

一种安全验证方法及装置

本申请要求于 2022 年 4 月 26 日提交中国专利局、申请号为 202210446683.8、申请名称为“一种安全验证方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种安全验证方法及装置。

背景技术

传统的无源射频识别（radio frequency identification, RFID）标签（也称电子标签）和读写器收发一体，具有部署成本高，盘点效率低等缺点。在第五代移动通信技术（5th generation, 5G）场景中，将读写器集成在基站中，企业通过 5G 核心网（5G core, 5GC）完成标签连接管理、读写器连接管理、标签定位功能和网络能力开放等能力。但是，由于读写器集成在基站中，标签与读写器的通信距离变远，可能导致通信安全问题。例如：标签被非法灭活、标签被非法写入信息、上报数据被窃听、上报数据被篡改、仿冒标签上报数据等。

发明内容

本申请实施例提供了一种安全验证方法及装置。可以保障终端设备与网络设备之间的通信安全。

第一方面，本申请实施例提供了一种安全验证方法，包括：

接收网络设备发送的第一命令，所述第一命令包括第一数值，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；根据所述第一数值和安全密钥，确定第一响应值；发送第一请求，所述第一请求包括所述第一响应值，所述第一响应值用于验证功能对所述终端设备进行验证。

终端设备根据接收到的网络设备的第一命令（例如选择命令、查询命令、查询重复命令、查询调整命令或确认命令）中包括的第一数值确定第一响应值，并将第一响应值发送给验证功能，使得验证功能对终端设备进行验证，避免非法的终端设备接入网络，避免终端设备上上报数据被窃听、上报数据被篡改、或仿冒终端设备上上报数据，从而保障终端设备与网络设备之间的通信安全。例如，恶意第三方通过窃听读写器与标签之间的通信，仿冒标签向读写器上报数据。通过对终端设备进行验证，可以避免标签上报的数据被篡改，避免仿冒标签上报数据，保障读写器与标签之间的通信安全。由于网络设备生成的第一数值是通过第一命令发送给终端设备的，因此可以减少终端设备与网络设备之间的交互次数，节省信令开销。

在一种可能的设计中，所述第一请求还包括第二数值，所述第二数值用于所述验证功能确定第二响应值：接收第一响应消息，所述第一响应消息包括所述第二响应值；根据所述第二响应值，对所述网络设备进行验证。终端设备通过接收验证功能确定的第二响应值，对网络设备进行验证。避免恶意的网络设备发送盘点指令，通过随机接入命令获得终端设备的 EPC 信息，导致贵重物品标签信息泄露。例如，避免标签被非法灭活或被非法写入信息。从而保障终端设备与网络设备之间的通信安全。

在另一种可能的设计中，根据所述第二数值和所述安全密钥，确定第三响应值；确定所

述第二响应值与所述第三响应值是否相同；当所述第二响应值与所述第三响应值相同时，确定所述网络设备通过验证。通过判断验证功能计算的第二响应值与终端设备计算的第三响应值是否相同，对网络设备进行验证，保障验证的准确性。

在另一种可能的设计中，所述第一响应消息还包括产品电子代码 EPC，所述 EPC 用于标识所述终端设备。通过对第一响应消息中第一响应值对网络设备进行验证，保障网络设备发送的 EPC 的真实性。

在另一种可能的设计中，通过接入和移动性管理功能 AMF 或标签管理功能 TMF 向所述验证功能发送第一验证结果，所述第一验证结果为所述网络设备的验证结果。

在另一种可能的设计中，所述第一请求中还包括产品电子代码 EPC，所述 EPC 用于标识所述终端设备；和/或，所述验证功能包括应用功能或认证、授权和计费功能。通过对第一请求中第一响应值，对终端设备进行验证，保障终端设备发送的 EPC 的真实性。

在另一种可能的设计中，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个。

其中，选择 (Select) 命令包括以下参数：

Target，指示是改变标签的 SL (选中标志) 还是盘存 (inventoried) 标志，在改变盘存标志情况下，指明是哪一个节 (session)。

Action，指示符合条件的标签是申明 SL 还是未申明 SL，或者置它们的盘存标志到 A 或 B。

MemBank，指示 Mask 是应用到 EPC、TID 还是用户区。

Pointer 和 Length，指示存贮范围。

Truncate，指示标签的回复是否截短。

其中，查询 (Query) 命令包括以下参数：

DR，设置 $T \Rightarrow R$ (标签到读写器) 链路频率。

M，设置 $T \Rightarrow R$ 数据速率以及调制格式。

TRext，选择 $T \Rightarrow R$ 帧头是否加入引导信号。

Sel，选择哪些标签对 Query 响应。

Session，为某个盘存周期选择一个节 (Session)。

Target，选择参与盘存周期标签的 inventoried 标志是 A 还是 B。

Q，设置盘存周期的时隙数目。

其中，查询重复 (QueryRep) 命令包括以下参数：

Session，确认本盘存周期的节 (Session) 值。

其中，查询调整 (QueryAdjust) 命令包括以下参数：

Session，确认本盘存周期的节 (Session) 值。

UpDn，决定标签是否调节 Q 值 (如盘存周期中的时隙数目) 和如何调节 Q 值。

其中，确认 (ACK) 命令包括以下参数：

RN16，16 位随机数或伪随机数。

第二方面，本申请实施例提供了一种安全验证方法，包括：

验证功能接收第一请求，所述第一请求包括第一响应值，所述第一响应值为根据安全密钥和网络设备的第一命令中包括的第一数值确定，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；所述验证功能根据所述第一响应值，对终端设备进行验证。

终端设备根据接收的网络设备的第一命令（例如选择命令、查询命令、查询重复命令、查询调整命令或确认命令）中包括的第一数值确定第一响应值，并将第一响应值发送给验证功能，使得验证功能对终端设备进行验证。避免非法的终端设备接入网络，以及避免终端设备上报数据被窃听、上报数据被篡改、或仿冒终端设备上报数据，从而保障终端设备与网络设备之间的通信安全。例如，恶意第三方通过窃听读写器与标签之间的通信，仿冒标签向读写器上报数据。通过对终端设备进行验证，可以避免标签上报的数据被篡改，避免仿冒标签上报数据，保障读写器与标签之间的通信安全。由于网络设备生成的第一数值是通过第一命令发送给终端设备的，因此可以减少终端设备与网络设备之间的交互次数，节省信令开销。

在一种可能的设计中，验证功能确定第三数值，根据所述第三数值和所述安全密钥，确定第四响应值；所述验证功能确定所述第一响应值与所述第四响应值是否相同；当所述第一响应值与所述第四响应值相同时，所述验证功能确定所述终端设备通过验证。

通过判断验证功能计算的第四响应值与终端设备计算的第一响应值是否相同，对终端设备进行验证，保障验证的准确性。

在另一种可能的设计中，所述第一请求还包括第二数值；验证功能根据所述第二数值和所述安全密钥，确定第二响应值；验证功能发送第一响应消息，所述第一响应消息包括所述第二响应值，所述第二响应值用于所述终端设备对所述网络设备进行验证。验证功能通过将第二响应值发送给终端设备，使得终端设备根据第二响应值对网络设备进行验证，避免恶意的网络设备发送盘点指令，通过随机接入命令获得终端设备的 EPC 信息，导致贵重物品标签信息泄露。例如，避免标签被非法灭活或被非法写入信息。实现终端设备与网络设备之间的双向验证，从而保障终端设备与网络设备之间的通信安全。

在另一种可能的设计中，所述验证功能接收所述终端设备通过接入和移动性管理功能 AMF 或标签管理功能 TMF 发送的第一验证结果，所述第一验证结果为所述网络设备的验证结果。

在另一种可能的设计中，所述验证功能向接入和移动性管理功能 AMF 或标签管理功能 TMF 发送第二响应消息，所述第二响应消息包括衍生密钥，所述衍生密钥为根据所述第一数值和所述第二数值中的至少一项，以及所述安全密钥和产品电子代码 EPC 生成，所述 EPC 用于标识所述终端设备。AMF 或 TMF 通过使用衍生密钥对信令进行加密或完整性保护，保障通信的安全。

在另一种可能的设计中，所述第二响应消息还包括第二验证结果，所述第二验证结果为所述终端设备的验证结果。

第三方面，本申请实施例提供了一种安全验证方法，包括：

接入和移动性管理功能 AMF 或标签管理功能 TMF 确定第一数值；向网络设备发送第二命令，所述第二命令包括所述第一数值，所述第二命令为盘点命令。

通过盘点命令向网络设备发送第一数值，使得网络设备向终端设备下发第一命令，这样终端设备根据第一命令中的第一数值确定第一响应值，从而减少了终端设备与网络设备的交互流程，减少了信令开销。

在另一种可能的设计中，接入和移动性管理功能 AMF 或标签管理功能 TMF 接收验证功能发送的第二请求，所述第二请求包括第一数值；或

所述第一数值是由所述 AMF 或所述 TMF 生成。

在另一种可能的设计中，所述 AMF 或所述 TMF 接收验证功能发送的第二响应消息，所述第二响应消息包括衍生密钥，所述衍生密钥为根据所述第一数值和所述第二数值中的至少

一项, 以及所述安全密钥和产品电子代码 EPC 生成, 所述 EPC 用于标识所述终端设备。通过衍生密钥对信令进行加密或完整性保护, 提高通信的安全性。

在另一种可能的设计中, 所述第二响应消息还包括第二验证结果, 所述第二验证结果为所述终端设备的验证结果。

第四方面, 本申请实施例提供了一种安全验证系统, 包括:

接入和移动性管理功能 AMF 或标签管理功能 TMF 确定第一数值; 向网络设备发送第二命令, 所述第二命令包括所述第一数值, 所述第二命令为盘点命令;

验证功能接收第一请求, 所述第一请求包括第一响应值, 所述第一响应值为根据安全密钥和网络设备的第一命令中包括的第一数值确定, 所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个; 根据所述第一响应值, 对终端设备进行验证。

验证功能通过接收终端设备确定的第一响应值对终端设备进行验证, 从而保障终端设备与网络设备之间的通信安全。由于网络设备生成的第一数值是通过第一命令发送给终端设备的, 因此可以减少终端设备与网络设备之间的交互次数, 节省信令开销。

在一种可能的设计中, 网络设备向终端设备发送第一命令, 所述第一命令包括所述第一数值。

第五方面, 本申请实施例提供了一种安全验证方法, 包括:

