(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118802297 A
(43)申请公布日 2024.10.18

(21)申请号 202410466115.3

(22)申请日 2024.04.18

(71)申请人 中国移动通信有限公司研究院
地址 100053 北京市西城区宣武门西大街32号
申请人 中国移动通信集团有限公司

(72)发明人 彭华熹 张艳 李邦灵

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
专利代理师 张蓉

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/14(2006.01)
H04L 9/08(2006.01)

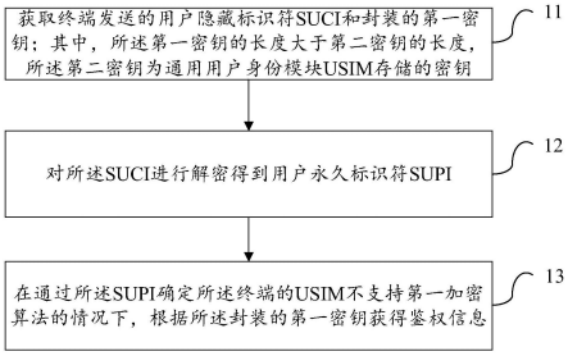
权利要求书3页 说明书18页 附图4页

(54)发明名称

鉴权处理方法、装置及相关设备

(57)摘要

本发明提供一种鉴权处理方法、装置及相关设备,涉及通信技术领域。该方法包括:获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM存储的密钥;对所述SUCI进行解密得到用户永久标识符SUPI;在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。本发明的方案,实现了提升鉴权过程的安全性的目的。



CN 118802297 A

1.一种鉴权处理方法,其特征在于,由网络侧设备执行,包括:

获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM存储的密钥;

对所述SUCI进行解密得到用户永久标识符SUPI;

在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

2.根据权利要求1所述的方法,其特征在于,所述根据所述封装的第一密钥获得鉴权信息,包括:

对所述封装的第一密钥进行解封装,得到所述第一密钥,并将所述第一密钥和所述SUPI进行关联存储;

根据所述第一密钥和所述第二密钥,得到所述鉴权信息。

3.根据权利要求2所述的方法,其特征在于,所述根据所述第一密钥和所述第二密钥,得到所述鉴权信息,包括:

根据第二加密算法和所述第二密钥得到第一信息;

根据所述第一加密算法、所述第一密钥和所述第一信息中的随机数,得到第二信息;

根据所述第一信息和所述第二信息,得到鉴权相关信息;

根据所述鉴权相关信息,得到所述鉴权信息。

4.根据权利要求3所述的方法,其特征在于,所述根据所述第一信息和所述第二信息,得到鉴权相关信息,包括:

基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌;

基于所述第一信息中的第一预期响应值以及所述第二信息中的第二预期响应值,得到第三预期响应值;

基于所述第三密钥和所述第一信息中的第六密钥,得到第七密钥;

基于所述第四密钥和所述第一信息中的第八密钥,得到第九密钥;

将所述随机数、所述第三认证令牌、所述第三预期响应值、所述第七密钥和所述第九密钥作为所述鉴权相关信息。

5.根据权利要求4所述的方法,其特征在于,所述基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌,包括:

将所述第一认证令牌与所述第二认证令牌进行串联,并使用所述第五密钥对串联的结果进行加密,得到所述三认证令牌;或者,

使用所述第五密钥对所述第一认证令牌进行加密,并将加密的结果与所述第二认证令牌进行串联,得到所述三认证令牌。

6.根据权利要求4或5所述的方法,其特征在于,所述根据所述鉴权相关信息,得到所述鉴权信息,包括:

基于所述第七密钥和所述第九密钥,得到第十密钥;

基于所述第三预期响应值,得到第四预期响应值;

将所述随机数、所述第三认证令牌、所述第四预期响应值和所述第九密钥作为所述鉴

权信息。

7.根据权利要求1所述的方法,其特征在于,所述根据所述封装的第一密钥获得鉴权信息之后,还包括:

向所述终端发送所述鉴权信息中的随机数和第三认证令牌。

8.根据权利要求7所述的方法,其特征在于,所述向所述终端发送所述鉴权信息中的随机数和第三认证令牌之后,还包括:

接收所述终端发送的第一响应值;

根据所述第一响应值,确定认证是否成功。

9.一种鉴权处理方法,其特征在于,由终端执行,包括:

