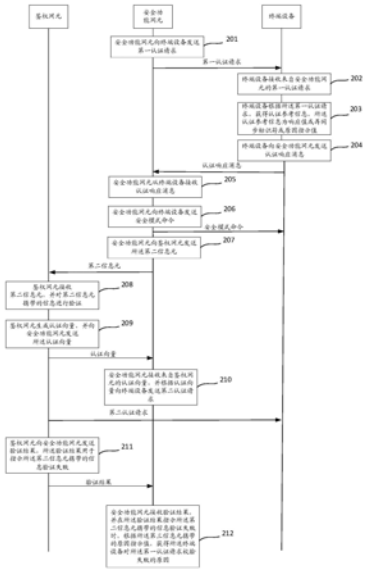
权利要求书4页 说明书21页 附图9页

(54)发明名称

一种通信方法及装置

(57)摘要

本申请公开了一种通信方法及装置，其中方法包括：终端设备接收来自安全功能网元的第一认证请求；所述终端设备根据所述第一认证请求，获得认证参考信息，所述认证参考信息为响应值或再同步标识符或原因指示值；所述终端设备向所述安全功能网元发送认证响应消息，所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元，所述认证参考信息携带在所述认证参考信息对应的信息元中。



CN 112492590 A

1.一种通信方法,其特征在于,所述方法包括:

终端设备接收来自安全功能网元的第一认证请求;

所述终端设备根据所述第一认证请求,获得认证参考信息,所述认证参考信息为响应值或再同步标识符或原因指示值;

所述终端设备向所述安全功能网元发送认证响应消息,所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元,所述认证参考信息携带在所述认证参考信息对应的信息元中。

2.根据权利要求1所述的方法,其特征在于,所述认证参考信息为所述响应值;

所述终端设备向所述安全功能网元发送认证响应消息之前,所述方法还包括:

所述终端设备将所述认证参考信息携带在所述第一信息元中,将第一随机数携带在所述第二信息元中,将第二随机数携带在所述第三信息元中。

3.根据权利要求1所述的方法,其特征在于,所述认证参考信息为所述再同步标识符;

所述终端设备向所述安全功能网元发送认证响应消息之前,所述方法还包括:

所述终端设备将所述认证参考信息携带在所述第二信息元中,将第三随机数携带在所述第一信息元中,将第二随机数携带在所述第三信息元中。

4.根据权利要求1所述的方法,其特征在于,所述认证参考信息为所述原因指示值;

所述终端设备向所述安全功能网元发送认证响应消息之前,所述方法还包括:

所述终端设备将所述认证参考信息携带在所述第三信息元中,将第三随机数携带在所述第一信息元中,将第一随机数携带在所述第二信息元中。

5.一种通信方法,其特征在于,所述方法包括:

安全功能网元向终端设备发送第一认证请求;

所述安全功能网元接收来自所述终端设备的认证响应消息,所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元;

当所述第一信息元携带的信息验证成功时,则所述安全功能网元向所述终端设备发送安全模式命令。

6.根据权利要求5所述的方法,其特征在于,所述方法还包括:

当所述第一信息元携带的信息验证失败时,所述安全功能网元向鉴权网元发送所述第二信息元;

所述安全功能网元接收来自所述鉴权网元的认证向量,并根据所述认证向量向所述终端设备发送第二认证请求;或者,

所述安全功能网元接收来自所述鉴权网元的验证结果,所述验证结果用于指示所述第二信息元携带的信息验证失败,所述安全功能网元根据所述第三信息元携带的原因指示值向所述终端设备发送认证拒绝消息。

7.一种通信方法,其特征在于,所述方法包括:

终端设备根据所述终端设备的用户身份标识,预设参数以及所述终端设备的根密钥,获得身份认证码;

所述终端设备向鉴权服务器功能AUSF网元发送所述身份认证码,所述用户身份标识的密文,以及所述预设参数的明文或密文。

8.根据权利要求7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安全功能网元的认证请求,所述认证请求为所述安全功能网元根据所述鉴权网元生成的认证向量确定的。

9.根据权利要求7或8所述的方法,其特征在于,所述终端设备根据所述终端设备的用户身份标识,预设参数以及所述终端设备的根密钥,获得身份认证码,包括:

所述终端设备根据所述预设参数、所述根密钥以及公共密钥,获得生成参数,所述公共密钥为用于加密所述用户身份标识的密钥;

所述终端设备根据所述生成参数和所述用户身份标识,获得所述身份认证码。

10.一种通信方法,其特征在于,所述方法包括:

鉴权网元从鉴权服务器功能AUSF网元接收身份认证码、终端设备的用户身份标识以及预设参数;

所述鉴权网元根据所述用户身份标识以及所述预设参数,校验所述身份认证码;

当所述身份认证码校验成功时,所述鉴权网元向所述AUSF网元发送认证向量。

11.根据权利要求10所述的方法,其特征在于,所述鉴权网元根据所述用户身份标识以及所述预设参数,校验所述身份认证码,包括:

所述鉴权网元根据所述用户身份标识,获得所述终端设备的根密钥;

所述鉴权网元根据所述根密钥以及所述预设参数获得生成参数,并根据所述生成参数、所述用户身份标识获得期望身份认证码;

当所述期望身份认证码与所述身份认证码相同时,所述身份认证码校验成功;或者,当所述期望身份认证码与所述身份认证码不同时,所述身份认证码校验失败。

12.根据权利要求10或11所述的方法,其特征在于,当所述身份认证码校验失败时,所述方法还包括:

所述鉴权网元向所述AUSF网元发送失败响应。

13.一种通信装置,其特征在于,包括:

收发单元,用于接收来自安全功能网元的第一认证请求;

处理单元,用于根据所述第一认证请求,获得认证参考信息,所述认证参考信息为响应值或再同步标识符或原因指示值;

所述收发单元,用于向所述安全功能网元发送认证响应消息,所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元,所述认证参考信息携带在所述认证参考信息对应的信息元中。

14.根据权利要求13所述的通信装置,其特征在于,所述认证参考信息为所述响应值;

所述收发单元向所述安全功能网元发送认证响应消息之前,所述处理单元还用于:

将所述认证参考信息携带在所述第一信息元中,将第一随机数携带在所述第二信息元中,将第二随机数携带在所述第三信息元中。

15.根据权利要求13所述的通信装置,其特征在于,所述认证参考信息为所述再同步标识符;

所述收发单元向所述安全功能网元发送认证响应消息之前,所述处理单元还用于:

将所述认证参考信息携带在所述第二信息元中,将第三随机数携带在所述第一信息元中,将第二随机数携带在所述第三信息元中。

16.根据权利要求13所述的通信装置,其特征在于,所述认证参考信息为所述原因指示值;

所述收发单元向所述安全功能网元发送认证响应消息之前,所述处理单元还用于:

将所述认证参考信息携带在所述第三信息元中,将第三随机数携带在所述第一信息元中,将第一随机数携带在所述第二信息元中。

17.一种通信装置,其特征在于,包括:

收发单元,用于向终端设备发送第一认证请求;接收来自所述终端设备的认证响应消息,所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元;

处理单元,用于当确定所述第一信息元携带的信息验证成功时,通过所述收发单元向所述终端设备发送安全模式命令。

18.根据权利要求17所述的通信装置,其特征在于,所述处理单元还用于:

当所述第一信息元携带的信息验证失败时,通过所述收发单元向鉴权网元发送所述第二信息元;

通过所述收发单元接收来自所述鉴权网元的认证向量,并根据所述认证向量向所述终端设备发送第二认证请求;或者,

通过所述收发单元接收来自所述鉴权网元的验证结果,所述验证结果用于指示所述第二信息元携带的信息验证失败,根据所述第三信息元携带的原因指示值向所述终端设备发送认证拒绝消息。

19.一种通信装置,其特征在于,包括:

处理单元,用于根据终端设备的用户身份标识,预设参数以及所述终端设备的根密钥,获得身份认证码;

收发单元,用于向鉴权服务器功能AUSF网元发送所述身份认证码,所述用户身份标识的密文,以及所述预设参数的明文或密文。

20.根据权利要求19所述的通信装置,其特征在于,所述收发单元还用于:

接收来自所述安全功能网元的认证请求,所述认证请求为所述安全功能网元根据所述鉴权网元生成的认证向量确定的。

21.根据权利要求19或20所述的通信装置,其特征在于,所述处理单元具体用于:

根据所述预设参数、所述根密钥以及公共密钥,获得生成参数,所述公共密钥为用于加密所述用户身份标识的密钥;

根据所述生成参数和所述用户身份标识,获得所述身份认证码。

22.根据权利要求19或20或21所述的通信装置,其特征在于,所述预设参数为序列号SQN或随机数。

23.一种通信装置,其特征在于,包括:

收发单元,用于从鉴权服务器功能AUSF网元接收身份认证码、终端设备的用户身份标识以及预设参数;

处理单元,用于根据所述用户身份标识以及所述预设参数,校验所述身份认证码;当所述身份认证码校验成功时,通过所述收发单元向所述AUSF网元发送认证向量。

24.根据权利要求23所述的通信装置,其特征在于,所述处理单元具体用于:

根据所述用户身份标识，获得所述终端设备的根密钥；

根据所述根密钥以及所述预设参数获得生成参数，并根据所述生成参数、所述用户身份标识获得期望身份认证码；

当所述期望身份认证码与所述身份认证码相同时，所述身份认证码校验成功；或者，当所述期望身份认证码与所述身份认证码不同时，所述身份认证码校验失败。

25.根据权利要求23或24所述的通信装置，其特征在于，当所述身份认证码校验失败时，所述收发单元还用于：

向所述AUSF网元发送失败响应。

26.一种通信装置，其特征在于，包括：存储器与处理器，与所述存储器相连的所述处理器用于执行所述存储器中存储的计算机程序或指令，以实现如权利要求1至12中任意一项所述的方法。

27.一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中存储有程序或指令，当所述程序或指令被计算机执行时，以实现如权利要求1至12中任意一项所述的方法。

28.一种计算机程序产品，其特征在于，当计算机读取并执行所述计算机程序产品时，使得所述计算机执行如权利要求1至12中任意一项所述的方法。

29.一种芯片，其特征在于，所述芯片与存储器相连，用于读取并执行所述存储器中存储的软件程序，以实现如权利要求1至12中任意一项所述的方法。

一种通信方法及装置

[0001] 本申请为申请号为201711123039.2、申请日为2017年11月14日、发明名称为“一种通信方法及装置”的分案申请。

技术领域

[0002] 本申请涉及通信技术领域，尤其涉及一种通信方法及装置。

背景技术

[0003] 目前，伪基站技术对通信系统的安全性造成了较大的威胁，例如，伪基站能够获取终端设备的身份，该身份可以为国际移动用户识别码(International Mobile Subscriber Identification Number，IMSI)等。进一步地，伪基站还可以根据终端设备的身份攻击该终端设备，例如，追踪到终端设备的位置，进而造成该终端设备的用户的隐私泄漏。

[0004] 例如，伪基站可以使用获取的IMSI向核心网申请认证向量(Authentication Vector，AV)，并根据认证向量生成认证请求，并向终端设备发送该认证请求。若该终端设备是IMSI对应的终端设备，则该终端设备会向伪基站发送用于指示认证成功的响应消息；若该终端设备不是IMSI对应的终端设备，则该终端设备会向伪基站发送用于指示认证失败的响应消息。进而，伪基站可以根据响应消息确定该终端设备是否为IMSI对应的终端设备。

[0005] 采用上述方法，伪基站可以确定IMSI对应的终端设备是否位于该伪基站的信号辐射范围内。通过不断更换伪基站的位置，追踪IMSI对应的终端设备的位置。

[0006] 综上，如何避免终端设备被攻击，是一个亟待解决的问题。

发明内容

[0007] 本申请提供一种通信方法及装置，用以解决终端设备被攻击的问题。

[0008] 第一方面，本申请实施例提供了一种通信方法，该方法包括：

[0009] 终端设备接收来自安全功能网元的第一认证请求；

[0010] 所述终端设备根据所述第一认证请求，获得认证参考信息，所述认证参考信息为响应值或再同步标识符或原因指示值；

[0011] 所述终端设备向所述安全功能网元发送认证响应消息，所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元，所述认证参考信息携带在所述认证参考信息对应的信息元中。

[0012] 根据上述方法，终端设备根据第一认证请求获得的认证参考消息不论是响应值，还是再同步标识符或原因指示值，终端设备向安全功能网元发送的认证响应消息中均包括第一信息元、第二信息元以及第三信息元。通过该方法，终端设备发送的认证响应消息的格式为统一的格式，使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值，还是再同步标识符或原因指示值，从而无法确定终端设备是否对第一认证请求检验通过，从而提高了终端设备的安全性。