终端设备在接收到网络设备的接入命令后, 生成第一数值, 所述接入命令为 Write, Kill, Lock 中的一个; 所述终端设备发送所述第一数值; 所述终端设备从验证功能接收第一响应值, 所述第一响应值根据所述第一数值计算得到; 所述终端设备根据所述第一响应值对所述网络设备进行验证。

终端设备接收到接入命令后对网络设备发起验证, 验证通过后执行接入命令, 从而防止恶意基站发起对终端设备的读、写、灭活等命令, 从而保障终端设备与网络设备之间的通信安全。

在另一种可能的设计中, 所述终端设备从所述验证功能接收第二数值; 所述终端设备根据所述第二数值和安全密钥计算第二响应值; 所述终端设备发送所述第二响应值, 所述第二响应值用于所述验证功能对所述终端设备进行验证。终端设备通过计算第二响应值, 并将第二响应值发送给验证功能, 使得验证功能对终端设备进行验证, 从而保障终端设备与网络设备之间的通信安全。

在另一种可能的设计中, 所述终端设备根据所述第一数值和安全密钥, 确定第三响应值; 所述终端设备确定所述第一响应值与所述第三响应值是否相同; 当所述第一响应值与所述第三响应值相同时, 所述终端设备确定所述网络设备通过验证。

通过判断验证功能计算的第一响应值与终端设备计算的第三响应值是否相同, 对网络设备进行验证, 保障验证的准确性。

在另一种可能的设计中, 所述第一数值包括在第一请求中, 所述第一响应值包括在第一响应消息中, 所述第一响应消息和/或所述第一请求还包括产品电子代码 EPC, 所述 EPC 用于标识所述终端设备。

在另一种可能的设计中, 所述验证功能包括应用功能或认证、授权和计费功能。

第六方面, 本申请实施例提供了一种安全验证装置, 所述装置包括:

接收模块, 用于接收网络设备发送的第一命令, 所述第一命令包括第一数值, 所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个;

处理模块，用于根据所述第一数值和安全密钥，确定第一响应值；

发送模块，用于发送第一请求，所述第一请求包括所述第一响应值，所述第一响应值用于验证功能对所述终端设备进行验证。

各个模块的实现可以对应参照第一方面所述的方法实施例的相应描述，执行上述终端设备所执行的方法和功能。

该安全验证装置执行的操作及有益效果可以参见上述第一方面所述的方法以及有益效果，重复之处不再赘述。

第七方面，本申请实施例提供了一种安全验证装置，所述装置包括：

接收模块，用于接收第一请求，所述第一请求包括第一响应值，所述第一响应值为根据安全密钥和网络设备的第一命令中包括的第一数值确定，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；

处理模块，用于根据所述第一响应值，对所述终端设备进行验证。

各个模块的实现可以对应参照第二方面所述的方法实施例的相应描述，执行上述验证功能所执行的方法和功能。

该安全验证装置执行的操作及有益效果可以参见上述第二方面所述的方法以及有益效果，重复之处不再赘述。

第八方面，本申请实施例提供了一种安全验证装置，包括：

处理模块，用于确定第一数值；

发送模块，用于向网络设备发送第二命令，所述第二命令包括所述第一数值，所述第二命令为盘点命令。

各个模块的实现可以对应参照第三方面所述的方法实施例的相应描述，执行上述 AMF 或 TMF 所执行的方法和功能。

该安全验证装置执行的操作及有益效果可以参见上述第三方面所述的方法以及有益效果，重复之处不再赘述。

第九方面，本申请实施例提供了一种安全验证装置，包括：

处理模块，用于在收到网络设备的接入命令后，生成第一数值，所述接入命令为 Write, Kill, Lock 中的一个；

发送模块，用于发送所述第一数值；

接收模块，用于从验证功能接收第一响应值，所述第一响应值根据所述第一数值计算得到；所述终端设备根据所述第一响应值对所述网络设备进行验证。

各个模块的实现可以对应参照第五方面所述的方法实施例的相应描述，执行上述终端设备所执行的方法和功能。

该安全验证装置执行的操作及有益效果可以参见上述第五方面所述的方法以及有益效果，重复之处不再赘述。

第十方面，本申请提供了一种安全验证装置，该装置可以是终端设备，也可以是终端设备中的装置，或者是能够和终端设备匹配使用的装置。该装置也可以是验证功能，也可以是验证功能中的装置，或者是能够和验证功能匹配使用的装置。该装置也可以是 AMF 或 TMF，也可以是 AMF 或 TMF 中的装置，或者是能够和 AMF 或 TMF 匹配使用的装置。其中，该安全验证装置还可以为芯片系统。该安全验证装置可执行上述的方法。该安全验证装置的功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。该模块可以是软件和/或硬件。该安全验证装置执行的操作及有益效果

果可以参见上述第一方面和第五方面所述的方法以及有益效果，重复之处不再赘述。

第十一方面，本申请提供了一种安全验证装置，所述安全验证装置包括处理器和存储器，当所述处理器调用存储器中的计算机程序时，如第一方面、第二方面、第三方面和第五方面中任意一项所述的方法被执行。

第十二方面，本申请提供了一种计算机可读存储介质，所述计算机可读存储介质用于存储计算机程序，当所述计算机程序被执行时，使得如第一方面至第五方面中任意一项所述的方法或系统被实现。

第十三方面，本申请提供一种包括计算机程序的计算机程序产品，当所述计算机程序被执行时，使得如第一方面至第五方面中任意一项所述的方法或系统被实现。

第十四方面，本申请实施例提供了一种通信系统，该通信系统包括至少一个终端设备和至少一个验证功能，该终端设备用于执行上述第一方面和第五方面中的步骤，该验证功能用于执行上述第二方面中的步骤。

第十五方面，本申请实施例提供了一种通信系统，该通信系统包括至少一个验证功能、和至少一个 AMF 或 TMF，该验证功能用于执行上述第二方面中的步骤，该 AMF 或 TMF 用于执行上述第三方面中的步骤。

第十六方面，本申请实施例提供了一种通信系统，该通信系统包括至少一个终端设备、至少一个验证功能、和至少一个 AMF 或 TMF，该终端设备用于执行上述第一方面和第五方面中的步骤，该验证功能用于执行上述第二方面中的步骤，所述 AMF 或 TMF 用于执行上述第三方面中的步骤。

附图说明

为了更清楚地说明本申请实施例或背景技术中的技术方案，下面将对本申请实施例或背景技术中所需要使用的附图进行说明。

图 1 是一种 5G 系统的架构示意图；

图 2 是一种 RFID 业务流程的示意图；

图 3 是一种读写器集成在基站后标签的业务流程的示意图；

图 4a 是本申请实施例提供的一种安全验证方法的流程示意图；

图 4b 是本申请实施例提供的另一种安全验证方法的流程示意图；

图 5 是本申请实施例提供的另一种安全验证方法的流程示意图；

图 6 是本申请实施例提供的另一种安全验证方法的流程示意图；

图 7 是本申请实施例提供的另一种安全验证方法的流程示意图；

图 8 是本申请实施例提供的一种安全验证装置的结构示意图；

图 9 是本申请实施例提供的另一种安全验证装置的结构示意图；

图 10 是本申请实施例提供的一种终端设备的结构示意图；

图 11 是本申请实施例提供的一种验证功能的结构示意图。

具体实施方式

图 1 是一种 5G 系统的架构示意图。该 5G 系统包括接入网和核心网两部分。接入网用于实现无线接入有关的功能。核心网主要包括以下几个关键逻辑网元：接入和移动性管理功能（access and mobility management function, AMF）实体、会话管理功能（session management function, SMF）实体、用户面功能（user plane function, UPF）实体、策略控制功能（policy

control function, PCF) 实体、统一数据管理 (unified data management, UDM) 实体和应用功能实体 (Application Function, AF)。

可选的, 核心网还可以包括标签管理功能 (tag management function, TMF), 认证、授权和计费 (Authentication Authorization and Accounting, AAA) 实体, 网络能力开放功能 (network exposure function, NEF) 实体。

下面对图 1 中所涉及各个网元进行介绍:

UE 可以是电子设备, 如手机、物联网终端设备等。

无线接入网络 (radio access network, (R) AN) 设备为 UE 提供无线接入的设备, 包括但不限于 5G 基站 (next generation node B, gNB)、无线保真 (wireless-fidelity, WiFi) 接入点 (access point, AP)、全球微波互联接入 (worldwide interoperability for microwave access, WiMAX) 基站 (base station, BS) 等。

AMF 实体主要负责移动网络中的移动性管理, 如用户位置更新、用户注册网络、用户切换等。

SMF 实体主要负责移动网络中的会话管理, 如会话建立、修改、释放。具体功能如为用户分配 IP 地址、选择提供报文转发功能的 UPF 等。

PCF 实体主要负责向 AMF、SMF 提供策略, 如服务质量 (quality of service, QoS) 策略、切片选择策略等。

UDM 实体用于存储用户数据, 如签约信息、鉴权/授权信息。

AF 实体主要负责向第三代合作伙伴计划 (3rd generation partnership project, 3GPP) 网络提供业务, 如影响业务路由、与 PCF 之间交互以进行策略控制等。

UPF 实体主要负责对用户报文进行处理, 如转发、计费等。

NEF 实体主要用于将 3GPP 的各个网元的能力暴露给其它网元, 提供相应的安全保障来保证外部应用到 3GPP 网络的安全。

数据网络 (data network, DN) 主要负责为用户提供数据传输服务, 如 IP 多媒体业务 (IP multi-media service, IMS)、因特网 (internet) 等。UE 通过建立 UE-RAN-UPF-DN 之间的会话 (session), 来访问 DN。

需要说明的是, 图 1 中各个网络功能和实体之间可以通过不同接口来交互消息。例如, UE 和 AMF 实体之间可以通过 N1 接口进行交互, 交互消息称为 N1 Message。部分接口采用服务化接口的方式实现。图 1 中的 UE、RAN 设备、UPF 实体和 DN 可以称为数据面的网络功能和实体, 用于承载业务数据, 用户层数据流量可以通过 UE 和 DN 之间建立的 PDU Session 进行传输, 并经过 RAN 设备和 UPF 实体两个网络功能实体。其他的网络功能和实体可以统称为控制面的网络功能和实体, 用于承载信令消息, 主要负责认证和鉴权、注册管理、会话管理、移动性管理以及策略控制等功能等等, 从而实现用户层数据流量传输的可靠性和稳定性。