判断通用用户身份模块USIM是否支持第一加密算法;

在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

10.根据权利要求9所述的方法,其特征在于,所述向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥之前,还包括:

获取所述USIM对应的归属网的公钥;

生成所述第一密钥,并使用所述公钥对所述第一密钥进行封装,得到所述封装的第一密钥。

11.根据权利要求9所述的方法,其特征在于,所述向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥之后,还包括:

接收所述网络侧设备发送的随机数和第三认证令牌;

根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌。

12.根据权利要求11所述的方法,其特征在于,所述根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌之后,还包括:

根据所述第一认证令牌进行验证;

在验证通过的情况下确定第一响应值;

向所述网络侧设备发送所述第一响应值。

13.根据权利要求11所述的方法,其特征在于,所述根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌,包括:

基于所述第一密钥和所述随机数,得到第二信息;

基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

使用所述第五密钥对所述第三认证令牌进行解密,得到所述第一认证令牌和第四认证令牌;或者,基于所述第三认证令牌确定第三信息和第四认证令牌,并使用所述第五密钥对所述第三信息进行解密,得到所述第一认证令牌。

14.根据权利要求13所述的方法,其特征在于,还包括:

根据所述第二信息中的第二认证令牌验证所述第四认证令牌。

15.根据权利要求12所述的方法,其特征在于,所述在验证通过的情况下确定第一响应值,包括:

根据第二加密算法和所述第二密钥得到第一信息;

基于所述第一信息中的第一预期响应值和第二信息中的第二预期响应值,得到所述第一响应值。

16.根据权利要求12所述的方法,其特征在于,还包括:

基于第一信息中的第六密钥和第二信息中的第三密钥,得到第七密钥;

基于所述第一信息中的第八密钥和所述第二信息中的第四密钥,得到第九密钥。

17.一种鉴权处理装置,其特征在于,包括:

第一接收模块,用于获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM存储的密钥;

第一处理模块,用于对所述SUCI进行解密得到用户永久标识符SUPI;

第二处理模块,用于在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

18.一种鉴权处理装置,其特征在于,包括:

第三处理模块,用于判断通用用户身份模块USIM是否支持第一加密算法;

第一发送模块,用于在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

19.一种网络侧设备,其特征在于,包括处理器和收发器,

所述收发器用于:获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM存储的密钥;

所述处理器用于:对所述SUCI进行解密得到用户永久标识符SUPI;

所述处理器还用于:在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

20.一种终端,其特征在于,包括处理器和收发器,

所述处理器用于:判断通用用户身份模块USIM是否支持第一加密算法;

所述收发器用于:在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

21.一种通信设备,包括:收发器、处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序或指令;其特征在于,所述处理器执行所述程序或指令时实现如权利要求1-8任一项所述的鉴权处理方法,或者,如权利要求9-16任一项所述的鉴权处理方法。

22.一种可读存储介质,其上存储有程序或指令,其特征在于,所述程序或指令被处理器执行时实现如权利要求1-8任一项所述的鉴权处理方法,或者,如权利要求9-16任一项所述的鉴权处理方法中的步骤。

23.一种计算机程序产品,其特征在于,包括计算机指令,所述计算机指令被处理器执行时实现如权利要求1-8任一项所述的鉴权处理方法,或者,如权利要求9-16任一项所述的鉴权处理方法的步骤。

鉴权处理方法、装置及相关设备

技术领域

[0001] 本发明涉及通信技术领域,特别是指一种鉴权处理方法、装置及相关设备。

背景技术

[0002] 随着互联网技术快速发展,信息系统的网络安全风险持续增加,威胁挑战日益严峻,密码安全是信息安全的重要基础,可以用于有效保障网络信息系统的数据安全,密码技术是保障网络信息系统的核心技术和重要手段。

[0003] 目前,通信网络的网络鉴权认证密钥协议(Authentication Key Agreement,AKA)基于MILENAGE算法实现,用于完成通用用户身份模块(Universal Subscriber Identity Module,USIM)和统一数据管理(Unified Data Manage,UDM)之间的鉴权认证和密钥协商。MILENAGE算法的底层算法是高级加密标准(Advanced Encryption Standard,AES)-128,USIM和UDM之间共享的密钥K是128bit。