[0013] 一种可选地实施方式中，所述响应值用于指示网络侧(例如，安全功能网元)对所

述终端设备进行认证，所述再同步标识符用于请求同步所述终端设备与鉴权网元之间的序列号，所述原因指示值用于指示所述第一认证请求验证失败的原因。

[0014] 一种可选地实施方式中，所述认证参考信息为所述响应值；

[0015] 所述终端设备向所述安全功能网元发送认证响应消息之前，所述方法还包括：

[0016] 所述终端设备将所述认证参考信息携带在所述第一信息元中，将第一随机数携带在所述第二信息元中，将第二随机数携带在所述第三信息元中。

[0017] 根据上述方法，终端设备可以将认证参考消息、第一随机数以及第二随机数，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。由于第一随机数携带在第二信息元中，第二随机数携带在第三信息元中，网络侧(例如，安全功能网元)在确认第一信息元中携带响应值后，可以忽略第二信息元以及第三信息元，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0018] 一种可选地实施方式中，所述认证参考信息为所述再同步标识符；

[0019] 所述终端设备向所述安全功能网元发送认证响应消息之前，所述方法还包括：

[0020] 所述终端设备将所述认证参考信息携带在所述第二信息元中，将第三随机数携带在所述第一信息元中，将第二随机数携带在所述第三信息元中。

[0021] 根据上述方法，终端设备可以将第三随机数、认证参考消息以及第二随机数，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。由于第三随机数携带在第一信息元中，第二随机数携带在第三信息元中，网络侧(例如，安全功能网元)在确认第一信息元中未携带响应值后，可以根据第二信息元以及第三信息元获得所述终端设备对所述第一认证请求校验失败的原因，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0022] 一种可选地实施方式中，所述认证参考信息为所述原因指示值；

[0023] 所述终端设备向所述安全功能网元发送认证响应消息之前，所述方法还包括：

[0024] 所述终端设备将所述认证参考信息携带在所述第三信息元中，将第三随机数携带在所述第一信息元中，将第一随机数携带在所述第二信息元中。

[0025] 根据上述方法，终端设备可以将第三随机数、第一随机数以及认证参考消息，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。由于第三随机数携带在第一信息元中，第二随机数携带在第三信息元中，网络侧(例如，安全功能网元)可以在确定第二信元中携带的信息验证失败时，根据第三信元携带的原因指示值，获得所述终端设备对所述第一认证请求校验失败的原因，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0026] 第二方面，本申请实施例提供一种通信装置，所述通信装置包括存储器、收发机和处理器，其中：存储器用于存储指令；处理器用于根据执行存储器存储的指令，并控制收发机进行信号接收和信号发送，当处理器执行存储器存储的指令时，所述通信装置用于执行上述第一方面或第一方面中任一种可能的设计中的方法。

[0027] 第三方面，本申请实施例提供一种通信装置，用于实现上述第一方面或第一方面中的任意一种方法，包括相应的功能模块，例如包括处理单元、接收单元、发送单元等，分别用于实现以上方法中的步骤。

[0028] 第四方面，本申请实施例提供一种计算机可读存储介质，所述计算机存储介质中

存储有计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述第一方面或第一方面中任一种可能的设计中的方法。

[0029] 第五方面，本申请实施例提供一种计算机程序产品，当计算机读取并执行所述计算机程序产品时，使得计算机执行上述第一方面或第一方面中任一种可能的设计中的方法。

[0030] 第六方面，本申请实施例提供一种芯片，所述芯片与存储器相连，用于读取并执行所述存储器中存储的软件程序，以实现上述第一方面或第一方面中任一种可能的设计中的方法。

[0031] 第七方面，本申请实施例提供了一种通信方法，所述方法包括：

[0032] 安全功能网元向终端设备发送第一认证请求；

[0033] 所述安全功能网元接收来自所述终端设备的认证响应消息，所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元；

[0034] 当所述第一信息元携带的信息验证成功时，则所述安全功能网元向所述终端设备发送安全模式命令。

[0035] 根据上述方法，安全功能网元接收到认证响应消息之后，在确定认证响应消息中第一信息元携带的信息验证成功时，忽略认证响应消息中的第二信息元以及第三信息元，并与终端设备进行安全密钥和算法协商。由于终端设备发送的认证响应消息的格式为统一的格式，使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值，还是再同步标识符或原因指示值，从而无法确定终端设备是否对第一认证请求检验通过，从而提高了终端设备的安全性。

[0036] 一种可选地实施方式中，所述方法还包括：

[0037] 当所述第一信息元携带的信息验证失败时，所述安全功能网元向鉴权网元发送所述第二信息元；

[0038] 所述安全功能网元接收来自所述鉴权网元的认证向量，并根据所述认证向量向所述终端设备发送第二认证请求；或者，所述安全功能网元接收来自所述鉴权网元的验证结果，所述验证结果用于指示所述第二信息元携带的信息验证失败，所述安全功能网元根据所述第三信息元携带的原因指示值向所述终端设备发送认证拒绝消息。

[0039] 第八方面，本申请实施例提供一种通信装置，所述通信装置包括存储器、通信接口和处理器，其中：存储器用于存储指令；处理器用于根据执行存储器存储的指令，并控制通信接口进行信号接收和信号发送，当处理器执行存储器存储的指令时，所述通信装置用于执行上述第七方面或第七方面中任一种可能的设计中的方法。

[0040] 第九方面，本申请实施例提供一种通信装置，用于实现上述第七方面或第七方面中的任意一种方法，包括相应的功能模块，例如包括处理单元、接收单元、发送单元等，分别用于实现以上方法中的步骤。

[0041] 第十方面，本申请实施例提供一种计算机可读存储介质，所述计算机存储介质中存储有计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述第七方面或第七方面中任一种可能的设计中的方法。

[0042] 第十一方面，本申请实施例提供一种计算机程序产品，当计算机读取并执行所述

计算机程序产品时，使得计算机执行上述第七方面或第七方面中任一种可能的设计中的方法。

[0043] 第十二方面，本申请实施例提供一种芯片，所述芯片与存储器相连，用于读取并执行所述存储器中存储的软件程序，以实现上述第七方面或第七方面中任一种可能的设计中的方法。

[0044] 第十三方面，本申请实施例提供了一种通信方法，包括：

[0045] 终端设备根据所述终端设备的用户身份标识，预设参数以及所述终端设备的根密钥，获得身份认证码；

[0046] 所述终端设备向鉴权服务器功能网元发送所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文。

[0047] 根据上述方法，终端设备向鉴权服务器功能网元发送身份认证码、用户身份标识的密文，以及预设参数的明文或密文，从而可以使得鉴权网元根据所述用户身份标识以及所述预设参数对身份认证码进行校验，并在对身份认证码校验成功时，确定所述终端设备为与所述用户身份标识对应的终端设备，从而完成对所述终端设备的验证。通过上述方法，避免了由于其他设备在截取所述终端设备的用户身份标识之后，冒充所述终端设备向网络侧发送所述终端设备的用户身份标识，导致所述终端设备受到非法攻击的问题，从而提高了终端设备的安全性。

[0048] 一种可选地实施方式中，所述终端设备接收来自所述安全功能网元的认证请求，所述认证请求为所述安全功能网元根据所述鉴权网元生成的认证向量确定的。

[0049] 一种可选地实施方式中，所述终端设备根据所述终端设备的用户身份标识，预设参数以及所述终端设备的根密钥，获得身份认证码，包括：

[0050] 所述终端设备根据所述预设参数、所述根密钥以及公共密钥，获得生成参数，所述公共密钥为用于加密所述用户身份标识的密钥；

[0051] 所述终端设备根据所述生成参数和所述用户身份标识，获得所述身份认证码。

[0052] 一种可选地实施方式中，所述预设参数为序列号SQN或随机数。

[0053] 第十四方面，本申请实施例提供一种通信装置，所述通信装置包括存储器、收发机和处理器，其中：存储器用于存储指令；处理器用于根据执行存储器存储的指令，并控制收发机进行信号接收和信号发送，当处理器执行存储器存储的指令时，所述通信装置用于执行上述第十三方面或第十三方面中任一种可能的设计中的方法。

[0054] 第十五方面，本申请实施例提供一种通信装置，用于实现上述第十三方面或第十三方面中的任意一种方法，包括相应的功能模块，例如包括处理单元、接收单元、发送单元等，分别用于实现以上方法中的步骤。

[0055] 第十六方面，本申请实施例提供一种计算机可读存储介质，所述计算机存储介质中存储有计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述第十三方面或第十三方面中任一种可能的设计中的方法。

[0056] 第十七方面，本申请实施例提供一种计算机程序产品，当计算机读取并执行所述计算机程序产品时，使得计算机执行上述第一方面或第一方面中任一种可能的设计中的方法。

[0057] 第十八方面，本申请实施例提供一种芯片，所述芯片与存储器相连，用于读取并执

行所述存储器中存储的软件程序，以实现上述第十三方面或第十三方面中任一种可能的设计中的方法。

[0058] 第十九方面，本申请实施例提供了一种通信方法，所述方法包括：

[0059] 鉴权网元从鉴权服务器功能网元接收身份认证码、终端设备的用户身份标识以及预设参数；

[0060] 所述鉴权网元根据所述用户身份标识以及所述预设参数，校验所述身份认证码；

[0061] 当所述身份认证码校验成功时，所述鉴权网元向所述AUSF网元发送认证向量。

[0062] 根据上述方法，鉴权网元接收到身份认证码、终端设备的用户身份标识以及预设参数之后，根据所述用户身份标识以及所述预设参数对所述身份认证码校验成功时，可以确定所述终端设备为与所述用户身份标识对应的终端设备，从而完成对所述终端设备的验证。通过上述方法，避免了其他设备通过冒充所述终端设备的身份，从而提高了终端设备的安全性。

[0063] 一种可选地实施方式中，所述鉴权网元根据所述用户身份标识以及所述预设参数，校验所述身份认证码，包括：

[0064] 所述鉴权网元根据所述用户身份标识，获得所述终端设备的根密钥；

[0065] 所述鉴权网元根据所述根密钥以及所述预设参数获得生成参数，并根据所述生成参数、所述用户身份标识获得期望身份认证码；

[0066] 当所述期望身份认证码与所述身份认证码相同时，所述身份认证码校验成功；或者，当所述期望身份认证码与所述身份认证码不同时，所述身份认证码校验失败。

[0067] 一种可选地实施方式中，当所述身份认证码校验失败时，所述方法还包括：

[0068] 所述鉴权网元向所述AUSF网元发送失败响应。

[0069] 第二十方面，本申请实施例提供一种通信装置，所述通信装置包括存储器、通信接口和处理器，其中：存储器用于存储指令；处理器用于根据执行存储器存储的指令，并控制通信接口进行信号接收和信号发送，当处理器执行存储器存储的指令时，所述通信装置用于执行上述第二十方面或第二十方面中任一种可能的设计中的方法。

[0070] 第二十一方面，本申请实施例提供一种通信装置，用于实现上述第二十方面或第二十方面中的任意一种方法，包括相应的功能模块，例如包括处理单元、接收单元、发送单元等，分别用于实现以上方法中的步骤。

[0071] 第二十二方面，本申请实施例提供一种计算机可读存储介质，所述计算机存储介质中存储有计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述第二十方面或第二十方面中任一种可能的设计中的方法。

[0072] 第二十三方面，本申请实施例提供一种计算机程序产品，当计算机读取并执行所述计算机程序产品时，使得计算机执行上述第二十方面或第二十方面中任一种可能的设计中的方法。

[0073] 第二十四方面，本申请实施例提供一种芯片，所述芯片与存储器相连，用于读取并执行所述存储器中存储的软件程序，以实现上述第二十方面或第二十方面中任一种可能的设计中的方法。

附图说明

[0074] 图1为适用于本申请实施例的一种系统架构示意图；

[0075] 图2为本申请实施例提供的一种通信方法的流程示意图；

[0076] 图3为本申请实施例提供的另一种通信方法的流程示意图；

[0077] 图4为本申请实施例提供的另一种通信方法的流程示意图；

[0078] 图5为本申请实施例提供的另一种通信方法的流程示意图；

[0079] 图6为本申请实施例提供的又一种通信方法的流程示意图；

[0080] 图7为本申请实施例提供的一种通信装置的结构示意图；

[0081] 图8为本申请实施例提供的一种通信装置的结构示意图；

[0082] 图9为本申请实施例提供的一种通信装置的结构示意图；

[0083] 图10为本申请实施例提供的一种通信装置的结构示意图；

[0084] 图11为本申请实施例提供的一种通信装置的结构示意图；

[0085] 图12为本申请实施例提供的另一种通信装置的结构示意图；

[0086] 图13为本申请实施例提供的另一种通信装置的结构示意图；

[0087] 图14为本申请实施例提供的又一种通信装置的结构示意图。

具体实施方式

[0088] 下面将结合附图对本申请作进一步地详细描述。

[0089] 本申请实施例可以适用于如下移动通信系统，例如：长期演进(Long Term Evolution,LTE)系统、先进的长期演进(Advanced long term evolution,LTE-A)系统、通用移动通信系统(Universal Mobile Telecommunication System,UMTS)、演进的长期演进(evolved Long Term Evolution,eLTE)系统、5G系统，或未来演进的其它移动通信系统等。