射频识别 (radio frequency identification, RFID) 是一种非接触式的自动识别技术, 通过无线射频方式进行非接触双向数据通信, 对标签进行读写, 从而完成读写器 (Reader) 与标签 (Tag) 之间的数据通信, 实现识别目标和数据交换的目的。在通常情况下, 标签进入读写器发射的电磁场后, 从天线获得的感应电流, 经升压电路后转化为芯片的电源, 同时将感应电流所获得的能量通过射频前端电路变为数据信号送入逻辑控制电路进行处理。在回复的信息时, 从标签的存储器中发出, 经逻辑控制电路送回射频前端电路, 最后通过天线发送回读写器。

如图 2 所示，图 2 是一种 RFID 业务流程的示意图。具体过程包括：

S201，企业打印标签，写入产品电子代码（Electronic product code, EPC），EPC 用于标识所附着的物品。

S202，读写器发送选择 Select 命令，选择一个标签群进行盘存和访问。在盘存之前，读写器使用一个或多个 Select 命令选择一个特定的标签群。

S203，读写器通过发送查询（Query）命令开始一个盘存周期。或者，通过查询重复（QueryRep）命令和查询调整（QueryAdjust）命令开始下一个标签的盘存周期。

S204，被选定的标签向读写器返回一个 RN16。

其中，RN16 可以表示 16 比特的随机数。

S205，读写器向标签发送 ACK 命令，ACK 命令携带 RN16。ACK 命令用于确认标签回复的 RN16。

S206，标签在接收到 ACK 命令之后，响应产品电子代码 EPC，将 EPC 发送给读写器。

S207，读写器向标签发送接入命令，以便执行读写等操作。

S208，标签向读写器发送接入命令响应。

其中，接入命令可以包括：Req_RN：请求新的 RN16；Read：读取数据；Write：写入数据；Kill：灭活标签（需要 kill password）；Lock：锁定操作（锁定区域不能读/写）；Access：使标签转入安全（Secured）状态，即可以执行 Lock 操作（需要 access password）；BlockWrite：多字的写入操作；BlockErase：多字的擦除操作。

在 5G 场景下，将读写器集成在基站中，企业通过 5GC 完成标签连接管理、读写器连接管理、标签定位功能和网络能力开放等能力。如图 3 所示，图 3 是一种读写器集成在基站后标签的业务流程的示意图。主要包括如下步骤：

S301，企业打印标签，在标签（tag）中写入 EPC，在验证功能中存储 EPC。其中，EPC 用于标识所附着的物品。

S302，验证功能通过 NEF 或 proxy 向 AMF/TMF 发送盘点请求，所述盘点请求包含指令类型、标签标识、标签类型等参数。其中，验证功能可以为 AF 或 AAA。

S303，AMF/TMF 根据盘点请求中的参数，确定多个基站中的盘点基站。

S304，AMF/TMF 向基站发送盘点命令。该基站为 S303 确定的盘点基站。

S305，基站发送 Select 命令，选择一个标签群进行盘存和访问。

S306-S308，基站和标签执行随机接入过程，随机接入过程与图 2 中 RFID 业务流程中的 S203-S205 相同，具体可以参考 S203-S205，此处不再赘述。

其中，当标签接收到基站发送的 ACK 命令时，表示随机接入成功。

S309，接入成功的标签向基站发送注册请求。

其中，所述注册请求包含参数 EPC。

S310，基站将向 AMF/TMF 发送注册请求。

其中，所述注册请求包含参数 EPC。

S311，标签和企业通过 5GC 进行认证流程。

S312，AMF/TMF 通过基站向标签发送注册响应。

S313，AMF/TMF 通过基站向标签发送接入命令。

S314，标签向 AMF/TMF 发送接入命令响应。

S315，AMF/TMF 通过 NEF 或 proxy 向验证功能发送标签的盘点结果。

S316, AMF/TMF 发送指示信息, 所述指示信息用于指示基站盘点下一个标签。

S317, 重复执行 S305-S316, 执行下一个标签的盘点流程。

S318, 基站向 AMF/TMF 发送盘点结束命令。

S319, AMF/TMF 通过 NEF 或 proxy 向验证功能发送所有标签的盘点结果。

其中, 上述各个网元可以执行上述部分或全部步骤, 例如 S312-S317 是可选的。

由于读写器集成在基站中, 标签与读写器的通信距离变远, 可能导致通信安全问题。例如: 标签被非法灭活、标签被非法写入信息、上报数据被窃听、上报数据被篡改、仿冒标签上报数据等。

现有 RFID 的认证方式主要通过口令 (password) 的形式。例如: 灭活操作前, 标签验证读写器发出的 kill password, 验证通过后标签执行灭活操作。同样地, 在标签安全 (Secured) 状态转换前, 标签验证读写器发出的接入口令 (access password), 验证通过后标签将转换到 Secured 状态。

由于原来的读写器与标签之间的通信距离很近, 不需要额外的认证过程。因此 RFID 在随机接入过程中, 没有相应的认证流程。但是, 将读写器集成在基站之后, 基站与标签之间无法相互认证。如果恶意的基站发送盘点命令, 通过随机接入命令获取标签的 EPC 信息, 可能造成贵重物品标签信息泄露。或者, 如果恶意的标签响应基站的随机接入命令, 上传虚假数据, 则可能影响盘点结果和数据真实性。

现有 RFID 在接入命令的执行过程中, 认证方式只支持在 Kill 和 Access 操作前对读写器进行认证。将读写器集成在基站之后, 对于 Read、Write 等命令也需要有效的认证过程。此外, 将读写器集成在基站之后, 原有的认证方式也会受到攻击。例如: 如果恶意第三方窃听基站与标签之间的通信, 可能获取 RN16 以及与随机数异或操作后的 kill password 或 access password。因此, 恶意第三方即可获得相应的 password 并对标签发起 Kill 或 Access 命令, 从而对标签进行恶意的读取或修改。

为了解决上述技术问题, 本申请实施例提供了如下解决方案。

如图 4a 所示, 图 4a 是本申请实施例提供的一种安全验证方法的流程示意图。本申请实施例中的步骤主要包括:

S401a, 终端设备接收网络设备发送的第一命令, 所述第一命令包括第一数值, 所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个。

其中, 第一数值是由网络设备生成的。网络设备可以为基站、TMF/AMF 或验证功能。验证功能可以为 AF 或 AAA。

其中, 所述第一数值可以为随机数 RAND1 或计数器 Count1。

其中, 终端设备可以为标签、UE 或者 UE 中的芯片。

S402a, 终端设备根据所述第一数值和安全密钥, 确定第一响应值。

其中, 第一响应值 $RES1 = MAC(K, RAND1)$ 。或者, 第一响应值 $RES1 = MAC(K, Count1)$ 。K 为安全密钥, 可以预先将安全密钥写入终端设备和验证功能中。MAC 是任意一个消息认证码算法。

需要说明的是, 可以通过其他方式, 根据第一数值和安全密钥计算第一响应值。通过其他方式计算的第一响应值或其他响应值都在本申请保护的范围内。

S403a, 终端设备发送第一请求, 所述第一请求包括所述第一响应值, 所述第一响应值用于验证功能对所述终端设备进行验证。

可选的, 终端设备通过基站、或 TMF/AMF 向验证功能发送第一请求。

验证功能接收到第一请求之后，确定第三数值，根据第三数值和安全密钥，确定第四响应值。其中，第三数值和第一数值都是由网络设备生成的，最初是同一个随机数或计数器。但是经过传输后，可能被篡改，因此第三数值可能与终端设备接收到第一命令中的第一数值相同，也可能与终端设备接收到第一命令中的第一数值不相同。第四响应值 $RES4 = MAC(K, RAND1)$ ，或者，第四响应值 $RES4 = MAC(K, Count1)$ 。K 为安全密钥，RAND1 和 Count1 为第三数值，MAC 是任意一个消息认证码算法。然后，验证功能确定所述第一响应值与所述第四响应值是否相同；当所述第一响应值与所述第四响应值相同时，确定所述终端设备通过验证，说明终端设备是安全的，当所述第一响应值与所述第四响应值不相同时，确定所述终端设备未通过验证，说明终端设备存在安全问题。

其中，所述第一请求可以为企业认证请求。

本实施例的具体实施方式可以参考下面如图 4b 所示的实施例。此处不再赘述。

如图 4b 所示，图 4b 是本申请实施例提供的一种安全验证方法的流程示意图。本申请实施例中的步骤主要包括：

S401，企业打印标签，在终端设备中写入 EPC 以及安全密钥 K，在验证功能中存储 EPC 以及安全密钥 K。

其中，终端设备可以为标签、UE 或者 UE 中的芯片。验证功能可以为 AF 或 AAA。终端设备和验证功能中的安全密钥 K 相同。

其中，EPC 用于标识终端设备。

S402，验证功能通过 NEF 或 proxy 向 TMF/AMF 发送盘点请求。

可选的，盘点请求可以包括第一数值。第一数值可以由验证功能生成。第一数值可以为随机数 RAND1 或计数器 Count1。其中，计数器 Count1 由验证功能存储，且每次发出 Count1 后计数器加 1。

S403，TMF/AMF 根据盘点请求确定盘点基站。

S404，TMF/AMF 向基站发送盘点命令。其中，该基站为 S403 确定的盘点基站。

可选的，盘点命令中包含第一数值，所述第一数值可以为随机数 RAND1 或计数器 Count1。

其中，第一数值可以是 TMF/AMF 从验证功能发送的盘点请求中获取，也可以是由 TMF/AMF 本地生成。

S405，基站向终端设备发送选择 (Select) 命令，选择一个或多个终端设备进行盘存和访问。

可选的，Select 命令中包含第一数值，所述第一数值可以为随机数 RAND1 或计数器 Count1。

其中，第一数值可以是基站从 TMF/AMF 发送的盘点命令中获取，也可以是由基站本地生成。

其中，选择 (Select) 命令可以包括以下参数：

Target，指示是改变标签的 SL (选中标志) 还是盘存 (inventoried) 标志，在改变盘存标志情况下，指明是哪一个节 (session)。

Action，指示符合条件的标签是申明 SL 还是未申明 SL，或者置它们的盘存标志到 A 或 B。

MemBank，指示 Mask (掩码) 是应用到 EPC、TID (标签标识符) 还是用户区。

Pointer 和 Length，指示存贮范围。

Truncate, 指示标签的回复是否截短。

S406-S408, 基站与终端设备之间执行随机接入过程, 随机接入过程与图 2 中 RFID 业务流程中的 S203-S205 相同, 可以参考 S203-S205。此处不再赘述。