[0004] 然而,随着量子计算技术的发展,传统的密码算法面临着严重的安全威胁。量子计算机具有强大的计算能力,可以大大降低对称密码算法的破解难度,使得AES-128被破解的风险大大增加,攻击者可以通过获取AES-128的明文从而计算出128bit的密钥,降低了系统安全性。

发明内容

[0005] 本发明的目的是提供一种鉴权处理方法、装置及相关设备,以提升鉴权过程的安全性。

[0006] 为达到上述目的,本发明的实施例提供一种鉴权处理方法,由网络侧设备执行,包括:

[0007] 获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM存储的密钥;

[0008] 对所述SUCI进行解密得到用户永久标识符SUPI;

[0009] 在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

[0010] 可选地,所述根据所述封装的第一密钥获得鉴权信息,包括:

[0011] 对所述封装的第一密钥进行解封装,得到所述第一密钥,并将所述第一密钥和所述SUPI进行关联存储;

[0012] 根据所述第一密钥和所述第二密钥,得到所述鉴权信息。

[0013] 可选地,所述根据所述第一密钥和所述第二密钥,得到所述鉴权信息,包括:

[0014] 根据第二加密算法和所述第二密钥得到第一信息;

[0015] 根据所述第一加密算法、所述第一密钥和所述第一信息中的随机数,得到第二信息;

[0016] 根据所述第一信息和所述第二信息,得到鉴权相关信息;

[0017] 根据所述鉴权相关信息,得到所述鉴权信息。

[0018] 可选地,所述根据所述第一信息和所述第二信息,得到鉴权相关信息,包括:

[0019] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0020] 基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌;

[0021] 基于所述第一信息中的第一预期响应值以及所述第二信息中的第二预期响应值,得到第三预期响应值;

[0022] 基于所述第三密钥和所述第一信息中的第六密钥,得到第七密钥;

[0023] 基于所述第四密钥和所述第一信息中的第八密钥,得到第九密钥;

[0024] 将所述随机数、所述第三认证令牌、所述第三预期响应值、所述第七密钥和所述第九密钥作为所述鉴权相关信息。

[0025] 可选地,所述基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌,包括:

[0026] 将所述第一认证令牌与所述第二认证令牌进行串联,并使用所述第五密钥对串联的结果进行加密,得到所述三认证令牌;或者,

[0027] 使用所述第五密钥对所述第一认证令牌进行加密,并将加密的结果与所述第二认证令牌进行串联,得到所述三认证令牌。

[0028] 可选地,所述根据所述鉴权相关信息,得到所述鉴权信息,包括:

[0029] 基于所述第七密钥和所述第九密钥,得到第十密钥;

[0030] 基于所述第三预期响应值,得到第四预期响应值;

[0031] 将所述随机数、所述第三认证令牌、所述第四预期响应值和所述第九密钥作为所述鉴权信息。

[0032] 可选地,所述根据所述封装的第一密钥获得鉴权信息之后,还包括:

[0033] 向所述终端发送所述鉴权信息中的随机数和第三认证令牌。

[0034] 可选地,所述向所述终端发送所述鉴权信息中的随机数和第三认证令牌之后,还包括:

[0035] 接收所述终端发送的第一响应值;

[0036] 根据所述第一响应值,确定认证是否成功。

[0037] 为达到上述目的,本发明的实施例提供一种鉴权处理方法,由终端执行,包括:

[0038] 判断通用用户身份模块USIM是否支持第一加密算法;

[0039] 在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

[0040] 可选地,所述向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥之前,还包括:

[0041] 获取所述USIM对应的归属网的公钥;

[0042] 生成所述第一密钥,并使用所述公钥对所述第一密钥进行封装,得到所述封装的第一密钥。

[0043] 可选地,所述向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥之后,还

包括：

[0044] 接收所述网络侧设备发送的随机数和第三认证令牌；

[0045] 根据所述第一密钥、所述随机数和所述第三认证令牌，得到第一认证令牌。

[0046] 可选地，所述根据所述第一密钥、所述随机数和所述第三认证令牌，得到第一认证令牌之后，还包括：

[0047] 根据所述第一认证令牌进行验证；

[0048] 在验证通过的情况下确定第一响应值；

[0049] 向所述网络侧设备发送所述第一响应值。

[0050] 可选地，所述根据所述第一密钥、所述随机数和所述第三认证令牌，得到第一认证令牌，包括：

[0051] 基于所述第一密钥和所述随机数，得到第二信息；

[0052] 基于所述第二信息中的第三密钥和第四密钥，得到第五密钥；

[0053] 使用所述第五密钥对所述第三认证令牌进行解密，得到所述第一认证令牌和第四认证令牌；或者，基于所述第三认证令牌确定第三信息和第四认证令牌，并使用所述第五密钥对所述第三信息进行解密，得到所述第一认证令牌。