[0090] 下面以5G系统为例，示例性示出了适用于本申请实施例的一种5G系统架构示意图，该系统架构可以应用于本申请各实施例，不予限制。

[0091] 如图1所示的系统架构中，终端设备101可以经接入网(Access Network,AN)网元102与核心网进行通信。核心网可以包括：会话管理功能(Session Management Function,SMF)网元103，用户面功能(user plane function,UPF)网元104，接入和移动性管理(Access and Mobility Management Function,AMF)网元105，策略控制功能(Policy Control Funtion,PCF)网元106，鉴权服务器功能(Authentication Server Function,AUSF)网元107，鉴权信任状存储和处理功能(Authentication Credential Repository and Processing Function,ARPF)网元108和安全锚点功能(Security Anchor Function,SEAF)109。

[0092] 终端设备101，可以指用户设备(User Equipment,UE)、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。终端设备还可以是蜂窝电话、无绳电话、会话启动协议(Session Initiation Protocol,SIP)电话、无线本地环路(Wireless Local Loop,WLL)站、个人数字处理(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，5G系统中的终端等。

[0093] AN网元102，也可以称之为无线接入网(Radio Access Network,RAN)网元，以下统

称为接入网网元,用于为终端设备101提供无线连接,保证终端设备101的上下行数据的可靠传输等。接入网网元102可为5G系统中的gNB(next generation Node B),可以是GSM系统或CDMA中的基站(Base Transceiver Station,BTS),也可以是WCDMA系统中的基站(NodeB,NB),还可以是LTE系统中的演进型基站(Evolved Node B,eNB或eNodeB)等。

[0094] SMF网元103,用于执行LTE系统中移动性管理实体(Mobility Management Entity,MME)的部分功能,例如,为终端设备101建立会话、管理会话等,也可以根据终端设备101的位置信息为终端设备101选择合适的UPF网元。

[0095] UPF网元104,用于分组路由和转发,用户面数据的服务质量(Quality of Service,QoS)处理等。

[0096] AMF网元105,用于移动性管理,合法监听,接入授权或鉴权等。

[0097] PCF网元106,用于为控制面、签约信息访问等提供策略等。

[0098] AUSF网元107,用于获取并处理收到的认证向量。

[0099] ARPF网元108,用于长期安全信任状的存储和处理。

[0100] SEAF网元109,用于非接入层根密钥的推演和发送。

[0101] 需要指出的是,上述系统中的SEAF网元可以与其它网元合并,例如,SEAF网元的功能也可以由AMF网元来实现,此时,上述系统可以不包含独立的SEAF网元,不予限制。

[0102] 下面对本申请中涉及的部分用语解释如下:

[0103] 鉴权网元,在5G系统中可以为ARPF网元,也可以为具备ARPF网元功能的网元等,例如,统一数据管理(Unified Data Management,UDM)网元;在4G系统中可以为归属用户服务器(Home Subscriber Server,HSS)。

[0104] 安全功能网元,在5G系统中可以为SEAF网元,也可以为AMF网元,该AMF网元可以具备SEAF功能,也可以为其它具备SEAF功能的网元等;在4G系统中,可以是移动性管理实体(Mobility Management Entity,MME)。

[0105] 在本申请中,上述提及的网元即可以是物理上的实体网元,也可以是虚拟网元,例如,物理设备上的一个功能模块等,在此不做限定。

[0106] 如图2所示,为本申请实施例提供的一种通信方法流程示意图。参见图2,该方法包括:

[0107] 步骤201:安全功能网元向终端设备发送第一认证请求。

[0108] 其中,第一认证请求可以包括鉴权令牌(authentication token,AUTN),第一认证请求可以用于请求终端设备对AUTN,换言之,用于请求对第一认证请求携带的内容进行认证,或用于请求对第一认证请求进行认证;第一认证请求还可以包括随机数(random number,RAND)。

[0109] 其中,AUTN可以采用下面的公式获得:

[0110] AUTN:=SQN xor AK||AMF||MAC

[0111] SQN为序列号(sequence number),AK为匿名密钥(anonymity key),xor为异或运算,AMF为鉴权管理域(Authentication Management Field),MAC为消息认证码(Message Authentication Code),||为拼接符。

[0112] 需要说明的是,安全功能网元可以直接向终端设备发送第一认证请求,也可以通过其它通信设备,例如,接入网设备等,向终端设备发送第一认证请求。此外,在安全功能网

元向终端设备发送第一认证请求之前，终端设备和安全功能网元之间还可以进行双向认证，属于现有技术，在此不再赘述。

[0113] 步骤202：终端设备接收来自安全功能网元的第一认证请求。

[0114] 步骤203：终端设备根据所述第一认证请求，获得认证参考信息，所述认证参考信息为响应值或再同步标识符或原因指示值。

[0115] 其中，所述响应值可以用于指示网络侧(例如，安全功能网元)对所述终端设备进行认证，或者，用于指示所述终端设备对AUTN或第一认证请求认证成功，本申请实施例不予限制。

[0116] 其中，再同步标识符可以用于请求同步所述终端设备与鉴权网元之间的序列号。

[0117] 其中，原因指示值可以用于指示所述第一认证请求验证失败的原因，例如，AMF错误，或者，终端设备与鉴权网元之间的SQN不同。

[0118] 其中，获得认证参考信息的方式可以参见下面图2至图4所示实施例中的相关描述，例如，步骤301，步骤401等。

[0119] 示例性地，当终端设备对第一认证请求验证通过时，终端设备可以根据第一认证请求生成响应值(response，RES)。当终端设备对第一认证请求校验失败，且失败的原因为：第一认证请求中的MAC验证成功，但第一认证请求中的SQN不在预设范围内时，终端设备可以生成再同步标识符(Resynchronisation Token，AUTS)。当终端设备对第一认证请求校验失败，且失败的原因为：第一认证请求中的MAC验证不成功时，终端设备可以生成原因指示值。

[0120] 步骤204：终端设备向安全功能网元发送认证响应消息。

[0121] 其中，认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元，所述认证参考信息携带在所述认证参考信息对应的信息元中。

[0122] 示例性地，当认证参考信息为响应值时，认证参考信息携带在第一信息元中；或者，当认证参考信息为再同步标识符时，证参考信息携带在第二信息元中；或者，当认证参考信息为原因指示值时，认证参考信息携带在第三信息元中。

[0123] 本申请实施例中，认证响应消息的长度可以是固定的，例如，认证响应消息为预设长度的消息。

[0124] 步骤205：安全功能网元从终端设备接收认证响应消息。

[0125] 其中，步骤206-207为可选步骤，例如，当认证响应消息中的第一信息元携带的信息验证成功时，执行步骤206；和/或，当所述第一信息元中携带的信息验证失败时，执行步骤207。

[0126] 具体的，安全功能网元可以通过以下方法对第一信息元中携带的信息进行验证：

[0127] 安全功能网元将第一认证请求对应的认证向量中的期望响应值(expected response，XRES)与第一信息元携带的信息进行比较，若相同，则第一信息元携带的信息验证成功，也可以理解为第一信息元携带的信息为响应值；否则第一信息元携带的信息验证失败，也可以理解为第一信息元携带的信息不为响应值。

[0128] 其中，所述第一认证请求对应的认证向量可以用于安全功能网元确定所述第一认证请求。具体地，第一认证请求对应的认证向量可以由鉴权网元生成并通过AUSF网元发送

至安全功能网元的。

[0129] 步骤206:安全功能网元向终端设备发送安全模式命令。

[0130] 其中,安全模式命令可以用于所述安全功能网元与终端设备进行安全密钥和算法协商。

[0131] 步骤207:安全功能网元向鉴权网元发送认证响应消息中携带的第二信息元。

[0132] 具体地,安全功能网元可以通过AUSF网元向鉴权网元发送第二信息元。

[0133] 可选地,上述方法还包括如下步骤208-212。

[0134] 步骤208:鉴权网元接收第二信息元,并对第二信息元携带的信息进行验证。

[0135] 当第二信息元携带的信息验证成功时,可以执行步骤209-210;和/或,当所述第二信息元携带的信息验证失败时,可以执行步骤211-212。

[0136] 步骤209:鉴权网元生成认证向量,并向安全功能网元发送所述认证向量。

[0137] 具体地,鉴权网元可以通过AUSF网元向安全功能网元发送所述认证向量。

[0138] 步骤210:安全功能网元接收来自鉴权网元的认证向量,并根据认证向量向终端设备发送第二认证请求。

[0139] 其中,认证向量可以包括RAND、期望响应值、密钥K_{ASME}和AUTN。

[0140] 其中,密钥K_{ASME}可以为终端设备和安全功能网元推演非接入层与接入层的锚点密钥。或者,认证向量可以包括RAND、根据期望响应值所确定的哈希值、用于终端设备和安全功能网元推演非接入层与接入层的锚点密钥和AUTN。

[0141] 具体地,安全功能网元可以将认证向量中的RAND和AUTN作为第二认证请求。

[0142] 步骤211:鉴权网元向安全功能网元发送验证结果,所述验证结果用于指示所述第二信息元携带的信息验证失败。

[0143] 具体地,鉴权网元可以通过AUSF网元向安全功能网元发送验证结果。

[0144] 步骤212:安全功能网元接收验证结果,并在所述验证结果指示所述第二信息元携带的信息验证失败时,根据所述第三信息元携带的原因指示值,获得所述终端设备对所述第一认证请求校验失败的原因。

[0145] 其中,原因指示值与对第一认证请求校验失败的原因之间可以存在对应关系,安全功能网元可以将与原因指示值对应的原因,作为终端设备对所述第一认证请求校验失败的原因。

[0146] 本实施例提供的方法中,终端设备根据第一认证请求获得的认证参考消息不论是响应值,还是再同步标识符或原因指示值,终端设备向安全功能网元发送的认证响应消息中均包括用于分别携带响应值,再同步标识符以及原因指示值的三个信息元,即终端设备发送的认证响应消息的格式为统一的格式。由于终端设备发送格式统一的认证响应消息,使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值,还是再同步标识符或原因指示值,从而无法确定终端设备是否对第一认证请求检验通过,提高了终端设备的安全性。

[0147] 当第一信息元中携带响应值时,安全功能网元在确认第一信息元中携带响应值后,可以忽略第二信息元以及第三信息元,相应的,当第一信息元中未携带响应值时,安全功能网元可以通过鉴权网元对第二信息元进行验证,从而根据第二信息元的验证结果确定第三信息元中携带的信息。上述通信方法与现有标准协议相同,因此可以在保证终端设备

安全的同时，实现与现有标准协议的兼容。

[0148] 下面分别描述不同情况下，终端设备根据所述第一认证请求获得不同的认证参考信息时，安全功能网元如何进行处理认证参考信息。

[0149] 如图3所示，为本申请实施例提供的一种通信方法流程示意图。图3所示实施例可以基于图2所示实施例，不予限制。在图3所示的流程中，以认证参考信息为响应(response，RES)值为例进行说明。

[0150] 步骤301：终端设备校验第一认证请求，当所述第一认证请求校验成功时，终端设备根据第一认证请求生成响应值。

[0151] 示例性地，终端设备根据第一认证请求获得期望(expected)消息认证码(XMAC)以及SQN，终端设备将XMAC与第一认证请求的AUTN中的MAC进行比较，若XMAC与MAC相同，且SQN位于预设范围内，表明第一认证请求校验成功，则终端设备根据所述第一认证请求生成响应值。具体的，所述终端设备可以将所述终端设备的根密钥K以及第一认证请求中的RAND作为预设函数的输入参数，并将所述预设函数以上述输入参数计算获得的输出结果作为响应值。其中，所述预设函数为现有通信标准中规定的函数，在此不再赘述。

[0152] 本申请实施例中，SQN可以根据第一认证请求中的AUTN、RAND以及K确定；XMAC可以根据RAND、K、SQN以及AUTN中的AMF确定；RES可以根据K以及RAND确定。SQN、XMAC的具体生成方式，属于现有技术，在此不再赘述。