其中, 当终端设备接收到基站发送的 ACK 命令时, 表示终端设备随机接入成功。

需要说明的是, 若 S405 中基站发送的选择命令中不包括第一数值, 则第一数值可以包含于随机接入过程中的查询(Query)命令、查询重复(QueryRep)命令、查询调整(QueryAdjust)命令或确认(ACK)命令中的一个。

其中, 所述第一数值可以为随机数 RAND1 或计数器 Count1。

其中, 查询(Query)命令包括以下参数: DR, 设置 $T \Rightarrow R$ (标签到读写器) 链路频率。M, 设置 $T \Rightarrow R$ 数据速率以及调制格式。TRext, 选择 $T \Rightarrow R$ 帧头是否加入引导信号。Sel, 选择哪些标签对 Query 响应。Session, 为某个盘存周期选择一个节(Session)。Target, 选择参与盘存周期标签的 inventoried 标志是 A 还是 B。Q, 设置盘存周期的时隙数目。

其中, 查询重复(QueryRep)命令包括以下参数: Session, 确认本盘存周期的节(Session)值。

其中, 查询调整(QueryAdjust)命令包括以下参数: Session, 确认本盘存周期的节(Session)值。UpDn, 决定标签是否调节 Q 值(如盘存周期中的时隙数目)和如何调节 Q 值。

其中, 确认(ACK)命令包括以下参数: RN16, 16 位随机或伪随机数。

S409, 终端设备根据第一数值和所述安全密钥, 确定第一响应值。

其中, 第一响应值 $RES1 = MAC(K, RAND1)$ 。或者, 第一响应值 $RES1 = MAC(K, Count1)$ 。K 为安全密钥, MAC 是任意一个消息认证码算法。

需要说明的是, 可以通过其他方式, 根据第一数值和安全密钥计算第一响应值。通过其他方式计算的第一响应值或其他响应值都在本申请保护的范围内。

S410, 终端设备向基站发送注册请求。

其中, 注册请求可以包括第一响应值 RES1。可选的, 注册请求可以包括 EPC。

可选的, 注册请求还可以包括第二数值, 第二数值为终端设备生成的随机数 RAND2 或计数器 Count2。终端设备可以选择以下两种方式中的一种方式生成计数器 Count2:

第一种方式, 终端设备在 Count1 的基础上加 1 生成 Count2。

第二种方式, 终端设备本地存储 Count2, 每次发出 Count2 后本地存储的 Count2 加 1。

S411, 基站向 AMF/TMF 发送注册请求。

其中, 所述注册请求包括第一响应值 RES1。

可选的, 所述注册请求还可以包括第二数值。可选的, 所述注册请求还可以包括 EPC。

S412, TMF/AMF 向验证功能发送第一请求。

可选的, 终端设备通过 TMF/AMF (或者 NEF/proxy) 向验证功能发送第一请求。

其中, 所述第一请求中包括第一响应值 RES1。可选的, 第一请求还可以包括第二数值。可选的, 所述注册请求还可以包括 EPC。

其中, 所述第一请求可以为企业认证请求。

可选的, TMF/AMF 可以向 UDM/AUSF 发送第一请求。其中, 所述第一请求中包含第一响应值 RES1。

可选的, 所述第一请求还可以包括第二数值。可选的, 所述第一请求还可以包括 EPC。

UDM/AUSF 接收到第一请求之后, 对终端设备进行验证。也即可以通过 UDM/AUSF 完成验证流程。在这种情况下, 图 4b 中 AF/AAA 与 TMF/AMF 的交互过程可以修改为

UDM/AUSF 与 TMF/AMF 的交互。UDM/AUSF 预先配置终端设备的 EPC、安全密钥 K 以及计数器 Count1 (计数器 Count1 的配置和维护是可选的)。

S413, 验证功能根据第一响应值, 对终端设备进行验证。

具体的, 验证功能接收到第一请求之后, 确定第三数值, 根据第三数值和安全密钥, 确定第四响应值。其中, 第三数值和第一数值都是由网络设备生成的, 最初是同一个随机数或计数器。但是经过传输后, 可能被篡改, 因此第三数值可能与终端设备接收到第一命令中的第一数值相同, 也可能与终端设备接收到第一命令中的第一数值不相同。第四响应值 $RES4 = MAC(K, RAND1)$, 或者, 第四响应值 $RES4 = MAC(K, Count1)$ 。K 为安全密钥, RAND1 和 Count1 为第三数值, MAC 是任意一个消息认证码算法。然后, 验证功能确定所述第一响应值与所述第四响应值是否相同; 当所述第一响应值与所述第四响应值相同时, 确定所述终端设备通过验证, 说明终端设备是安全的, 当所述第一响应值与所述第四响应值不相同, 确定所述终端设备未通过验证, 说明终端设备存在安全问题。

需要说明的是, 所述第三数值可以由验证功能生成, 如果第三数值不是由验证功能生成的 (例如 TMF/AMF 或基站生成), 第三数值可以由终端设备发送给验证功能。

可选的, 当验证功能确定终端设备通过验证时, 验证功能可以根据接收到的第一请求中的第二数值和所述安全密钥, 确定第二响应值。其中, 第二响应值 $RES2 = MAC(K, RAND2)$, 或者, 第二响应值 $RES2 = MAC(K, Count2)$ 。

需要说明的是, 由于终端设备与网络设备之间存在通信距离, 在传输过程中数据有可能被篡改。验证功能接收到的第一请求中第二数值与终端设备发送的注册请求中的第二数值可能相同, 也有可能不相同。

其中, 第二数值为终端设备生成的随机数 RAND2 或计数器 Count2。如果 S410 中的计数器 Count2 是在 Count1 的基础上加 1 生成, 则验证功能将本地维护的 Count1 加 1。

可选的, 验证功能可以根据所述第一数值和所述第二数值中的至少一项、以及所述安全密钥和产品电子代码 EPC 生成确定衍生密钥 Ktmf。其中, 所述衍生密钥 Ktmf 可以用于信令加密或完整性保护。

S414, 验证功能发送第一响应消息。

可选的, 验证功能可以通过 TMF/AMF 或基站向终端设备发送第一响应消息。

其中, 第一响应消息包括所述第二响应值。可选的, 第一响应消息还可以包括 EPC。

其中, 第一响应消息可以为标签认证响应。

S415, 终端设备根据第二响应值, 对网络设备进行验证。

具体的, 终端设备可以根据第二数值和所述安全密钥, 确定第三响应值。其中, 该第二数值为终端设备生成的随机数 RAND2 或计数器 Count2, 与 S410 中终端设备发送的注册请求中的第二数值相同。第三响应值 $RES3 = MAC(K, RAND2)$, 或者, 第三响应值 $RES3 = MAC(K, Count2)$ 。然后, 确定所述第二响应值与所述第三响应值是否相同; 当所述第二响应值与所述第三响应值相同时, 确定所述网络设备通过验证, 说明网络设备是安全的, 当所述第二响应值与所述第三响应值不相同, 确定所述网络设备未通过验证, 说明网络设备存在通信安全问题。

其中, 网络设备可以是基站、TMF/AMF 或验证功能等。

S416, 终端设备通过 AMF 实体或 TMF 实体向验证功能发送第一验证结果。

其中, 所述第一验证结果为所述网络设备的验证结果, 第一验证结果包括网络设备通过验证或网络设备未通过验证。

其中，第一验证结果为标签认证结果。

S417，验证功能向 AMF 实体或 TMF 实体发送第二响应消息。

其中，所述第二响应消息可以包括第二验证结果，所述第二验证结果为所述终端设备的验证结果。第二验证结果包括终端设备通过验证或终端设备未通过验证。

可选的，所述第二响应消息包括衍生密钥，所述衍生密钥为根据所述第一数值和所述第二数值中的至少一项，以及所述安全密钥和产品电子代码 EPC 生成，所述 EPC 用于标识所述终端设备。

如果 S413 中验证功能对终端设备进行验证后没有生成衍生密钥，则可以在此步骤生成衍生密钥。

可选的，如果确定终端设备通过验证、和/或确定网络设备通过验证时，验证功能可以向 AMF 实体或 TMF 实体发送第二响应消息。

其中，第二响应消息可以为企业认证响应。

S418，AMF/TMF 通过基站向终端设备发送注册响应。

S419，AMF/TMF 通过基站向终端设备发送接入命令。

其中，接入命令可以包括：Req_RN：请求新的 RN16；Read：读取数据；Write：写入数据；Kill：灭活标签（需要 kill password）；Lock：锁定操作（锁定区域不能读/写）；Access：使标签转入安全(Secured)状态，即可以执行 Lock 操作（需要 access password）；BlockWrite：多字的写入操作；BlockErase：多字的擦除操作。

S420，终端设备向 AMF/TMF 发送接入命令响应。

在本申请实施例中，终端设备根据接收到的网络设备的第一命令（例如选择命令、查询命令、查询重复命令、查询调整命令或确认命令）中包括的第一数值确定第一响应值，并将第一响应值发送给验证功能，使得验证功能对终端设备进行验证。并且，验证功能根据终端设备生成的第二数值确定第二响应值，并将第二响应值发送给终端设备，使得终端设备对网络设备进行验证。实现终端设备与网络设备之间的双向验证，从而保障终端设备与网络设备之间的通信安全。由于网络设备生成的第一数值是通过第一命令发送给终端设备计算第一响应值，因此可以减少终端设备与网络设备之间的交互次数，节省信令开销。

图 4b 所示的实施例中先对终端设备进行验证，然后对网络设备进行验证。下面图 5 所示的实施例中先对网络设备进行验证，然后对终端设备进行验证。并且，该实施例中的终端设备可以根据本地配置的安全策略发起验证流程。

如图 5 所示，图 5 是本申请实施例提供的一种安全验证方法的流程示意图。本申请实施例中的步骤主要包括：

S501，企业打印标签，在终端设备中写入 EPC、安全密钥 K 和安全策略，在验证功能中存储 EPC 以及安全密钥 K。

其中，终端设备可以为标签、UE 或者 UE 中的芯片。验证功能可以为 AF 或 AAA。终端设备和验证功能中的安全密钥 K 相同。

其中，EPC 用于标识终端设备。

其中，安全策略用于指示双向验证的执行条件。也即终端设备在确定满足执行条件时，发起验证流程。

S502，验证功能通过 NEF 或 proxy 向 AMF/TMF 发送盘点请求，所述盘点请求包含指令类型、标签标识、标签类型等参数。

S503, AMF/TMF 根据盘点请求中的参数, 确定多个基站中的盘点基站。

S504, AMF/TMF 向基站发送盘点命令。该基站为 S503 确定的盘点基站。

S505, 基站发送 Select 命令, 选择一个或多个终端设备进行盘存和访问。

S506-S508, 基站与终端设备之间执行随机接入过程, 随机接入过程与图 2 中 RFID 业务流程中的 S203-S205 相同, 可以参考 S203-S205。此处不再赘述。