[0054] 可选地，所述方法还包括：

[0055] 根据所述第二信息中的第二认证令牌验证所述第四认证令牌。

[0056] 可选地，所述在验证通过的情况下确定第一响应值，包括：

[0057] 根据第二加密算法和所述第二密钥得到第一信息；

[0058] 基于所述第一信息中的第一预期响应值和第二信息中的第二预期响应值，得到所述第一响应值。

[0059] 可选地，所述方法还包括：

[0060] 基于第一信息中的第六密钥和第二信息中的第三密钥，得到第七密钥；

[0061] 基于所述第一信息中的第八密钥和所述第二信息中的第四密钥，得到第九密钥。

[0062] 为达到上述目的，本发明的实施例提供一种鉴权处理装置，包括：

[0063] 第一接收模块，用于获取终端发送的用户隐藏标识符SUCI和封装的第一密钥；其中，所述第一密钥的长度大于第二密钥的长度，所述第二密钥为通用用户身份模块USIM存储的密钥；

[0064] 第一处理模块，用于对所述SUCI进行解密得到用户永久标识符SUPI；

[0065] 第二处理模块，用于在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下，根据所述封装的第一密钥获得鉴权信息。

[0066] 为达到上述目的，本发明的实施例提供一种鉴权处理装置，包括：

[0067] 第三处理模块，用于判断通用用户身份模块USIM是否支持第一加密算法；

[0068] 第一发送模块，用于在所述USIM不支持所述第一加密算法的情况下，向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥，所述第一密钥的长度大于第二密钥的长度，所述第二密钥为所述USIM存储的密钥。

[0069] 为达到上述目的，本发明的实施例提供一种网络侧设备，包括处理器和收发器，

[0070] 所述收发器用于：获取终端发送的用户隐藏标识符SUCI和封装的第一密钥；其中，所述第一密钥的长度大于第二密钥的长度，所述第二密钥为通用用户身份模块USIM存储的

密钥;

[0071] 所述处理器用于:对所述SUCI进行解密得到用户永久标识符SUPI;

[0072] 所述处理器还用于:在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

[0073] 为达到上述目的,本发明的实施例提供一种终端,包括处理器和收发器,

[0074] 所述处理器用于:判断通用用户身份模块USIM是否支持第一加密算法;

[0075] 所述收发器用于:在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

[0076] 为达到上述目的,本发明的实施例提供一种通信设备,包括收发器、处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序或指令;所述处理器执行所述程序或指令时实现如上所述的鉴权处理方法。

[0077] 为达到上述目的,本发明的实施例提供一种可读存储介质,其上存储有程序或指令,所述程序或指令被处理器执行时实现如上所述的鉴权处理方法中的步骤。

[0078] 为达到上述目的,本发明的实施例提供一种计算机程序产品,包括计算机指令,所述计算机指令被处理器执行时实现如上所述的鉴权处理方法的步骤。

[0079] 本发明的上述技术方案的有益效果如下:

[0080] 本发明实施例的方法,通过获取终端发送的SUCI以及封装的第一密钥,在对SUCI进行解密得到SUPI之后,由SUPI确定所述终端的USIM是否支持第一加密算法,从而针对所述终端的USIM不支持第一加密算法的情况,由封装的第一密钥来获得鉴权信息。其中,由于第一密钥的长度大于USIM的密钥的长度,因此即使USIM不支持第一加密算法,所获得的鉴权信息也增强了抵御量子计算的能力,提升了鉴权过程的安全性。

附图说明

[0081] 图1为本发明实施例的应用于网络侧设备的方法的流程图;

[0082] 图2为本发明实施例的方法的应用流程示意图;

[0083] 图3为本发明实施例的应用于终端的方法的流程图;

[0084] 图4为本发明实施例的装置模块示意图之一;

[0085] 图5为本发明实施例的装置模块示意图之二;

[0086] 图6为本发明实施例的终端的结构图;