[0153] 其中，第一认证请求可以参见图2所示实施例中的步骤201-202的相关描述，此外，步骤301可以理解为步骤203的一种具体实现方式，即步骤203可以包括步骤301，不予限制。

[0154] 步骤302：终端设备将所述响应值携带在认证响应消息的第一信息元中，将第一随机数携带在所述认证响应消息的第二信息元中，将第二随机数携带在所述认证响应消息的第三信息元中，并向安全功能网元发送所述认证响应消息。

[0155] 其中，第一随机数以及第二随机数可以是随机生成的，也可以是根据其他方式生成的，本申请实施例对此并不限定。

[0156] 步骤303：安全功能网元接收到认证响应消息之后，对所述认证响应消息中第一信息元携带的信息进行验证。

[0157] 示例性地，若所述认证响应消息中第一信息元携带的信息验证成功，则安全功能网元可以确定所述第一信息元中包括所述响应值，并忽略第二信息元以及第三信息元。

[0158] 步骤304：安全功能网元向终端设备发送安全模式命令。

[0159] 其中，安全模式命令可以用于安全功能网元与所述终端设备进行安全密钥和算法协商。

[0160] 该步骤的具体内容可以参考现有技术中的描述，在此不再赘述。

[0161] 本实施例提供的方法中，当第一信息元中携带响应值时，安全功能网元在确认第一信息元中携带响应值后，可以忽略第二信息元以及第三信息元，因此可以在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0162] 如图4所示，为本申请实施例提供的一种通信方法流程示意图。在图4所示的流程中，以认证参考信息为再同步标识符为例进行说明。

[0163] 步骤401：终端设备校验第一认证请求，当所述第一认证请求校验失败时，终端设备生成再同步标识符。

[0164] 示例性地，终端设备根据第一认证请求获得XMAC以及SQN，终端设备将XMAC与第一认证请求中的AUTN中包括的MAC进行比较，若XMAC与MAC相同，但SQN不在预设范围内，则表明第一认证请求校验失败，终端设备生成再同步标识符。

[0165] 其中，XMAC和SQN可以参见图3所示实施例中的相关描述，不再赘述。

[0166] 其中，再同步标识符可以根据SQN、AK、XMAC生成，再同步标识符的表达式可以参考如下：

[0167] AUTS＝SQN xor AK||XMAC

[0168] 其中，xor为异或运算，||为拼接符。

[0169] 其中，第一认证请求可以参见图2所示实施例中的步骤201-202中的相关描述，此外，步骤401可以理解为步骤203的一种具体实现方式，即步骤203可以包括步骤401，不予限制。

[0170] 步骤402：终端设备将第三随机数携带在认证响应消息的第一信息元中，将所述再同步标识符携带在所述认证响应消息的第二信息元中，将第二随机数携带在所述认证响应消息的第三信息元中，并向安全功能网元发送所述认证响应消息。

[0171] 其中，第三随机数可以是随机生成的，也可以是根据其他方式生成的，本申请实施例对此并不限定。

[0172] 步骤403：安全功能网元接收到认证响应消息之后，对所述认证响应消息中第一信息元携带的信息进行验证。

[0173] 其中，步骤403中对第一信息元携带的信息进行验证可以参见图3所示实施例中的相关描述，不再赘述。

[0174] 步骤404：当所述认证响应消息中第一信息元携带的信息验证失败时，安全功能网元通过AUSF网元向鉴权网元发送第二信息元。

[0175] 当然，移动管理性网元可以将第一信息元以及第三信息元也发送至鉴权网元，本申请实施例对此并不限定。

[0176] 步骤405：鉴权网元接收到第二信息元之后，对第二信息元携带的信息进行验证。

[0177] 具体的，鉴权网元可以按照终端设备生成再同步标识符的方法(该方法可以安全功能网元与终端设备预先约定的)，例如，根据SQN、AK、XMAC生成期望再同步标识符，并判断期望再同步标识符与第二消息元携带的信息是否相同，若相同，则第二信息元携带的信息验证成功，否则第二信息元携带的信息验证失败。

[0178] 步骤406a：当所述第二信息元携带的信息验证成功时，鉴权网元通过AUSF网元向安全功能网元发送认证向量。

[0179] 步骤407：安全功能网元接收鉴权网元发送的认证向量之后，确定第二信息元中携带的信息验证成功，向终端设备发送所述第二认证请求。

[0180] 可替换地，当步骤405中所述第二信息元携带的信息验证失败时，步骤406a和407可以替换为步骤406b：

[0181] 步骤406b：当所述第二信息元携带的信息验证失败时，鉴权网元通过AUSF网元向安全功能网元发送验证结果，所述验证结果用于指示所述第二信息元携带的信息验证失败。

[0182] 本实施例提供的方法中，安全功能网元在确认第一信息元中未携带响应值后，可

以在确定第二信元中携带的信息验证成功时，忽略第三信元并确定终端设备对第一认证请求校验失败的原因，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0183] 如图5所示，为本申请实施例提供的一种通信方法流程示意图。在图5所示的流程中，以认证参考信息为原因指示值为例进行说明。

[0184] 步骤501：终端设备校验第一认证请求，当第一认证请求校验失败时，终端设备获得验证失败的原因指示值。

[0185] 示例性地，终端设备根据第一认证请求计算出XMAC以及SQN，终端将XMAC与第一认证请求中的AUTN中包括的MAC进行比较，若XMAC与MAC不相同，则表明第一认证请求验证失败，终端设备获得该验证失败对应的原因指示值。

[0186] 其中，XMAC和SQN可以参见图3所示实施例中的相关描述，不再赘述。

[0187] 其中，第一认证请求可以参见图2所示实施例中的步骤201-202中的相关描述，此外，步骤501可以理解为步骤203的一种具体实现方式，即步骤203可以包括步骤501，不予限制。

[0188] 步骤502：终端设备将第三随机数携带在认证响应消息的第一信息元中，将第二随机数携带在所述认证响应消息的第二信息元中，将原因指示值携带在所述认证响应消息的第三信息元中，并向安全功能网元发送所述认证响应消息。

[0189] 其中，第三随机数可以是随机生成的，也可以是根据其他方式生成的，本申请实施例对此并不限定。

[0190] 步骤503：安全功能网元接收到认证响应消息之后，对所述认证响应消息中第一信息元携带的信息进行验证。

[0191] 其中，步骤503中对第一信息元携带的信息进行验证可以参见图4所示实施例中的相关描述，不再赘述。

[0192] 步骤504：当所述认证响应消息中第一信息元携带的信息验证失败时，安全功能网元通过AUSF网元向鉴权网元发送第二信息元。

[0193] 当然，移动管理性网元可以将第一信息元以及第三信息元也发送至鉴权网元，本申请实施例对此并不限定。

[0194] 步骤505：鉴权网元接收到第二信息元之后，对第二信息元携带的信息进行验证。

[0195] 其中，步骤505中对第二信息元携带的信息进行验证可以参见图4所示实施例中的相关描述，不再赘述。

[0196] 步骤506：当所述第二信息元携带的信息验证失败时，鉴权网元通过AUSF网元向安全功能网元发送验证结果，所述验证结果用于指示所述第二信息元携带的信息验证失败。

[0197] 步骤507：安全功能网元接收验证结果，并在所述验证结果指示所述第二信息元携带的信息验证失败时，根据所述第三信息元携带的原因指示值，获得所述终端设备对所述第一认证请求校验失败的原因。

[0198] 本实施例提供的方法中，安全功能网元在确认第一信息元中未携带响应值后，可以在确定第二信元中携带的信息验证失败时，根据第三信元携带的原因指示值，获得所述终端设备对所述第一认证请求校验失败的原因，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0199] 本申请实施例中，在安全功能网元向终端设备发送认证请求之前，还可以对终端

设备进行验证，并在验证通过后向终端设备发送认证请求，下面详细描述。

[0200] 如图6所示，为本申请实施例提供的一种通信方法流程示意图。该方法可以基于图2-5所示的任一实施例，不予限制。参见图6，该方法包括：

[0201] 步骤601：终端设备根据所述终端设备的用户身份标识，预设参数以及所述终端设备的根密钥，获得身份认证码。

[0202] 其中，身份认证码可以用于对终端设备的用户身份标识进行签名。

[0203] 其中，用户身份标识可以为终端设备的身份用户永久身份标识(Subscriber Permanent Identity，SUPI)、国际移动用户识别码(International Mobile Subscriber Identification Number，IMSI)等，在此不再逐一举例说明。

[0204] 具体的，步骤601可以包括：所述终端设备根据所述预设参数、所述根密钥以及公共密钥，获得生成参数；所述终端设备根据所述生成参数和所述用户身份标识，获得所述身份认证码。

[0205] 其中，所述公共密钥可以为用于加密所述用户身份标识的密钥，所述公共密钥可以为核心网预先为终端配置的。

[0206] 例如，终端设备对所述预设参数、所述根密钥以及公共密钥进行哈希计算，将计算的结果作为所述生成参数。进一步地，为对生成参数和用户身份标识进行哈希计算，将计算的结果作为身份认证码。

[0207] 其中，预设参数可以为SQN或随机数，也可以为根据其他方式生成的数，本申请实施例对此并不限定。

[0208] 需要指出的是，当预设参数为随机数时，可以仅在SQN发生改变的情况下生成一个新的随机数，限定了预设参数的生成次数，避免恶意设备在获得足够多数量的预设参数时，通过暴力破解的方法获得身份认证码。

[0209] 步骤602：所述终端设备向AUSF网元发送所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文。

[0210] 其中，所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文可以由终端设备通过安全功能网元发送至AUSF网元的。其中，所述安全功能网元可以参见图2所示实施例中的相关描述，不再赘述。

[0211] 例如，终端设备所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文可以携带在注册请求消息或附着请求消息中发送至安全功能网元；进一步地，安全功能网元将身份认证码、所述终端设备的用户身份标识以及预设参数发送至AUSF网元。

[0212] 其中，所述用户身份标识的密文可以为将用户身份标识用公共密钥加密后的比特序列，相应的，预设参数的密文可以为将预设参数用公共密钥加密后的比特序列。

[0213] 步骤603：AUSF网元从安全功能网元接收身份认证码、所述终端设备的用户身份标识以及预设参数，并向鉴权网元发送身份认证码、所述终端设备的用户身份标识以及预设参数。

[0214] 步骤604：鉴权网元从AUSF网元接收身份认证码、终端设备的用户身份标识以及预设参数。

[0215] 步骤605：所述鉴权网元根据所述用户身份标识以及所述预设参数，校验所述身份

认证码;当所述身份认证码校验成功时,所述鉴权网元向所述AUSF网元发送认证向量。

[0216] 具体的,步骤605可以包括:

[0217] 所述鉴权网元可以根据所述用户身份标识,获得与所述用户身份标识对应的终端设备的根密钥;其中,用户身份标识与根密钥的对应关系为预先设置;

[0218] 所述鉴权网元根据所述根密钥以及所述预设参数获得生成参数,并根据所述生成参数、所述用户身份标识获得期望身份认证码;

[0219] 所述鉴权网元将期望身份认证码与接收到的身份认证码进行比较,当所述期望身份认证码与所述身份认证码相同时,可以确定所述身份认证码校验成功;或者,当所述期望身份认证码与所述身份认证码不同时,可以确定所述身份认证码校验失败。

[0220] 相应地,AUSF网元接收到所述认证向量之后,向安全功能网元发送所述认证向量。

[0221] 步骤606:安全功能网元接收AUSF网元发送的认证向量,根据所述认证向量向所述终端设备发送认证请求。

[0222] 其中,安全功能网元可以根据认证向量确定认证请求的具体内容,可以参考图2所示实施例中的相关描述,不再赘述。

[0223] 步骤607:所述终端设备接收来自所述安全功能网元的认证请求。

[0224] 其中,所述认证请求为所述安全功能网元根据所述鉴权网元生成的认证向量确定的。

[0225] 本实施例提供的方法中,终端设备发送身份认证码、用户身份标识的密文,以及预设参数的明文或密文之后,鉴权网元可以根据所述用户身份标识以及所述预设参数对身份认证码进行校验,并在对身份认证码校验成功时,确定所述终端设备为与所述用户身份标识对应的终端设备,从而完成对所述终端设备的验证。通过上述方法,避免了由于其他设备在截取所述终端设备的用户身份标识之后,冒充所述终端设备从而导致所述终端设备受到非法攻击的问题,从而提高了终端设备的安全性。