其中, 当终端设备接收到基站发送的 ACK 命令时, 表示终端设备随机接入成功。

S509, 终端设备向基站发送注册请求。

其中, 所述注册请求包含参数 EPC。

S510, 基站向 AMF/TMF 发送注册请求。

其中, 所述注册请求包含参数 EPC。

S511, AMF/TMF 通过基站向终端设备发送注册响应。

S512, AMF/TMF 通过基站向终端设备发送接入命令。

其中, 接入命令可以包括: Req_RN: 请求新的 RN16; Read: 读取数据; Write: 写入数据; Kill: 灭活标签 (需要 kill password); Lock: 锁定操作 (锁定区域不能读/写); Access: 使标签转入安全(Secured)状态, 即可以执行 Lock 操作 (需要 access password); BlockWrite: 多字的写入操作; BlockErase: 多字的擦除操作。

S513, 终端设备根据本地配置的安全策略发起验证流程。

可选的, 终端设备接收到接入命令后, 根据接入命令发起验证流程。

S514, 终端设备向 TMF/AMF 发送第一请求。

其中, 所述第一请求可以包括第一数值。可选的, 第一请求还可以包括 EPC。

其中, 第一数值可以为终端设备生成的随机数 RAND1 或计数器 Count1。当终端设备本地维护计数器 Count1 时, 在终端设备每次发出计数器 Count1 之后将本地维护的 Count1 加 1。

其中, 所述第一请求可以为认证请求响应。

S515, AMF/TMF 通过 NEF 或 proxy 向验证功能发送第一请求。

其中, 所述第一请求可以包括第一数值。可选的, 第一请求还可以包括 EPC。第一数值可以包括终端设备生成的随机数 RAND1 或计数器 Count1。

其中, 所述第一请求可以为企业认证请求。

可选的, TMF/AMF 可以向 UDM/AUSF 发送第一请求。其中, 所述第一请求中包括第一数值。可选的, 所述第一请求还可以包括 EPC。在这种情况下, 图 5 中 AF/AAA 与 TMF/AMF 的交互过程可以修改为 UDM/AUSF 与 TMF/AMF 的交互。UDM/AUSF 预先配置终端设备的 EPC、安全密钥 K 以及计数器 Count2 (计数器 Count2 的配置和维护是可选的)。也即通过 UDM/AUSF 完成验证流程。

S516, 验证功能根据接收到的第一请求中的第一数值和所述安全密钥, 确定第一响应值。

其中, 第一响应值 $RES1 = MAC(K, RAND1)$ 。或者, 第一响应值 $RES1 = MAC(K, Count1)$ 。K 为安全密钥, RAND1 为第一数值, MAC 是任意一个消息认证码算法。

需要说明的是, 由于终端设备与网络设备之间存在通信距离, 在传输过程中数据有可能被篡改。验证功能接收到的第一请求中第一数值与终端设备发送的第一请求中的第一数值可能相同, 也有可能不相同。

需要说明的是, 可以通过其他方式, 根据第一数值和安全密钥计算第一响应值。通过其他方式计算的第一响应值或其他响应值都在本申请保护的范围内。

S517, 验证功能向终端设备第一响应消息。

其中, 第一响应消息包括第一响应值。

可选的, 第一响应消息包括第二数值。第二数值可以为网络设备(例如基站、TMF/AMF或验证功能)生成的随机数 RAND2 或计数器 Count 2。当验证功能本地维护计数器 Count2, 验证功能在每次发出计数器 Count2 之后将本地维护的 Count2 加 1。

其中, 如果第二数值不是由验证功能生成的, 例如第二数值是由 TMF/AMF 或基站生成, 验证功能也可以从 TMF/AMF 或基站获取第二数值。

可选的, 第一响应消息还可以包括 EPC。

其中, 第一响应消息可以为标签认证响应。

S518, 终端设备根据第一响应值, 对网络设备进行验证。

具体的, 终端设备可以根据第一数值和所述安全密钥, 确定第三响应值。其中, 该第一数值为终端设备生成的随机数 RAND1 或计数器 Count1, 与 S514 中终端设备发送的第一请求中的第一数值相同。第三响应值 $RES3 = MAC(K, RAND1)$, 或者, 第三响应值 $RES3 = MAC(K, Count1)$ 。然后, 确定所述第一响应值与所述第三响应值是否相同; 当所述第一响应值与所述第三响应值相同时, 确定所述网络设备通过验证, 说明网络设备是安全的, 当所述第一响应值与所述第三响应值不相同, 确定所述网络设备未通过验证, 说明网络设备存在通信安全问题。

可选的, 当终端设备确定网络设备通过验证时, 可以根据接收到的第一响应消息中的第二数值和所述安全密钥, 确定第二响应值。其中, 第二数值为网络设备生成的随机数 RAND2 或计数器 Count2。第二响应值 $RES2 = MAC(K, RAND2)$, 或者, 第二响应值 $RES2 = MAC(K, Count2)$ 。

需要说明的是, 由于终端设备与网络设备之间存在通信距离, 在传输过程中数据有可能被篡改。终端设备接收到的第一响应消息中第二数值与验证功能发送的第一响应消息中的第二数值可能相同, 也有可能不相同。

S519, 终端设备向验证功能发送第二请求。

可选的, 终端设备通过 TMF/AMF(或通过 NEF 或 proxy) 向验证功能发送第二请求。

其中, 第二请求可以包括第二响应值。可选的, 第二请求还可以包括 EPC。

其中, 第二请求可以为标签认证请求。

S520, 验证功能根据第二响应值, 对终端设备进行验证。

具体的, 验证功能根据第二数值和安全密钥, 确定第四响应值。其中, 该第二数值可以为随机数 RAND2 或计数器 Count 2, 与 S517 中验证功能发送的第一响应消息中第二数值相同。第四响应值 $RES4 = MAC(K, RAND2)$, 或者, 第四响应值 $RES4 = MAC(K, Count2)$ 。K 为安全密钥, MAC 是任意一个消息认证码算法。然后, 验证功能确定所述第二响应值与所述第四响应值是否相同; 当所述第二响应值与所述第四响应值相同时, 确定所述终端设备通过验证, 说明终端设备是安全的, 当所述第二响应值与所述第四响应值不相同, 确定所述终端设备未通过验证, 说明终端设备存在安全问题。

可选的, 验证功能可以根据所述第一数值和所述第二数值中的至少一项、以及所述安全密钥和产品电子代码 EPC 生成确定衍生密钥 Ktmf。其中, 所述衍生密钥 Ktmf 可以用于信令加密和/或完整性保护。

S521, 验证功能通过 NEF 或 proxy 向 TMF/AMF 发送第二响应消息。

其中, 第二响应消息可以包括验证结果, 所述验证结果包括终端设备通过验证或终端设

备未通过验证。

可选的，当验证功能确定终端设备通过验证时，验证功能可以向 AMF 实体或 TMF 实体发送第二响应消息。其中，第二响应消息可以包括衍生密钥 K_{tmf}。

其中，第二响应消息可以为企业认证响应。

S522，终端设备通过基站向 TMF/AMF 发送接入命令响应。

在本申请实施例中，终端设备在接收到接入命令之后，根据安全策略发起验证流程。验证功能根据终端设备生成的第一数值确定第一响应值，并将第一响应值发送给终端设备，使得终端设备对网络设备进行验证。并且，终端设备根据网络设备生成的第二数值确定第二响应值，并将第二响应值发送给网络设备，使得网络设备对终端设备进行验证。实现终端设备与网络设备之间的双向验证，从而保障终端设备与网络设备之间的通信安全。

上述实施例中实现了终端设备与网络设备的双向验证，下面图 6 所示的实施例仅对网络设备进行单向验证。并且，该实施例中的终端设备可以根据接入命令判断是否执行对网络设备的单向验证。

如图 6 所示，图 6 是本申请实施例提供的一种安全验证方法的流程示意图。本申请实施例中的步骤主要包括：

S601，企业打印标签，在终端设备中写入 EPC 和安全密钥 K，在验证功能中存储 EPC 以及安全密钥 K。

其中，终端设备可以为标签、UE 或者 UE 中的芯片。验证功能可以为 AF 或 AAA。终端设备和验证功能中的安全密钥 K 相同。

其中，EPC 用于标识终端设备。

S602-S612，与图 5 中 S502-S512 相同，具体实现方式可以参考图 5 中的 502-S512，此处不再赘述。

S613，终端设备生成第一数值。

可选的，终端设备可以根据接入命令判断是否执行对网络设备的单向验证。在确定执行对网络设备的单向验证之后，生成第一数值。

进一步的，终端设备判断是否执行对网络设备的单向验证的方式包括：

第一种方式，终端设备只要接收到接入命令，开始执行对网络设备的单向验证。

第二种方式，终端设备只有在接收到指定的接入命令之后，开始执行对网络设备的单向验证。所述指定的接入命令可以包括 Write、Kill、Lock 等命令。

以上判断方式可以在打印标签时写入终端设备。

其中，第一数值可以为终端设备生成的随机数 RAND 或计数器 Count。当终端设备本地维护计数器 Count 时，在终端设备每次发出计数器 Count 之后将本地维护的 Count 加 1。

S614，终端设备向 TMF/AMF 发送第一请求。

其中，第一请求可以包括第一数值。

可选的，第一请求可以包括 EPC，所述 EPC 用于标识终端设备。

其中，第一请求可以为认证请求。

S615，TMF/AMF 通过 NEF 或 proxy 向验证功能发送第二请求。

其中，所述第二请求可以包括第一数值。可选的，第二请求还可以包括 EPC。

其中，所述第二请求可以为企业认证请求。

可选的，TMF/AMF 可以向 UDM/AUSF 发送第二请求。其中，所述第二请求中包括第

一数值。可选的,所述第二请求还可以包括EPC。在这种情况下,图6中AF/AAA与TMF/AMF的交互过程可以修改为UDM/AUSF与TMF/AMF的交互。UDM/AUSF预先配置终端设备的EPC、安全密钥K以及计数器Count(计数器Count的配置和维护是可选的)。也即通过UDM/AUSF完成验证流程。