[0087] 图7为本发明另一实施例的终端的结构图;

[0088] 图8为本发明实施例的网络侧设备的结构图。

具体实施方式

[0089] 为使本发明要解决的技术问题、技术方案和优点更加清楚,下面将结合附图及具体实施例进行详细描述。

[0090] 应理解,说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本发明的至少一个实施例中。因此,在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外,这些特定的特征、结

构或特性可以任意适合的方式结合在一个或多个实施例中。

[0091] 在本发明的各种实施例中,应理解,下述各过程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,而不应对本发明实施例的实施过程构成任何限定。

[0092] 另外,本文中术语“系统”和“网络”在本文中常可互换使用。

[0093] 在本申请所提供的实施例中,应理解,“与A相应的B”表示B与A相关联,根据A可以确定B。但还应理解,根据A确定B并不意味着仅仅根据A确定B,还可以根据A和/或其它信息确定B。

[0094] 为了方便理解,以下对本发明实施例涉及的一些内容进行说明:

[0095] 1)通用用户身份模块(Universal Subscriber Identity Module,USIM):保存了用户的核心密钥和标识符等数据。

[0096] 2)移动设备(Mobile Equipment,ME):与USIM配合完成网络鉴权。

[0097] 3)用户设备(User Equipment,UE):ME和USIM的统称。

[0098] 4)安全锚功能(Security Anchor Function,SEAF):访问网络实现对UE的鉴权。

[0099] 5)认证服务器功能(Authentication Server Function,AUSF):归属网络实现对UE的鉴权。

[0100] 6)统一数据管理(Unified Data Management,UDM)/归属用户服务器(Home Subscriber Server,HSS):存储用户的签约信息,鉴权数据等。

[0101] 7)密钥封装机制(Key Encapsulation Mechanism,KEM):C=KEM_ENC(PK,M),使用公钥PK对M进行加密封装,KEM_ENC是量子安全的密钥封装算法。

[0102] 8)密钥解封装机制:M=KEM_DEC(SK,C),使用私钥SK对C进行解封装得到明文M,KEM_DEC是量子安全的密钥解封装算法。

[0103] 9)对称加密函数:C=E(K,M),使用对称密钥K对M进行对称加密,E是量子安全的对称加密算法。

[0104] 10)对称解密函数:M=D(K,C),使用对称密钥K对C进行对称解密,D是量子安全的对称解密算法。

[0105] 11)非对称加密函数:C=E_PUB(PK,M),使用公钥PK对M进行非对称加密,E_PUB是量子安全的公钥加密算法。

[0106] 12)非对称解密函数:M=D_PUB(SK,C),使用私钥SK对C进行非对称解密,D_PUB是量子安全的公钥解密算法。

[0107] 13)签名函数:S=SIGN(K,M),使用私钥K对M进行签名。

[0108] 14)验签函数:VERIFY(K,M,S),使用公钥K对S进行验签。

[0109] 15)摘要函数:H=HASH(M),使用量子安全的摘要算法计算M的摘要值。

[0110] 如图1所示,本发明实施例的一种鉴权处理方法,由网络侧设备执行,包括:

[0111] 步骤11,获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM存储的密钥;

[0112] 步骤12,对所述SUCI进行解密得到用户永久标识符SUPI;

[0113] 步骤13,在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

[0114] 如此,按照上述步骤,网络侧设备能够通过获取终端发送的SUCI以及封装的第一密钥,在对SUCI进行解密得到SUPI之后,由SUPI确定所述终端的USIM是否支持第一加密算法,从而针对所述终端的USIM不支持第一加密算法的情况,由封装的第一密钥来获得鉴权信息。其中,由于第一密钥的长度大于USIM的密钥的长度,因此即使USIM不支持第一加密算法,所获得的鉴权信息也增强了抵御量子计算的能力,提升了鉴权过程的安全性。

[0115] 可选地,所述网络侧设备为UDM或HSS。

[0116] 在该实施例中,第一加密算法是基于与第一密钥的长度相同的密钥实现的。例如,第二密钥的长度为128bit,第一密钥的长度为256bit,第一加密算法需要基于256bit的密钥实现,如MILENAGE-256算法。