[0226] 可选的,当所述身份认证码校验失败时,所述鉴权网元可以向所述AUSF网元发送失败响应,所述失败响应指示所述终端设备请求认证请求失败。AUSF网元可以将所述失败响应转发至移动管理系统网元,移动管理系统网元可以根据所述失败响应向所述终端设备发送拒绝响应消息,从而拒绝所述终端设备的请求(例如,注册请求或附着请求)。在该场景下,当所述身份认证码校验失败时,所述鉴权网元可以确定发送所述用户身份标识的终端设备并不是拥有所述用户身份标识的合法设备,因此不会向AUSF网元发送认证向量,从而可以避免其他设备根据认证向量获取所述终端设备的认证请求,从而提高终端设备的安全性。

[0227] 如图7所示,为本申请实施例提供一种通信装置的结构示意图,该通信装置700可以用于执行图2至图5任一所示的流程中的终端设备的动作。该通信装置700可以是终端设备或终端设备内的芯片或片上系统。具体地,通信装置700包括收发单元701和处理单元702。

[0228] 收发单元701,用于接收来自安全功能网元的第一认证请求。

[0229] 处理单元702,用于根据所述第一认证请求,获得认证参考信息,所述认证参考信息为响应值或再同步标识符或原因指示值。

[0230] 所述收发单元701,用于向所述安全功能网元发送认证响应消息,所述认证响应消

息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元，所述认证参考信息携带在所述认证参考信息对应的信息元中。

[0231] 上述方案中，终端设备根据第一认证请求获得的认证参考消息不论是响应值，还是再同步标识符或原因指示值，终端设备向安全功能网元发送的认证响应消息中均包括第一信息元、第二信息元以及第三信息元。通过该方法，终端设备发送的认证响应消息的格式为统一的格式，使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值，还是再同步标识符或原因指示值，从而无法确定终端设备是否对第一认证请求检验通过，从而提高了终端设备的安全性。

[0232] 一种可选地实施方式中，所述认证参考信息为所述响应值；

[0233] 收发单元701向所述安全功能网元发送认证响应消息之前，处理单元702还用于：

[0234] 将所述认证参考信息携带在所述第一信息元中，将第一随机数携带在所述第二信息元中，将第二随机数携带在所述第三信息元中。

[0235] 上述方案中，终端设备可以将认证参考消息、第一随机数以及第二随机数，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。网络侧(例如，安全功能网元)在确认第一信息元中携带响应值后，可以忽略第二信息元以及第三信息元，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0236] 一种可选地实施方式中，所述认证参考信息为所述再同步标识符；

[0237] 收发单元701向所述安全功能网元发送认证响应消息之前，处理单元702还用于：

[0238] 将所述认证参考信息携带在所述第二信息元中，将第三随机数携带在所述第一信息元中，将第二随机数携带在所述第三信息元中。

[0239] 上述方案中，终端设备可以将第三随机数、认证参考消息以及第二随机数，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。网络侧(例如，安全功能网元)在确认第一信息元中未携带响应值后，可以根据第二信息元以及第三信息元获得所述终端设备对所述第一认证请求校验失败的原因，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0240] 一种可选地实施方式中，所述认证参考信息为所述原因指示值；

[0241] 收发单元701向所述安全功能网元发送认证响应消息之前，处理单元702还用于：

[0242] 将所述认证参考信息携带在所述第三信息元中，将第三随机数携带在所述第一信息元中，将第一随机数携带在所述第二信息元中。

[0243] 上述方案中，终端设备可以将第三随机数、第一随机数以及认证参考消息，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。网络侧(例如，安全功能网元)可以在确定第一信息元以及第二信元中携带的信息验证失败时，根据第三信元携带的原因指示值，获得所述终端设备对所述第一认证请求校验失败的原因，从而在保证终端设备安全的同时，实现与现有标准协议的兼容。

[0244] 如图8所示，为本申请实施例提供一种通信装置的结构示意图，该通信装置800可执行图2至图5任一所示的流程中的安全功能网元的动作。该通信装置800可以是安全功能网元或安全功能网元内的芯片或片上系统。

[0245] 该通信装置800包括收发单元801和处理单元802。

[0246] 收发单元801，用于向终端设备发送第一认证请求；接收来自所述终端设备的认证

响应消息，所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元。

[0247] 处理单元802，用于当确定所述第一信息元携带的信息验证成功时，通过所述收发单元801向所述终端设备发送安全模式命令。

[0248] 上述方案中，安全功能网元接收到认证响应消息之后，在确定认证响应消息中第一信息元携带的信息验证成功时，忽略认证响应消息中的第二信息元以及第三信息元，并与终端设备进行安全密钥和算法协商。由于终端设备发送的认证响应消息的格式为统一的格式，使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值，还是再同步标识符或原因指示值，从而无法确定终端设备是否对第一认证请求检验通过，从而提高了终端设备的安全性。

[0249] 一种可选地实施方式中，处理单元802还用于：

[0250] 当所述第一信息元携带的信息验证失败时，通过收发单元801向鉴权网元发送所述第二信息元；

[0251] 通过收发单元801接收来自所述鉴权网元的认证向量，并根据所述认证向量向所述终端设备发送第二认证请求；或者，通过收发单元801接收来自所述鉴权网元的验证结果，所述验证结果用于指示所述第二信息元携带的信息验证失败，所述安全功能网元根据所述第三信息元携带的原因指示值向所述终端设备发送认证拒绝消息。

[0252] 如图9所示，为本申请实施例提供一种通信装置的结构示意图，该通信装置900可执行图6所示的流程中的终端设备的动作。该通信装置900可以是终端设备或终端设备内的芯片或片上系统。该通信装置900包括处理单元901和收发单元902。

[0253] 处理单元901，用于根据所述终端设备的用户身份标识，预设参数以及所述终端设备的根密钥，获得身份认证码。

[0254] 收发单元902，用于向AUSF网元发送所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文。

[0255] 上述方案中，终端设备向鉴权服务器功能网元发送身份认证码、用户身份标识的密文，以及预设参数的明文或密文，从而可以使得鉴权网元根据所述用户身份标识以及所述预设参数对身份认证码进行校验，并在对身份认证码校验成功时，确定所述终端设备为与所述用户身份标识对应的终端设备，从而完成对所述终端设备的验证。通过上述方法，避免了由于其他设备在截取所述终端设备的用户身份标识之后，冒充所述终端设备向网络侧发送所述终端设备的用户身份标识，导致所述终端设备受到非法攻击的问题，从而提高了终端设备的安全性。

[0256] 一种可选地实施方式中，收发单元902还用于：

[0257] 接收来自所述安全功能网元的认证请求，所述认证请求为所述安全功能网元根据所述鉴权网元生成的认证向量确定的。

[0258] 一种可选地实施方式中，处理单元901具体用于：

[0259] 根据所述预设参数、所述根密钥以及公共密钥，获得生成参数，所述公共密钥为用于加密所述用户身份标识的密钥；

[0260] 根据所述生成参数和所述用户身份标识，获得所述身份认证码。

[0261] 一种可选地实施方式中，所述预设参数为序列号SQN或随机数。

[0262] 如图10所示，为本申请实施例提供一种通信装置的结构示意图，该通信装置1000可执行图6所示的流程中的鉴权网元的动作。该通信装置1000可以是鉴权网元或鉴权网元内的芯片或片上系统。该通信装置1000包括收发单元1001和处理单元1002。

[0263] 收发单元1001，用于从AUSF网元接收身份认证码、终端设备的用户身份标识以及预设参数。

[0264] 处理单元1002，用于根据所述用户身份标识以及所述预设参数，校验所述身份认证码；当所述身份认证码校验成功时，通过收发单元1001向所述AUSF网元发送认证向量。

[0265] 上述方案中，鉴权网元接收到身份认证码、终端设备的用户身份标识以及预设参数之后，根据所述用户身份标识以及所述预设参数对所述身份认证码校验成功时，可以确定所述终端设备为与所述用户身份标识对应的终端设备，从而完成对所述终端设备的验证。通过上述方法，避免了其他设备通过冒充所述终端设备的身份，从而提高了终端设备的安全性。

[0266] 一种可选地实施方式中，所述处理单元1002具体用于：

[0267] 根据所述用户身份标识，获得所述终端设备的根密钥；

[0268] 根据所述根密钥以及所述预设参数获得生成参数，并根据所述生成参数、所述用户身份标识获得期望身份认证码；

[0269] 当所述期望身份认证码与所述身份认证码相同时，所述身份认证码校验成功；或者，当所述期望身份认证码与所述身份认证码不同时，所述身份认证码校验失败。

[0270] 一种可选地实施方式中，当所述身份认证码校验失败时，所述收发单元1001还用于：

[0271] 向所述AUSF网元发送失败响应。

[0272] 如图11所示，为本申请实施例提供一种通信装置的结构示意图，该通信装置1100可以为终端设备，可用于执行图2至图5任一所示的流程中的终端设备的动作。

[0273] 参见图11，该通信装置1100包括：处理器1101、收发机1102、存储器1103；其中，处理器1101、收发机1102、存储器1103通过总线1104相互连接。

[0274] 处理器1101可以是中央处理器(central processing unit，CPU)，网络处理器(network processor，NP)或者CPU和NP的组合。处理器1101还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路(application-specific integrated circuit，ASIC)，可编程逻辑器件(programmable logic device，PLD)或其组合。上述PLD可以是复杂可编程逻辑器件(complex programmable logic device，CPLD)，现场可编程逻辑门阵列(field-programmable gate array，FPGA)，通用阵列逻辑(generic array logic，GAL)或其任意组合。

[0275] 存储器1103可以包括易失性存储器(volatile memory)，例如随机存取存储器(random-access memory，RAM)；存储器也可以包括非易失性存储器(non-volatile memory)，例如快闪存储器(flash memory)，硬盘(hard disk drive，HDD)或固态硬盘(solid-state drive，SSD)；存储器1103还可以包括上述种类的存储器的组合。

[0276] 总线1104可以是外设部件互连标准(peripheral component interconnect，PCI)总线或扩展工业标准结构(extended industry standard architecture，EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图11中仅用一条双向箭头表示，

但并不表示仅有一根总线或一种类型的总线。

[0277] 存储器1103可以用于存储程序指令，处理器1101调用该存储器1103中存储的程序指令，可以执行上述各方法实施例中终端设备的一个或多个步骤，或其中可选的实施方式，使得通信装置1100实现上述方法中的功能。

[0278] 收发机1102，用于接收来自安全功能网元的第一认证请求。

[0279] 处理器1101，用于根据所述第一认证请求，获得认证参考信息，所述认证参考信息为响应值或再同步标识符或原因指示值。

[0280] 收发机1102，用于向所述安全功能网元发送认证响应消息，所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元，所述认证参考信息携带在所述认证参考信息对应的信息元中。

[0281] 上述方案中，通信装置根据第一认证请求获得的认证参考消息不论是响应值，还是再同步标识符或原因指示值，并向安全功能网元发送的认证响应消息中均包括第一信息元、第二信息元以及第三信息元。通过该方法，通信装置发送的认证响应消息的格式为统一的格式，使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值，还是再同步标识符或原因指示值，从而无法确定通信装置是否对第一认证请求检验通过，从而提高了该通信装置的安全性。

[0282] 一种可选地实施方式中，所述认证参考信息为所述响应值；

[0283] 收发机1102向所述安全功能网元发送认证响应消息之前，处理器1101还用于：

[0284] 将所述认证参考信息携带在所述第一信息元中，将第一随机数携带在所述第二信息元中，将第二随机数携带在所述第三信息元中。

[0285] 上述方案中，通信装置可以将认证参考消息、第一随机数以及第二随机数，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。网络侧(例如，安全功能网元)在确认第一信息元中携带响应值后，可以忽略第二信息元以及第三信息元，从而在保证通信装置安全的同时，实现与现有标准协议的兼容。

[0286] 一种可选地实施方式中，所述认证参考信息为所述再同步标识符；

[0287] 收发机1102向所述安全功能网元发送认证响应消息之前，处理器1101还用于：

[0288] 将所述认证参考信息携带在所述第二信息元中，将第三随机数携带在所述第一信息元中，将第二随机数携带在所述第三信息元中。

[0289] 上述方案中，通信装置可以将第三随机数、认证参考消息以及第二随机数，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应消息。网络侧(例如，安全功能网元)在确认第一信息元中未携带响应值后，可以根据第二信息元以及第三信息元获得通信装置对所述第一认证请求校验失败的原因，从而在保证通信装置安全的同时，实现与现有标准协议的兼容。

[0290] 一种可选地实施方式中，所述认证参考信息为所述原因指示值；

[0291] 收发机1102向所述安全功能网元发送认证响应消息之前，处理器1101还用于：

[0292] 将所述认证参考信息携带在所述第三信息元中，将第三随机数携带在所述第一信息元中，将第一随机数携带在所述第二信息元中。

[0293] 上述方案中，通信装置可以将第三随机数、第一随机数以及认证参考消息，分别携带在第一信息元、第二信息元以及第三信息元中，从而可以实现生成格式统一的认证响应