S616,验证功能根据接收到的第二请求中的第一数值和所述安全密钥,确定第一响应值。

其中,第一数值为终端设备生成的随机数RAND或计数器Count。第一响应值 $RES1 = MAC(K, RAND)$,或者,第一响应值 $RES1 = MAC(K, Count)$ 。K为安全密钥,MAC是任意一个消息认证码算法。

需要说明的是,由于终端设备与网络设备之间存在通信距离,在传输过程中数据有可能被篡改。验证功能接收到的第二请求中第一数值与终端设备发送的第一请求中的第一数值可能相同,也有可能不相同。

需要说明的是,可以通过其他方式,根据第一数值和安全密钥计算第一响应值。通过其他方式计算的第一响应值或其他响应值都在本申请保护的范围内。

可选的,验证功能可以根据所述第一数值、所述安全密钥和产品电子代码EPC生成确定衍生密钥Ktmf。其中,所述衍生密钥Ktmf可以用于信令加密和/或完整性保护。

S617,验证功能通过NEF或proxy向AMF/TMF发送第一响应消息。

其中,第一响应消息可以包括第一响应值。

可选的,第一响应消息可以包括衍生密钥Ktmf。AMF/TMF接收到衍生密钥Ktmf之后,可以使用衍生密钥Ktmf进行信令加密或完整性保护。

可选的,第一响应消息可以包括EPC。

S618,AMF/TMF向终端设备发送第二响应消息。

其中,第二响应消息可以包括第一响应值。

可选的,第二响应消息可以包括EPC。

S619,终端设备根据第一响应值,对网络设备进行验证。

具体的,终端设备可以根据第一数值和所述安全密钥,确定第二响应值。其中,该第一数值为终端设备生成的随机数RAND或计数器Count,与S614中终端设备发送的第一请求中的第一数值相同。第二响应值 $RES2 = MAC(K, RAND)$,或者,第二响应值 $RES2 = MAC(K, Count)$ 。然后,确定所述第一响应值与所述第二响应值是否相同;当所述第一响应值与所述第二响应值相同时,确定所述网络设备通过验证,说明网络设备是安全的,当所述第一响应值与所述第二响应值不相同,确定所述网络设备未通过验证,确定所述网络设备未通过验证,说明网络设备存在通信安全问题。

其中,网络设备可以是基站、TMF/AMF或验证功能等。

S620,终端设备通过基站向TMF/AMF发送接入命令响应。

具体的,当确定网络设备通过验证时,终端设备可以向TMF/AMF返回接入命令响应。当确定网络设备未通过验证时,终端设备可以向TMF/AMF返回拒绝消息或不返回接入命令响应。

在本申请实施例中,终端设备接收到接入命令后对网络设备发起验证,验证通过后执行接入命令,从而防止恶意基站发起对终端设备的读、写、灭活等命令,从而保障终端设备与网络设备之间的通信安全。

图6所示的实施例中仅对网络设备进行单向验证,而图7所示的实施例仅对终端设备进行

行单向验证。并且，该实施例是在终端设备发出注册请求之后发起对终端设备的验证过程。

如图 7 所示，图 7 是本申请实施例提供的一种安全验证方法的流程示意图。本申请实施例中的步骤主要包括：

S701，企业打印标签，在终端设备中写入 EPC 和安全密钥 K，在验证功能中存储 EPC 以及安全密钥 K。

其中，终端设备可以为标签、UE 或者 UE 中的芯片。验证功能可以为 AF 或 AAA。终端设备和验证功能中的安全密钥 K 相同。

其中，EPC 用于标识终端设备。

S702-S710，与图 5 中 S502-S510 相同，具体实现方式可以参考图 5 中的 502-S510，此处不再赘述。

S711，AMF/TMF 向验证功能发送第一请求。

其中，第一请求可以包括所述 EPC。

其中，所述第一请求可以为企业认证请求。

S712，验证功能向终端设备发送第一响应消息。

可选的，验证功能通过 TMF/AMF（或通过 NEF 或 proxy）向终端设备发送第一响应消息。

其中，所述第一响应消息包括第一数值。所述第一数值为网络设备（例如基站、TMF/AMF 或验证功能）生成的随机数 RAND 或计数器 Count。当验证功能本地维护计数器 Count，验证功能在每次发出计数器 Count 之后将本地维护的 Count 加 1。

其中，如果第一数值不是由验证功能生成的，例如第一值是由 TMF/AMF 或基站生成，验证功能也可以从 TMF/AMF 或基站获取第一数值。

可选的，第一响应消息可以包括 EPC。

其中，第一响应消息可以为标签认证响应。

S713，终端设备根据接收到的第一响应消息中的第一数值和安全密钥，确定第一响应值。

其中，第一数值为网络设备生成的随机数 RAND 或计数器 Count。第一响应值 $RES1 = MAC(K, RAND)$ ，或者，第一响应值 $RES1 = MAC(K, Count)$ 。K 为安全密钥，MAC 是任意一个消息认证码算法。

需要说明的是，由于终端设备与网络设备之间存在通信距离，在传输过程中数据有可能被篡改。终端设备接收到的第一响应消息中第一数值与验证功能发送的第一响应消息中的第一数值可能相同，也有可能不相同。

需要说明的是，可以通过其他方式，根据第一数值和安全密钥计算第一响应值。通过其他方式计算的第一响应值或其他响应值都在本申请保护的范围内。

S714，终端设备向验证功能发送第二请求。

可选的，终端设备通过 TMF/AMF（或通过 NEF 或 proxy）向 AF/AAA 发送第二请求。

其中，第二请求可以包括第一响应值。

可选的，第二请求可以包括 EPC。

其中，所述第二请求可以为标签认证请求。

S715，验证功能根据第一响应值，对终端设备进行验证。

具体的，验证功能可以根据第一数值和所述安全密钥，确定第二响应值。其中，该第一数值为网络设备生成的随机数 RAND 或计数器 Count，与 S712 中验证功能发送的第一响应消息中的第一数值相同。第二响应值 $RES2 = MAC(K, RAND)$ ，或者，第二响应值 $RES2 =$

MAC (K, Count)。然后, 确定所述第一响应值与所述第二响应值是否相同; 当所述第一响应值与所述第二响应值相同时, 确定所述终端设备通过验证, 说明终端设备是安全的, 当所述第一响应值与所述第二响应值不相同, 确定所述终端设备未通过验证, 确定所述终端设备未通过验证, 说明终端设备存在通信安全问题。

可选的, 验证功能可以根据所述第一数值、所述安全密钥和产品电子代码 EPC 生成确定衍生密钥 Ktmf。其中, 所述衍生密钥 Ktmf 可以用于信令加密和/或完整性保护。

S716, 验证功能向 TMF/AMF 发送第二响应消息。

可选的, 验证功能通过 NEF 或 proxy 向 TMF/AMF 发送第二响应消息。

其中, 第二响应消息包括验证结果, 所述验证结果包括终端设备通过验证或终端设备未通过验证。

可选的, 当验证功能确定终端设备验证通过时, 向 TMF/AMF 发送第二响应消息, 所述第二响应消息包括衍生密钥 Ktmf。AMF/TMF 接收到衍生密钥 Ktmf 之后, 可以使用衍生密钥 Ktmf 进行信令加密或完整性保护。

其中, 第二响应消息可以为企业认证响应。

S717, AMF/TMF 通过基站向终端设备发送注册响应。

S718, AMF/TMF 通过基站向终端设备发送接入命令。

S719, 终端设备向 AMF/TMF 发送接入命令响应。

在本申请实施例中, 在终端设备发出注册请求之后, 网络设备对终端设备执行单向验证, 从而保证终端设备上传的 EPC 以及后续数据的真实性, 防止伪终端设备上传虚假 EPC 以及虚假数据, 从而保障终端设备与网络设备之间的通信安全。

在上文实施例中, 终端设备、基站、TMF/AMF 和/或验证功能可以执行各实施例中的部分或全部步骤。例如, 图 4b 所示的实施例中的 S418-S420 是可选的。这些步骤或操作仅是示例, 本申请实施例还可以执行其它操作或者各种操作的变形。此外, 各个步骤可以按照各实施例呈现的不同的顺序来执行, 并且有可能并非要执行本申请实施例中的全部操作。且, 各步骤的序号的大小并不意味着执行顺序的先后, 各过程的执行顺序应以其功能和内在逻辑确定, 而不对本申请实施例的实施过程构成任何限定。

上述各实施例中, 验证功能可以是 AF 或者 AAA, 该验证功能还可以是 UDM。

可以理解的是, 上述各个方法实施例中, 由终端设备实现的方法和操作, 也可以由可用于终端设备的部件 (例如芯片或者电路) 实现, 由验证功能实现的方法和操作, 也可以由可用于验证功能的部件 (例如芯片或者电路) 实现。

上述主要从各个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, 各个网元, 例如发射端设备或者接收端设备, 为了实现上述功能, 其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该可以意识到, 结合本文中所公开的实施例描述的各示例的单元及算法步骤, 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。

本申请实施例可以根据上述方法示例对终端设备或者验证功能进行功能模块的划分, 例如, 可以对应各个功能划分各个功能模块, 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使用硬件的形式实现, 也可以使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。下面以使用对应各个功能划分各个功能模块为例进行说明。

以上, 结合图 4a-图 7 详细说明了本申请实施例提供的方法。以下, 结合图 8 至图 9 详细说明本申请实施例提供的安全验证装置。应理解, 装置实施例的描述与方法实施例的描述相对应, 因此, 未详细描述的内容可以参见上文方法实施例, 为了简洁, 这里不再赘述。

请参见图 8, 图 8 是本申请实施例提供的一种安全验证装置的结构示意图。该安全验证装置可以包括接收模块 801、处理模块 802 和发送模块 803。接收模块 801 和发送模块 803 可以与外部进行通信, 处理模块 802 用于进行处理, 如确定第一响应值等。接收模块 801 和发送模块 803 还可以称为通信接口、收发单元或收发模块。该接收模块 801、处理模块 802 和发送模块 803 可以用于执行上文方法实施例中终端设备所执行的动作。

例如: 接收模块 801 和发送模块 803 也可以称为收发模块或收发单元 (包括接收单元和/或发送单元), 分别用于执行上文方法实施例中终端设备接收和发送的步骤。

在一种可能的设计中, 该安全验证装置可实现对应于上文方法实施例中的终端设备执行的步骤或者流程, 例如, 可以为终端设备, 或者配置于终端设备中的芯片或电路。接收模块 801 和发送模块 803 用于执行上文方法实施例中终端设备的收发相关操作, 处理模块 802 用于执行上文方法实施例中终端设备的处理相关操作。

比如, 接收模块 801, 用于接收网络设备发送的第一命令, 所述第一命令包括第一数值, 所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个;