消息。网络侧(例如,安全功能网元)可以在确定第一信息元以及第二信元中携带的信息验证失败时,根据第三信元携带的原因指示值,获得所述通信装置对所述第一认证请求校验失败的原因,从而在保证通信装置安全的同时,实现与现有标准协议的兼容。

[0294] 本申请实施例提供还一种通信装置,所述通信装置包括处理器、存储器。所述存储器中存储有计算机程序,所述处理器读取并执行所述存储器中存储的计算机程序时,使得所述通信装置实现如图2至图5任一所示的流程中的终端设备所执行的方法。

[0295] 本申请实施例还提供一种芯片,所述芯片与存储器相连,所述存储器中存储有计算机程序,所述芯片用于读取并执行所述存储器中存储的计算机程序,以实现如图2至图5任一所示的流程中的终端设备所执行的方法。

[0296] 如图12所示,为本申请实施例提供一种通信装置的结构示意图,该通信装置1200可执行图2至图5任一所示的流程中的安全功能网元的动作。

[0297] 该通信装置1200包括:处理器1201、通信接口1202、存储器1203;其中,处理器1201、通信接口1202、存储器1203通过总线1204相互连接,上述模块的具体内容可以参考图11中相关模块的描述,在此不再赘述。

[0298] 通信接口1202可以为有线通信接入口,无线通信接口或其组合,其中,有线通信接口例如可以为以太网接口。以太网接口可以是光接口,电接口或其组合。无线通信接口可以为无线局域网接口。

[0299] 通信接口1202,用于向终端设备发送第一认证请求;接收来自所述终端设备的认证响应消息,所述认证响应消息包括用于携带响应值的第一信息元、用于携带再同步标识符的第二信息元以及用于携带原因指示值的第三信息元。

[0300] 处理器1201,用于当确定所述第一信息元携带的信息验证成功时,通过通信接口1202向所述终端设备发送安全模式命令。

[0301] 上述方案中,通信装置接收到认证响应消息之后,在确定认证响应消息中第一信息元携带的信息验证成功时,忽略认证响应消息中的第二信息元以及第三信息元,并与终端设备进行安全密钥和算法协商。由于终端设备发送的认证响应消息的格式为统一的格式,使得其他设备无法直接根据认证响应消息的格式确定认证响应消息中携带的是响应值,还是再同步标识符或原因指示值,从而无法确定终端设备是否对第一认证请求检验通过,从而提高了终端设备的安全性。

[0302] 一种可选地实施方式中,所述处理器1201还用于:

[0303] 当所述第一信息元携带的信息验证失败时,通过通信接口1202向鉴权网元发送所述第二信息元。

[0304] 通过通信接口1202接收来自所述鉴权网元的认证向量,并根据所述认证向量向所述终端设备发送第二认证请求;或者,通过通信接口1202接收来自所述鉴权网元的验证结果,所述验证结果用于指示所述第二信息元携带的信息验证失败,所述安全功能网元根据所述第三信息元携带的原因指示值向所述终端设备发送认证拒绝消息。

[0305] 如图13所示,为本申请实施例提供一种通信装置结构示意图,该通信装置1300可执行图6所示的流程中的终端设备的动作。

[0306] 该通信装置1300包括:处理器1301、收发机1302、存储器1303;其中,处理器1301、收发机1302、存储器1303通过总线1304相互连接,上述模块的具体内容可以参考图11中相

关模块的描述，在此不再赘述。

[0307] 处理器1301，用于根据所述终端设备的用户身份标识，预设参数以及所述通信装置的根密钥，获得身份认证码。

[0308] 收发机1302，用于向鉴权服务器功能AUSF网元发送所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文。

[0309] 上述方案中，通信装置向鉴权服务器功能网元发送身份认证码、用户身份标识的密文，以及预设参数的明文或密文，从而可以使得鉴权网元根据所述用户身份标识以及所述预设参数对身份认证码进行校验，并在对身份认证码校验成功时，确定所述通信装置为与所述用户身份标识对应的设备，从而完成对所述通信装置的验证。通过上述方法，避免了由于其他设备在截取所述通信装置的用户身份标识之后，冒充所述通信装置向网络侧发送所述通信装置的用户身份标识，导致所述通信装置受到非法攻击的问题，从而提高了通信装置的安全性。

[0310] 一种可选地实施方式中，收发机1302还用于：接收来自所述安全功能网元的认证请求，所述认证请求为所述安全功能网元根据所述鉴权网元生成的认证向量确定的。

[0311] 一种可选地实施方式中，处理器1301具体用于：根据所述预设参数、所述根密钥以及公共密钥，获得生成参数，所述公共密钥为用于加密所述用户身份标识的密钥；根据所述生成参数和所述用户身份标识，获得所述身份认证码。

[0312] 一种可选地实施方式中，所述预设参数为序列号SQN或随机数。

[0313] 本申请实施例提供还一种通信装置，所述通信装置包括处理器、存储器。所述存储器中存储有计算机程序，所述处理器读取并执行所述存储器中存储的计算机程序时，使得所述通信装置实现如图6所示的流程中的终端设备所执行的方法。

[0314] 本申请实施例还提供一种芯片，所述芯片与存储器相连，所述存储器中存储有计算机程序，所述芯片用于读取并执行所述存储器中存储的计算机程序，以实现如图6所示的流程中的终端设备所执行的方法。

[0315] 如图14所示，为本申请实施例提供一种通信装置结构示意图，该通信装置1400可执行图6所示的流程中的鉴权网元的动作。

[0316] 该通信装置1400包括：处理器1401、通信接口1402、存储器1403；其中，处理器1401、通信接口1402、存储器1403通过总线1404相互连接，上述模块的具体内容可以参考图11中相关模块的描述，在此不再赘述。

[0317] 通信接口1402，用于从鉴权服务器功能AUSF网元接收身份认证码、终端设备的用户身份标识以及预设参数。

[0318] 处理器1401，用于根据所述用户身份标识以及所述预设参数，校验所述身份认证码；当所述身份认证码校验成功时，通过通信接口402向所述AUSF网元发送认证向量。

[0319] 上述方案中，通信装置接收到身份认证码、终端设备的用户身份标识以及预设参数之后，根据所述用户身份标识以及所述预设参数对所述身份认证码校验成功时，可以确定所述终端设备为与所述用户身份标识对应的终端设备，从而完成对所述终端设备的验证。通过上述方法，避免了其他设备通过冒充所述终端设备的身份，从而提高了终端设备的安全性。

[0320] 一种可选地实施方式中，处理器1401具体用于：根据所述用户身份标识，获得所述

终端设备的根密钥;根据所述根密钥以及所述预设参数获得生成参数,并根据所述生成参数、所述用户身份标识获得期望身份认证码;当所述期望身份认证码与所述身份认证码相同时,所述身份认证码校验成功;或者,当所述期望身份认证码与所述身份认证码不同时,所述身份认证码校验失败。

[0321] 一种可选地实施方式中,当所述身份认证码校验失败时,通信接口1402还用于:向所述AUSF网元发送失败响应。

[0322] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、光学存储器等)上实施的计算机程序产品的形式。

[0323] 本申请是参照根据本申请的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0324] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0325] 显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

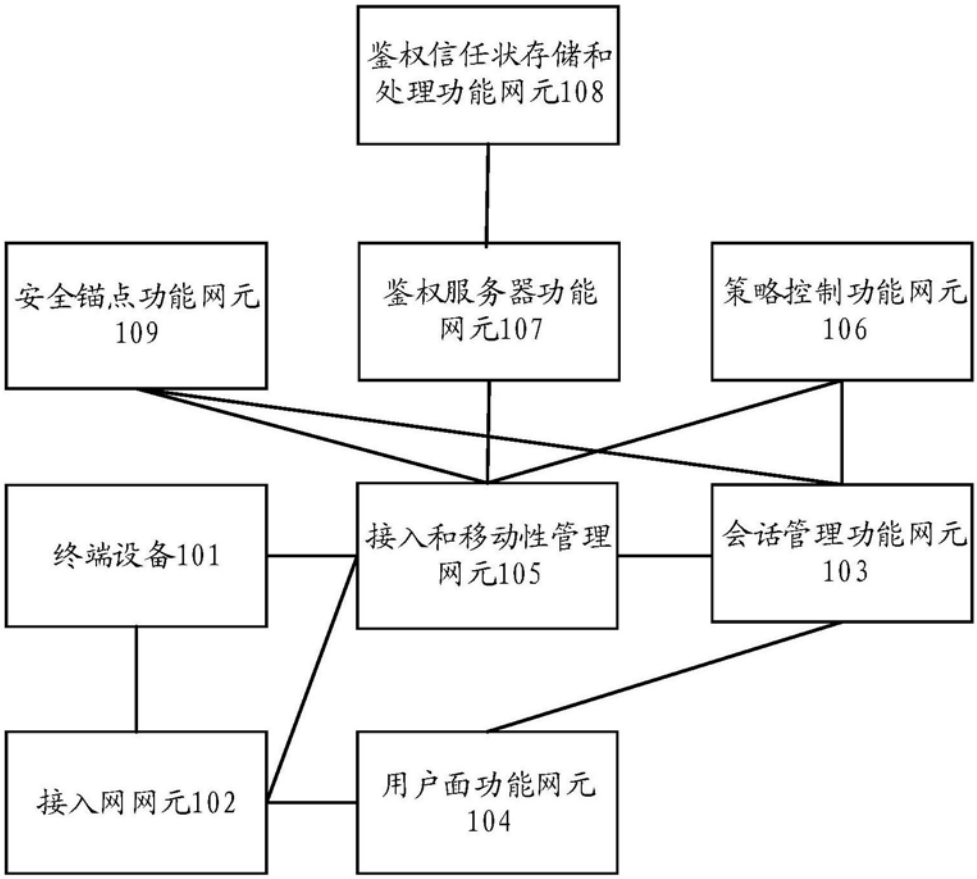

鉴权信任状存储和处理功能网元108
安全锚点功能网元109
鉴权服务器功能网元107
策略控制功能网元106
终端设备101
接入和移动性管理网元105
会话管理功能网元103
接入网网元102
用户面功能网元104