处理模块 802, 用于根据所述第一数值和安全密钥, 确定第一响应值;

发送模块 803, 用于发送第一请求, 所述第一请求包括所述第一响应值, 所述第一响应值用于验证功能对所述终端设备进行验证。

需要说明的是, 各个模块的实现还可以对应参照图 4a-图 7 所示的方法实施例的相应描述, 执行上述实施例中终端设备所执行的方法和功能。

请参见图 9, 图 9 是本申请实施例提供的一种安全验证装置的结构示意图。该安全验证装置可以包括接收模块 901、处理模块 902 和发送模块 903。接收模块 901 和发送模块 903 可以与外部进行通信。接收模块 901 和发送模块 903 还可以称为通信接口、收发单元或收发模块。处理模块 902 用于进行处理, 如对终端设备进行验证等。该接收模块 901、处理模块 902 和发送模块 903 可以用于执行上文方法实施例中验证功能所执行的动作。

例如: 接收模块 901 和发送模块 903 也可以称为收发模块或收发单元 (包括接收单元和/或发送单元), 分别用于执行上文方法实施例中验证功能接收和发送的步骤。

在一种可能的设计中, 该安全验证装置可实现对应于上文方法实施例中的验证功能执行的步骤或者流程, 例如, 可以为验证功能, 或者配置于验证功能中的芯片或电路。接收模块 901 和发送模块 903 用于执行上文方法实施例中验证功能的收发相关操作。处理模块 902 用于执行上文方法实施例中验证功能的处理相关操作。

比如, 接收模块 901, 用于接收第一请求, 所述第一请求包括第一响应值, 所述第一响应值为根据安全密钥和网络设备的第一命令中包括的第一数值确定, 所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个;

处理模块 902, 用于根据所述第一响应值, 对所述终端设备进行验证。

需要说明的是, 各个模块的实现还可以对应参照图 4a-图 7 所示的方法实施例的相应描述, 执行上述实施例中验证功能所执行的方法和功能。

图 10 是本申请实施例提供的一种终端设备的结构示意图。该终端设备可应用于如图 1 所示的系统中, 执行上述方法实施例中终端设备的功能, 或者实现上述方法实施例中终端设备执行的步骤或者流程。

如图 10 所示, 该终端设备包括处理器 1001 和收发器 1002。可选地, 该终端设备还包括存储器 1003。其中, 处理器 1001、收发器 1002 和存储器 1003 之间可以通过内部连接通路互相通信, 传递控制和/或数据信号, 该存储器 1003 用于存储计算机程序, 该处理器 1001 用于从该存储器 1003 中调用并运行该计算机程序, 以控制该收发器 1002 收发信号。可选地, 终端设备还可以包括天线, 用于将收发器 1002 输出的上行数据或上行控制信令通过无线信号发送出去。

上述处理器 1001 可以与图 8 中的处理模块对应, 上述处理器 1001 可以和存储器 1003 可以合成一个处理装置, 处理器 1001 用于执行存储器 1003 中存储的程序代码来实现上述功能。具体实现时, 该存储器 1003 也可以集成在处理器 1001 中, 或者独立于处理器 1001。

上述收发器 1002 可以与图 8 中的接收模块和发送模块对应, 也可以称为收发单元或收发模块。收发器 1002 可以包括接收器 (或称接收机、接收电路) 和发射器 (或称发射机、发射电路)。其中, 接收器用于接收信号, 发射器用于发射信号。

应理解, 图 10 所示的终端设备能够实现图 4a-图 7 所示方法实施例中涉及终端设备的各个过程。终端设备中的各个模块的操作和/或功能, 分别为了实现上述方法实施例中的相应流程。具体可参见上述方法实施例中的描述, 为避免重复, 此处适当省略详述描述。

上述处理器 1001 可以用于执行前面方法实施例中描述的由终端设备内部实现的动作, 而收发器 1002 可以用于执行前面方法实施例中描述的终端设备向验证功能发送或从验证功能接收的动作。具体请见前面方法实施例中的描述, 此处不再赘述。

其中, 处理器 1001 可以是中央处理器单元, 通用处理器, 数字信号处理器, 专用集成电路, 现场可编程门阵列或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框, 模块和电路。处理器 1001 也可以是实现计算功能的组合, 例如包含一个或多个微处理器组合, 数字信号处理器和微处理器的组合等等。通信总线 1004 可以是外设部件互连标准 PCI 总线或扩展工业标准结构 EISA 总线等。所述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 10 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。通信总线 1004 用于实现这些组件之间的连接通信。其中, 本申请实施例中收发器 1002 用于与其他节点设备进行信令或数据的通信。存储器 1003 可以包括易失性存储器, 例如非挥发性动态随机存取内存 (nonvolatile random access memory, NVRAM)、相变化随机存取内存 (phase change RAM, PRAM)、磁阻式随机存取内存 (magnetoresistive RAM, MRAM) 等, 还可以包括非易失性存储器, 例如至少一个磁盘存储器件、电子可擦除可编程只读存储器 (electrically erasable programmable read-only memory, EEPROM)、闪存器件, 例如反或闪存 (NOR flash memory) 或是反及闪存 (NAND flash memory)、半导体器件, 例如固态硬盘 (solid state disk, SSD) 等。存储器 1003 可选的还可以是至少一个位于远离前述处理器 1001 的存储装置。存储器 1003 中可选的还可以存储一组计算机程序代码或配置信息。可选的, 处理器 1001 还可以执行存储器 1003 中所存储的程序。处理器可以与存储器和收发器相配合, 执行上述申请实施例中终端设备的任意一种方法和功能。

图 11 是本申请实施例提供的一种验证功能的结构示意图。该验证功能可应用于如图 1 所示的系统中, 执行上述方法实施例中验证功能的功能, 或者实现上述方法实施例中验证功能

执行的步骤或者流程。

如图 11 所示, 该验证功能包括处理器 1101 和收发器 1102。可选地, 该验证功能还包括存储器 1103。其中, 处理器 1101、收发器 1102 和存储器 1103 之间可以通过内部连接通路互相通信, 传递控制和/或数据信号, 该存储器 1103 用于存储计算机程序, 该处理器 1101 用于从该存储器 1103 中调用并运行该计算机程序, 以控制该收发器 1102 收发信号。可选地, 验证功能还可以包括天线, 用于将收发器 1102 输出的上行数据或上行控制信令通过无线信号发送出去。

上述处理器 1101 可以与图 9 中的处理模块对应, 上述处理器 1101 和存储器 1103 可以合成为一个处理装置, 处理器 1101 用于执行存储器 1103 中存储的程序代码来实现上述功能。具体实现时, 该存储器 1103 也可以集成在处理器 1101 中, 或者独立于处理器 1101。

上述收发器 1102 可以与图 9 中的发送模块和接收模块对应, 也可以称为收发单元或收发模块。收发器 1102 可以包括接收器 (或称接收机、接收电路) 和发射器 (或称发射机、发射电路)。其中, 接收器用于接收信号, 发射器用于发射信号。

应理解, 图 11 所示的验证功能能够实现图 4a-图 7 所示方法实施例中涉及验证功能的各个过程。验证功能中的各个模块的操作和/或功能, 分别为了实现上述方法实施例中的相应流程。具体可参见上述方法实施例中的描述, 为避免重复, 此处适当省略详述描述。

上述处理器 1101 可以用于执行前面方法实施例中描述的由验证功能内部实现的动作, 而收发器 1102 可以用于执行前面方法实施例中描述的验证功能向终端设备发送或从终端设备接收的动作。具体请见前面方法实施例中的描述, 此处不再赘述。

其中, 处理器 1101 可以是前文提及的各种类型的处理器。通信总线 1104 可以是外设部件互连标准 PCI 总线或扩展工业标准结构 EISA 总线等。所述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 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。通信总线 1104 用于实现这些组件之间的连接通信。其中, 本申请实施例中设备的收发器 1102 用于与其他设备进行信令或数据的通信。存储器 1103 可以是前文提及的各种类型的存储器。存储器 1103 可选的还可以是至少一个位于远离前述处理器 1101 的存储装置。存储器 1103 中存储一组计算机程序代码或配置信息, 且处理器 1101 执行存储器 1103 中程序。处理器可以与存储器和收发器相配合, 执行上述申请实施例中验证功能的任意一种方法和功能。

本申请实施例还提供了一种芯片系统, 该芯片系统包括处理器, 用于支持终端设备或验证功能以实现上述任一实施例中所涉及的功能, 例如生成或处理上述方法中所涉及的第一响应值。在一种可能的设计中, 所述芯片系统还可以包括存储器, 所述存储器, 用于终端设备或验证功能必要的程序指令和数据。该芯片系统, 可以由芯片构成, 也可以包含芯片和其他分立器件。其中, 芯片系统的输入和输出, 分别对应方法实施例终端设备或验证功能的接收与发送操作。

本申请实施例还提供了一种处理装置, 包括处理器和接口。所述处理器可用于执行上述方法实施例中的方法。

应理解, 上述处理装置可以是一个芯片。例如, 该处理装置可以是现场可编程门阵列 (field programmable gate array, FPGA), 可以是专用集成芯片 (application specific integrated circuit, ASIC), 还可以是系统芯片 (system on chip, SoC), 还可以是中央处理器 (central processor unit, CPU), 还可以是网络处理器 (network processor, NP), 还可以是数字信号处理电路 (digital signal processor, DSP), 还可以是微控制器 (micro controller unit, MCU), 还可以是可编程

控制器 (programmable logic device, PLD) 或其他集成芯片。

在实现过程中, 上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成, 或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器, 闪存、只读存储器, 可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器, 处理器读取存储器中的信息, 结合其硬件完成上述方法的步骤。为避免重复, 这里不再详细描述。

根据本申请实施例提供的方法, 本申请还提供一种计算机程序产品, 该计算机程序产品包括: 计算机程序, 当该计算机程序在计算机上运行时, 使得该计算机执行图 4a-图 7 所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法, 本申请还提供一种计算机可读介质, 该计算机可读介质存储有计算机程序, 当该计算机程序在计算机上运行时, 使得该计算机执行图 4a-图 7 所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法, 本申请还提供一种通信系统, 其包括前述的一个或多个终端设备以及一个或多个验证功能。

在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时, 全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。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、服务器或数据中心通过有线 (例如同轴电缆、光纤、数字用户线 (digital subscriber line, DSL)) 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 (例如, 高密度数字视频光盘 (digital video disc, DVD))、或者半导体介质 (例如, 固态硬盘 (solid state disc, SSD)) 等。