图1

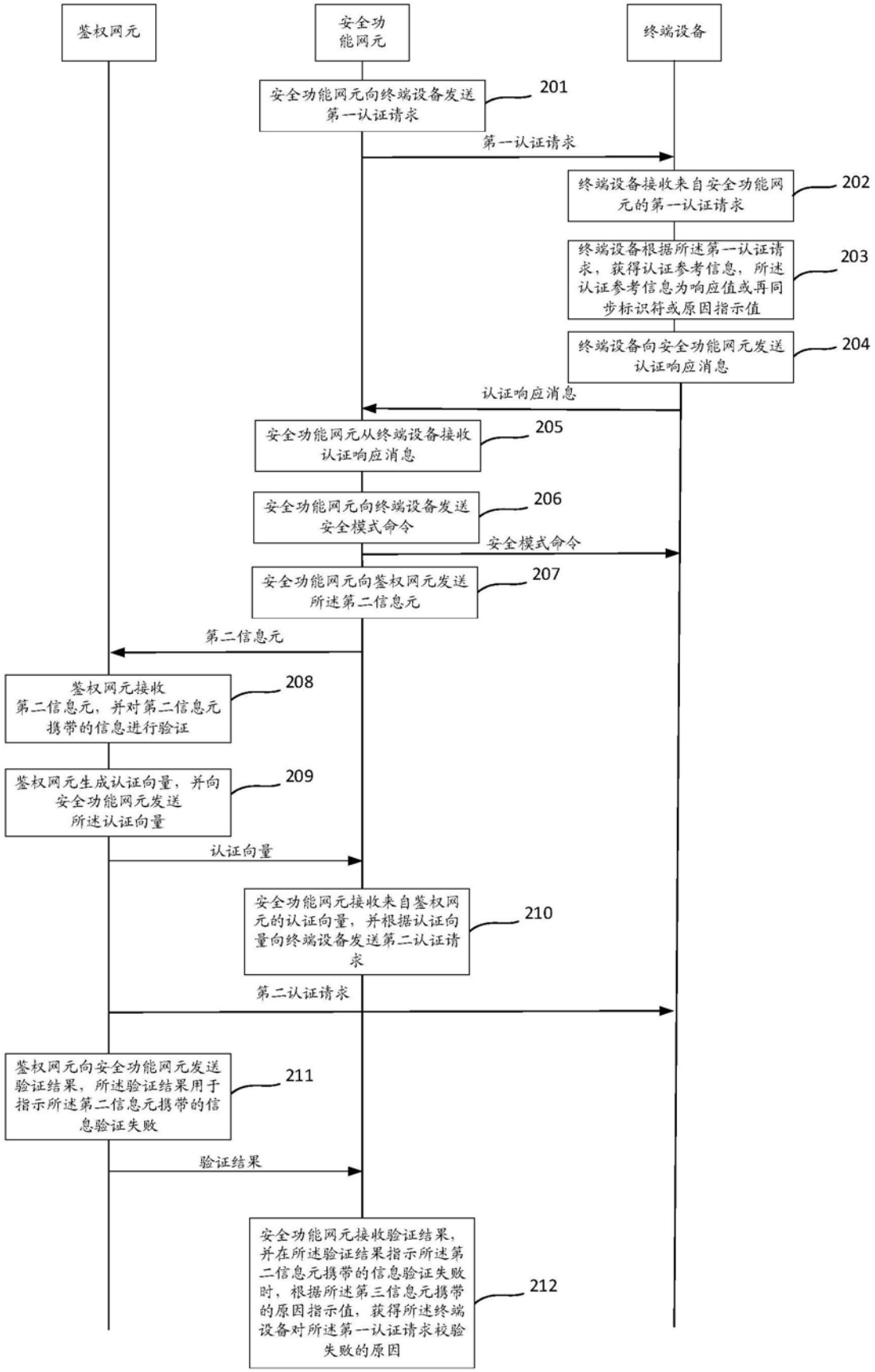

鉴权网元
安全功能网元
终端设备
安全功能网元向终端设备发送第一认证请求
201
第一认证请求
终端设备接收来自安全功能网元的第一认证请求
202
终端设备根据所述第一认证请求，获得认证参考信息，所述认证参考信息为响应值或再同步标识符或原因指示值
203
终端设备向安全功能网元发送认证响应消息
204
认证响应消息
安全功能网元从终端设备接收认证响应消息
205
安全功能网元向终端设备发送安全模式命令
206
安全模式命令
安全功能网元向鉴权网元发送所述第二信息元
207
第二信息元
鉴权网元接收第二信息元，并对第二信息元携带的信息进行验证
208
鉴权网元生成认证向量，并向安全功能网元发送所述认证向量
209
认证向量
安全功能网元接收来自鉴权网元的认证向量，并根据认证向量向终端设备发送第二认证请求
210
第二认证请求
鉴权网元向安全功能网元发送验证结果，所述验证结果用于指示所述第二信息元携带的信息验证失败
211
验证结果
安全功能网元接收验证结果，并在所述验证结果指示所述第二信息元携带的信息验证失败时，根据所述第三信息元携带的原因指示值，获得所述终端设备对所述第一认证请求校验失败的原因
212

图2

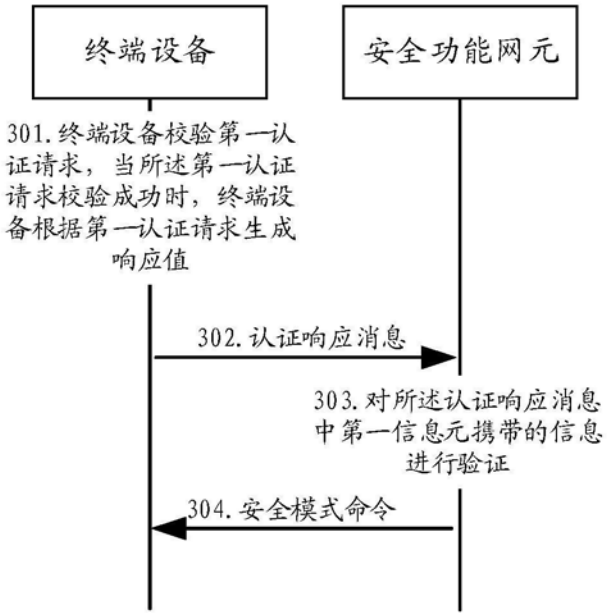

终端设备
安全功能网元
301.终端设备校验第一认证请求，当所述第一认证请求校验成功时，终端设备根据第一认证请求生成响应值
302.认证响应消息
303.对所述认证响应消息中第一信息元携带的信息进行验证
304.安全模式命令

图3

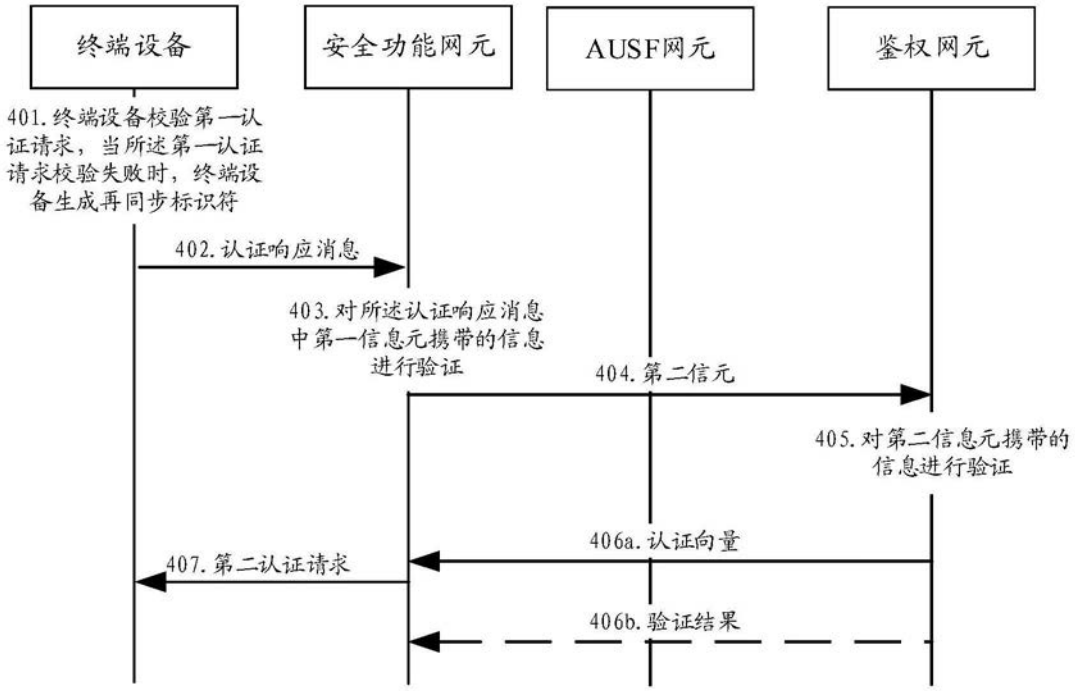

终端设备
安全功能网元
AUSF网元
鉴权网元
401.终端设备校验第一认证请求，当所述第一认证请求校验失败时，终端设备生成再同步标识符
402.认证响应消息
403.对所述认证响应消息中第一信息元携带的信息进行验证
404.第二信元
405.对第二信息元携带的信息进行验证
406a.认证向量
407.第二认证请求
406b.验证结果

图4

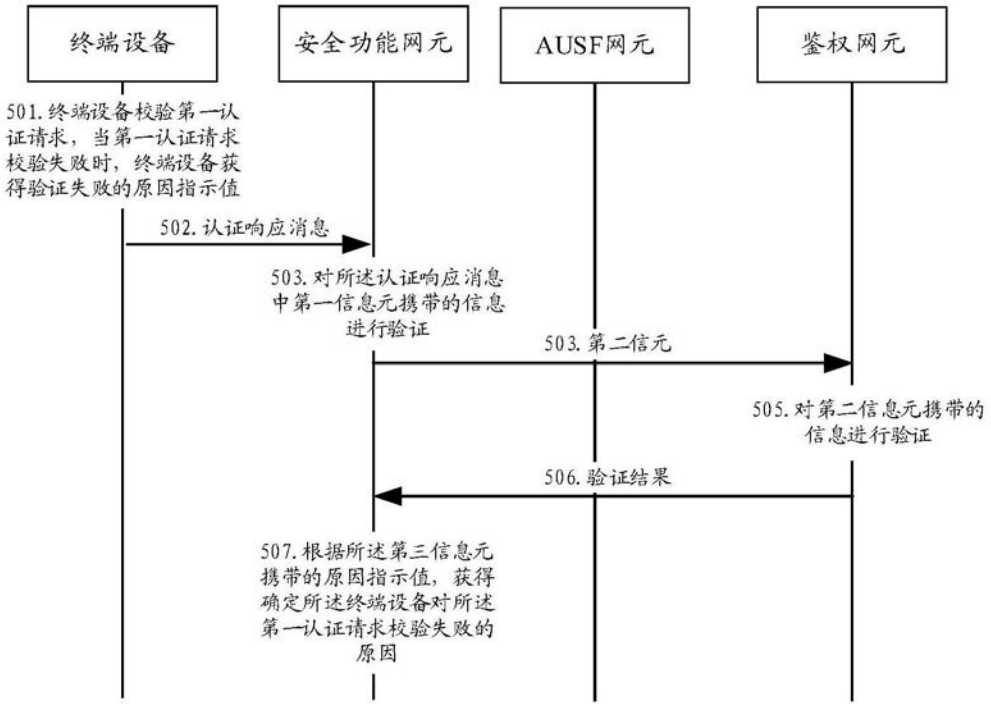

终端设备
安全功能网元
AUSF网元
鉴权网元
501.终端设备校验第一认证请求，当第一认证请求校验失败时，终端设备获得验证失败的原因指示值
502.认证响应消息
503.对所述认证响应消息中第一信息元携带的信息进行验证
503.第二信元
505.对第二信息元携带的信息进行验证
506.验证结果
507.根据所述第三信息元携带的原因指示值，获得确定所述终端设备对所述第一认证请求校验失败的原因

图5

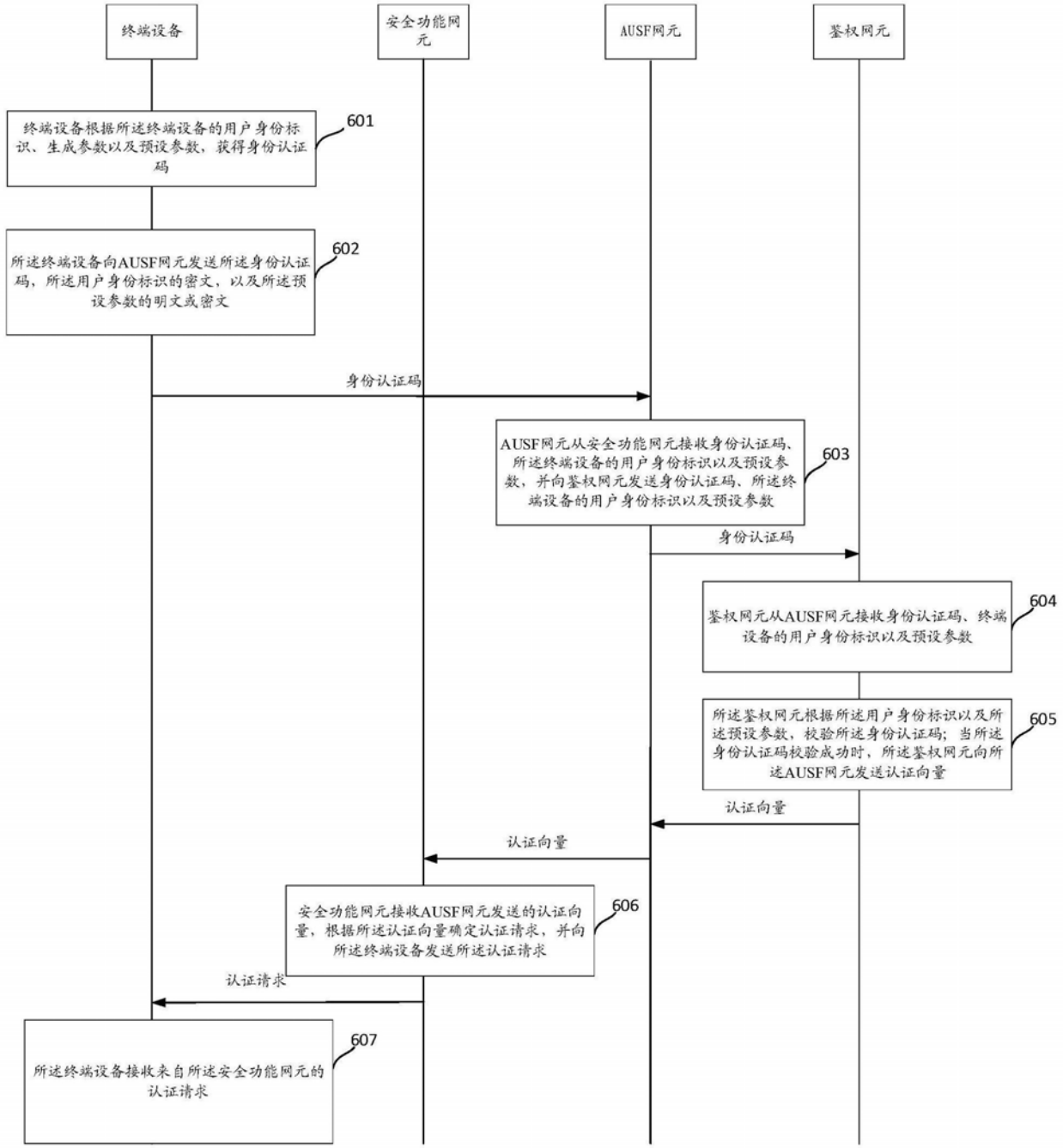

终端设备
安全功能网元
AUSF网元
鉴权网元
终端设备根据所述终端设备的用户身份标识、生成参数以及预设参数，获得身份认证码
601
所述终端设备向AUSF网元发送所述身份认证码，所述用户身份标识的密文，以及所述预设参数的明文或密文
602
身份认证码
AUSF网元从安全功能网元接收身份认证码、所述终端设备的用户身份标识以及预设参数，并向鉴权网元发送身份认证码、所述终端设备的用户身份标识以及预设参数
603
身份认证码
鉴权网元从AUSF网元接收身份认证码、终端设备的用户身份标识以及预设参数
604
所述鉴权网元根据所述用户身份标识以及所述预设参数，校验所述身份认证码；当所述身份认证码校验成功时，所述鉴权网元向所述AUSF网元发送认证向量
605
认证向量
认证向量
安全功能网元接收AUSF网元发送的认证向量，根据所述认证向量确定认证请求，并向所述终端设备发送所述认证请求
606
认证请求
所述终端设备接收来自所述安全功能网元的认证请求
607