上述各个装置实施例中验证功能与终端设备和方法实施例中的验证功能或终端设备对应, 由相应的模块或单元执行相应的步骤, 例如接收模块和发送模块 (收发器) 执行方法实施例中接收或发送的步骤, 除发送、接收外的其它步骤可以由处理模块 (处理器) 执行。具体模块的功能可以参考相应的方法实施例。其中, 处理器可以为一个或多个。

在本申请所提供的几个实施例中, 应该理解到, 所揭露的系统、装置和方法, 可以通过其它的方式实现。例如, 以上所描述的装置实施例仅仅是示意性的, 例如, 所述单元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个系统, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性, 机械或其它的形式。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用, 可以存储在一个计算机可读存储介质中。基于这样的理解, 本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来, 该计算机软件产品存储在一个存储介质中, 包括若干指令用以使得一台计算机设备 (可以是个人计算机, 服

务器，或者验证功能等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory, ROM）、随机存取存储器（random access memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种安全验证方法，其特征在于，所述方法包括：
接收网络设备发送的第一命令，所述第一命令包括第一数值，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；
根据所述第一数值和安全密钥，确定第一响应值；
发送第一请求，所述第一请求包括所述第一响应值，所述第一响应值用于验证功能对终端设备进行验证。
2. 如权利要求1所述的方法，其特征在于，所述第一请求还包括第二数值，所述第二数值用于所述验证功能确定第二响应值；所述方法还包括：
接收第一响应消息，所述第一响应消息包括所述第二响应值；
根据所述第二响应值，对所述网络设备进行验证。
3. 如权利要求2所述的方法，其特征在于，所述根据所述第二响应值，对所述网络设备进行验证包括：
根据所述第二数值和所述安全密钥，确定第三响应值；
确定所述第二响应值与所述第三响应值是否相同；
当所述第二响应值与所述第三响应值相同时，确定所述网络设备通过验证。
4. 如权利要求2或3所述的方法，其特征在于，所述第一响应消息还包括产品电子代码EPC，所述EPC用于标识所述终端设备。
5. 如权利要求1-4任一项所述的方法，其特征在于，所述第一请求中还包括产品电子代码EPC，所述EPC用于标识所述终端设备；和/或
所述验证功能包括应用功能或认证、授权和计费功能。
6. 如权利要求1-5任一项所述的方法，所述验证功能包括统一数据管理功能。
7. 一种安全验证方法，其特征在于，所述方法包括：
验证功能接收第一请求，所述第一请求包括第一响应值，所述第一响应值为根据安全密钥和网络设备的第一命令中包括的第一数值确定，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；
所述验证功能根据所述第一响应值，对终端设备进行验证。
8. 如权利要求7所述的方法，其特征在于，所述验证功能根据所述第一响应值，对终端设备进行验证包括：
所述验证功能确定第三数值，根据所述第三数值和所述安全密钥，确定第四响应值；
所述验证功能确定所述第一响应值与所述第四响应值是否相同；
当所述第一响应值与所述第四响应值相同时，所述验证功能确定所述终端设备通过验证。

9. 如权利要求 7 或 8 所述的方法, 其特征在于, 所述第一请求还包括第二数值; 所述方法还包括:

所述验证功能根据所述第二数值和所述安全密钥, 确定第二响应值;

所述验证功能发送第一响应消息, 所述第一响应消息包括所述第二响应值, 所述第二响应值用于所述终端设备对所述网络设备进行验证。

10. 如权利要求 9 所述的方法, 其特征在于, 所述方法还包括:

所述验证功能向接入和移动性管理功能 AMF 或标签管理功能 TMF 发送第二响应消息, 所述第二响应消息包括衍生密钥, 所述衍生密钥为根据所述第一数值和所述第二数值中的至少一项、以及所述安全密钥和产品电子代码 EPC 生成, 所述 EPC 用于标识所述终端设备。

11. 如权利要求 9 或 10 所述的方法, 其特征在于, 所述第一响应消息还包括产品电子代码 EPC, 所述 EPC 用于标识所述终端设备。

12. 如权利要求 7-11 任一项所述的方法, 其特征在于, 所述第一请求中还包括产品电子代码 EPC, 所述 EPC 用于标识所述终端设备; 和/或

所述验证功能包括应用功能或认证、授权和计费功能。

13. 如权利要求 7-12 任一项所述的方法, 所述验证功能包括统一数据管理功能。

14. 一种安全验证装置, 其特征在于, 所述装置包括:

接收模块, 用于接收网络设备发送的第一命令, 所述第一命令包括第一数值, 所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个;

处理模块, 用于根据所述第一数值和安全密钥, 确定第一响应值;

发送模块, 用于发送第一请求, 所述第一请求包括所述第一响应值, 所述第一响应值用于验证功能对终端设备进行验证。

15. 如权利要求 14 所述的装置, 其特征在于, 所述第一请求还包括第二数值, 所述第二数值用于所述验证功能确定第二响应值;

所述接收模块, 还用于接收第一响应消息, 所述第一响应消息包括所述第二响应值;

所述处理模块, 还用于根据所述第二响应值, 对所述网络设备进行验证。

16. 如权利要求 15 所述的装置, 其特征在于,

所述处理模块, 还用于根据所述第二数值和所述安全密钥, 确定第三响应值; 确定所述第二响应值与所述第三响应值是否相同; 当所述第二响应值与所述第三响应值相同时, 确定所述网络设备通过验证。

17. 如权利要求 15 或 16 所述的装置, 其特征在于, 所述第一响应消息还包括产品电子代码 EPC, 所述 EPC 用于标识所述终端设备。

18. 如权利要求 14-17 任一项所述的装置, 其特征在于, 所述第一请求中还包括产品电

子代码 EPC，所述 EPC 用于标识所述终端设备；和/或
所述验证功能包括应用功能或认证、授权和计费功能。

19. 如权利要求 14-18 任一项所述的装置，所述验证功能包括统一数据管理功能。

20. 一种安全验证装置，其特征在于，所述装置包括：

接收模块，用于接收第一请求，所述第一请求包括第一响应值，所述第一响应值为根据安全密钥和网络设备的第一命令中包括的第一数值确定，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；

处理模块，用于根据所述第一响应值，对终端设备进行验证。

21. 如权利要求 20 所述的装置，其特征在于，

所述处理模块，还用于确定第三数值，根据所述第三数值和所述安全密钥，确定第四响应值；确定所述第一响应值与所述第四响应值是否相同；当所述第一响应值与所述第四响应值相同时，确定所述终端设备通过验证。

22. 如权利要求 20 或 21 所述的装置，其特征在于，所述第一请求还包括第二数值；

所述处理模块，还用于根据所述第二数值和所述安全密钥，确定第二响应值；

所述发送模块，还用于发送第一响应消息，所述第一响应消息包括所述第二响应值，所述第二响应值用于所述终端设备对所述网络设备进行验证。

23. 如权利要求 22 所述的装置，其特征在于，

所述发送模块，还用于向接入和移动性管理功能 AMF 或标签管理功能 TMF 发送第二响应消息，所述第二响应消息包括衍生密钥，所述衍生密钥为根据所述第一数值和所述第二数值中的至少一项、以及所述安全密钥和产品电子代码 EPC 生成，所述 EPC 用于标识所述终端设备。

24. 如权利要求 22 或 23 所述的装置，其特征在于，所述第一响应消息还包括产品电子代码 EPC，所述 EPC 用于标识所述终端设备。

25. 如权利要求 20-24 任一项所述的装置，其特征在于，所述第一请求中还包括产品电子代码 EPC，所述 EPC 用于标识所述终端设备；和/或

所述安全验证装置包括应用功能或认证、授权和计费功能。

26. 如权利要求 20-25 任一项所述的装置，所述安全验证装置包括统一数据管理功能。

27. 一种安全验证方法，其特征在于，所述方法包括：

终端设备接收网络设备发送的第一命令，所述第一命令包括第一数值，所述第一命令为选择命令、查询命令、查询重复命令、查询调整命令或确认命令中的一个；根据所述第一数值和安全密钥，确定第一响应值；发送第一请求，所述第一请求包括所述第一响应值；

验证功能接收所述第一请求；根据所述第一响应值，对所述终端设备进行验证。

28. 如权利要求 27 所述的方法, 其特征在于, 所述根据所述第一响应值, 对所述终端设备进行验证包括:

所述验证功能确定第三数值, 根据所述第三数值和所述安全密钥, 确定第四响应值;

所述验证功能确定所述第一响应值与所述第四响应值是否相同;

当所述第一响应值与所述第四响应值相同时, 所述验证功能确定所述终端设备通过验证。

29. 如权利要求 27 或 28 所述的方法, 其特征在于, 所述第一请求还包括第二数值; 所述方法还包括:

所述验证功能根据所述第二数值和所述安全密钥, 确定第二响应值; 发送第一响应消息, 所述第一响应消息包括所述第二响应值;

所述终端设备接收所述第一响应消息; 根据所述第二响应值, 对所述网络设备进行验证。

30. 如权利要求 29 所述的方法, 其特征在于, 所述根据所述第二响应值, 对所述网络设备进行验证包括:

所述终端设备根据所述第二数值和所述安全密钥, 确定第三响应值;

所述终端设备确定所述第二响应值与所述第三响应值是否相同;

当所述第二响应值与所述第三响应值相同时, 所述终端设备确定所述网络设备通过验证。

31. 如权利要求 29 或 30 所述的方法, 其特征在于, 所述第一响应消息还包括产品电子代码 EPC, 所述 EPC 用于标识所述终端设备。

32. 如权利要求 27-31 任一项所述的方法, 其特征在于, 所述第一请求中还包括产品电子代码 EPC, 所述 EPC 用于标识所述终端设备; 和/或

所述验证功能包括应用功能或认证、授权和计费功能。

33. 如权利要求 27-32 任一项所述的方法, 所述验证功能包括统一数据管理功能。

34. 一种安全验证系统, 其特征在于, 所述系统包括终端设备和验证功能, 所述终端设备包括如权利要求 14-19 任一项所述的装置, 所述验证功能包括如权利要求 20-26 任一项所述的装置。

35. 一种计算机可读存储介质, 其特征在于, 用于存储计算机程序, 当所述计算机程序在计算机上运行时, 使所述计算机执行权利要求 1-13 中任一项所述的方法。

36. 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计算机程序, 当所述计算机程序在计算机上运行时, 使所述计算机执行权利要求 1-6 中任一项或权利要求 7-13 中任一项所述的方法。