图6

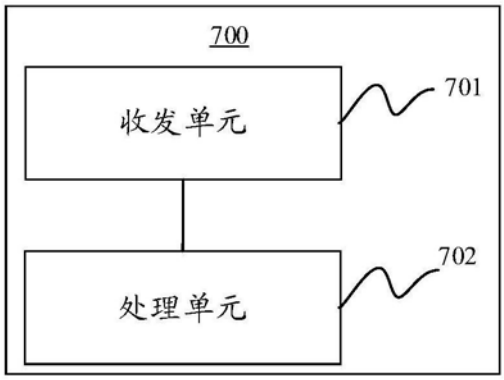

700
收发单元
701
处理单元
702

图7

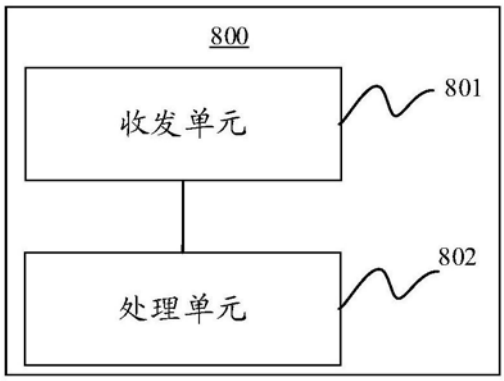

800
收发单元
801
处理单元
802

图8

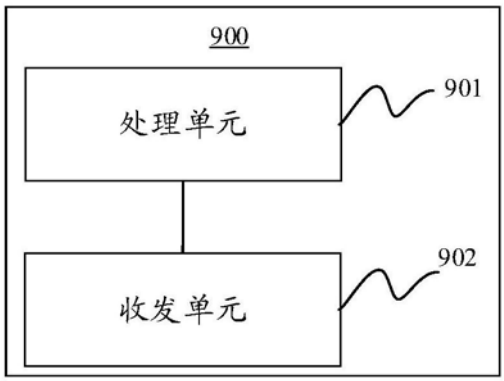

900
处理单元
901
收发单元
902

图9

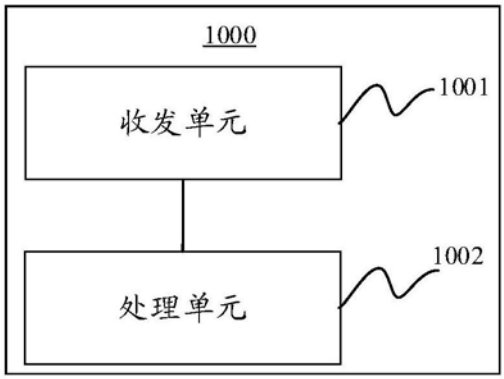


图10

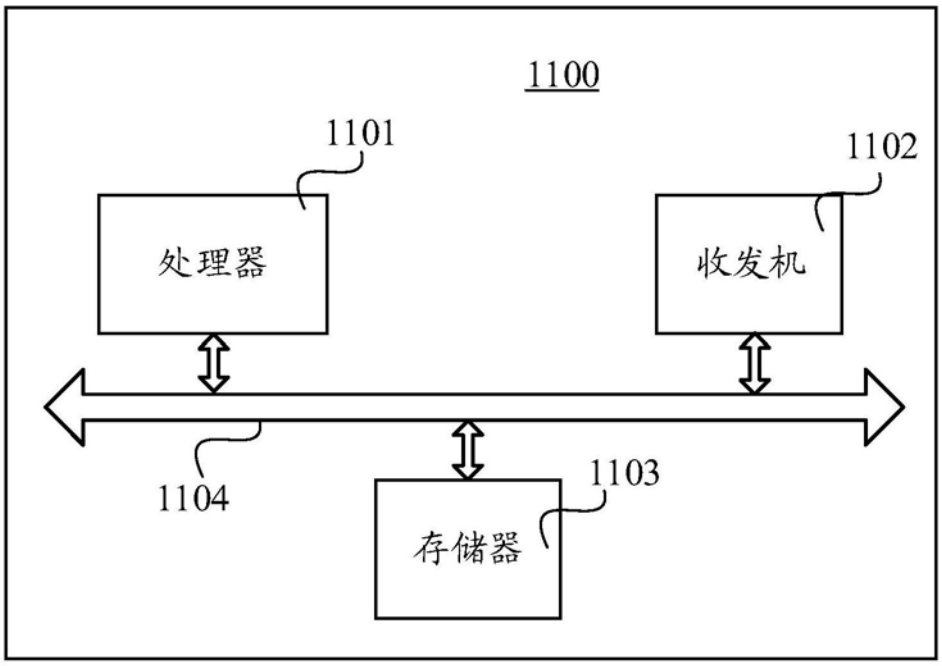


图11

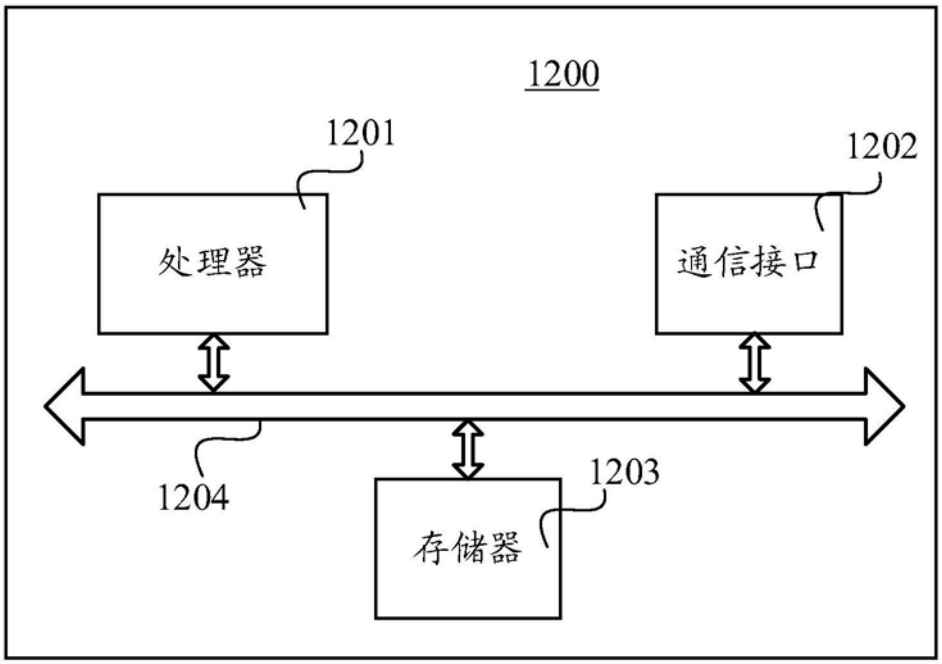

1200
1201
处理器
1202
通信接口
1204
1203
存储器

图12

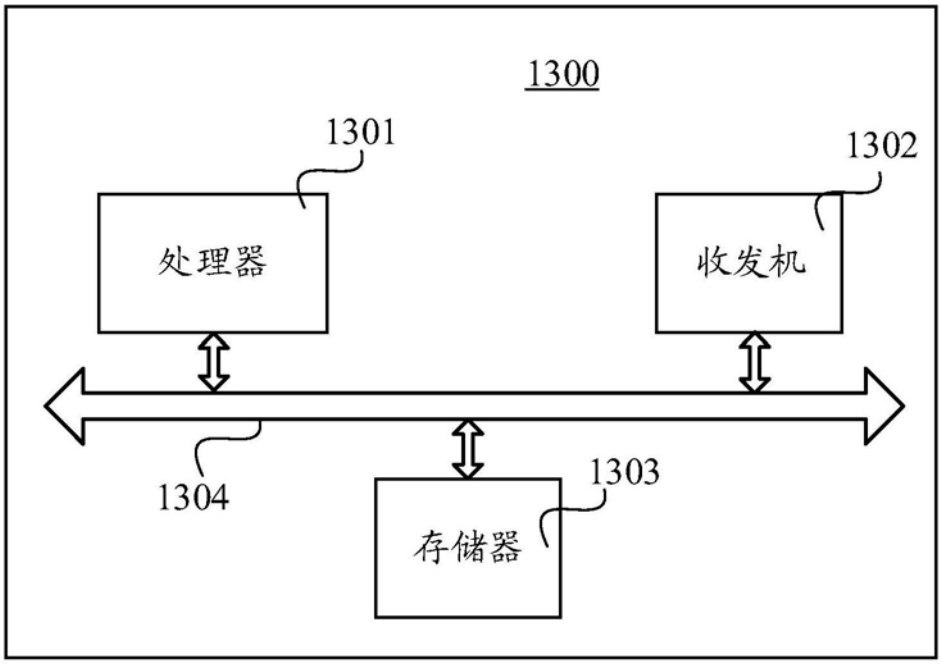

1300
1301
处理器
1302
收发机
1304
1303
存储器

图13

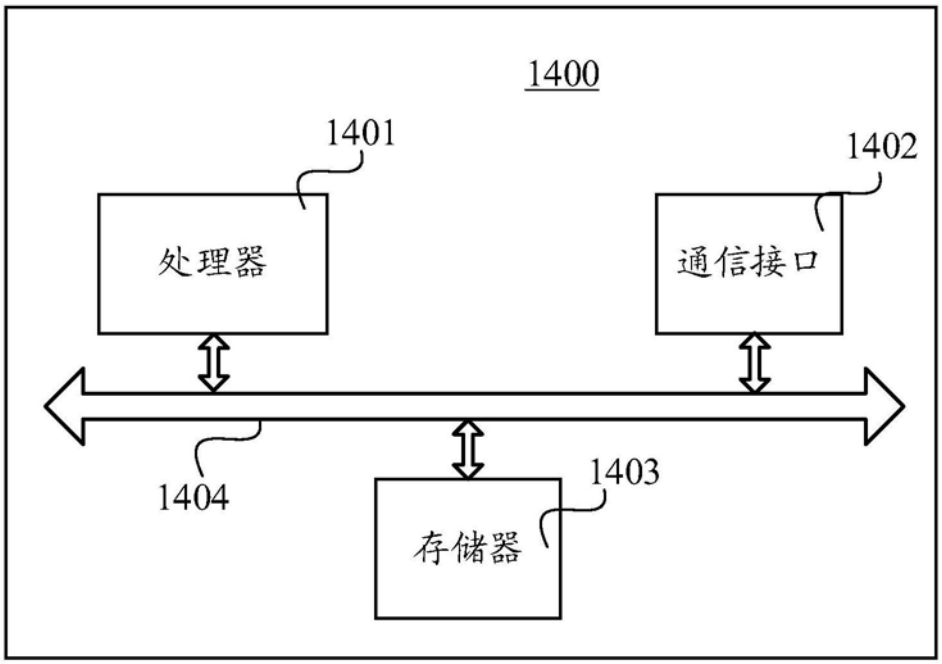


图14