[0117] 可选地,该实施例中,所述终端通过判断USIM是否支持第一加密算法,在USIM不支持所述第一加密算法的情况下发送SUCI和封装的第一密钥。具体的,终端发送初始化注册请求(Initial Registration Request)消息,该消息携带所述SUCI和所述封装的第一密钥。相应的,所述网络侧设备通过接收Initial Registration Request消息或者经由其它设备转发的消息,获取到所述SUCI和所述封装的第一密钥。例如,UDM接收AUSF发送的鉴权请求(Nudm_Authenticate_Get Request)消息,该消息携带所述SUCI和所述封装的第一密钥。

[0118] 其中,判断USIM是否支持第一加密算法,也可以理解为检查USIM是否为新卡,当USIM为新卡时,该USIM是支持第一加密算法的。

[0119] 可选地,所述终端发送所述SUCI和所述封装的第一密钥之前,获取所述USIM对应的归属网的公钥;生成所述第一密钥,并使用所述公钥对所述第一密钥进行封装,得到所述封装的第一密钥。

[0120] 即,对于不支持第一加密算法的USIM,终端可以通过获取其归属网的公钥PK_HN,使用PK_HN对生成的第一密钥进行封装。其中,终端读取卡上的归属网信息,并获取PK_HN。而获取PK_HN的方式包括:从卡上读取PK_HN;或者,从归属网运营商获取。此外,使用PK_HN对生成的第一密钥K_ME进行封装,可以采用安全的公钥算法,如PQC算法,则对于封装的第一密钥K_ME_ENC,K_ME_ENC=KEM_ENC(PK_HN,K_ME)。

[0121] 其中,K_ME可以是随机生成安全的密钥,如256bit的密钥。

[0122] 可选地,该实施例中,在对所述SUCI进行解密得到SUPI之后,所述网络侧设备如UDM,可以根据SUPI查询对应的USIM的签约数据,来确定USIM是否支持所述第一加密算法。

[0123] 可选地,该实施例中,所述根据所述封装的第一密钥获得鉴权信息,包括:

[0124] 对所述封装的第一密钥进行解封装,得到所述第一密钥,并将所述第一密钥和所述SUPI进行关联存储;

[0125] 根据所述第一密钥和所述第二密钥,得到所述鉴权信息。

[0126] 即,在对K_ME_ENC进行解封装得到K_ME之后,在本地保存K_ME并与SUPI相关联。且,使用K_ME和第二密钥K_USIM获得所述鉴权信息。

[0127] 其中,对K_ME_ENC进行解封装,可以采用KEM_DEC和归属网私钥SK_HN实现,即K_ME=KEM_DEC(SK_HN,K_ME_ENC)。

[0128] 可选地,所述根据所述第一密钥和所述第二密钥,得到所述鉴权信息,包括:

[0129] 根据第二加密算法和所述第二密钥得到第一信息;

[0130] 根据所述第一加密算法、所述第一密钥和所述第一信息中的随机数,得到第二信息;

[0131] 根据所述第一信息和所述第二信息,得到鉴权相关信息;

[0132] 根据所述鉴权相关信息,得到所述鉴权信息。

[0133] 这里,第二加密算法是基于与第二密钥的长度相同的密钥实现的。例如,第二密钥的长度为128bit,第一密钥的长度为256bit,第二加密算法需要基于128bit的密钥实现,如MILENAGE-128算法。

[0134] 可选地,将K_USIM输入到第二加密算法,计算得到的第一信息AV_USIM包括:随机数RAND,第一认证令牌AUTN_USIM,第一预期响应值XRES_USIM,第六密钥CK_USIM,第八密钥IK_USIM。即,AV_USIM=(RAND,AUTN_USIM,XRES_USIM,CK_USIM,IK_USIM)。

[0135] 可选地,将K_ME和AV_USIM中的RAND输入到第一加密算法,计算得到的第二信息AV_ME包括:RAND,第二认证令牌AUTN_ME,第二预期响应值XRES_ME,第三密钥CK_ME,第四密钥IK_ME。即,AV_ME=(RAND,AUTN_ME,XRES_ME,CK_ME,IK_ME)。

[0136] 可选地,该实施例中,所述根据所述第一信息和所述第二信息,得到鉴权相关信息,包括:

[0137] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0138] 基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌;

[0139] 基于所述第一信息中的第一预期响应值以及所述第二信息中的第二预期响应值,得到第三预期响应值;

[0140] 基于所述第三密钥和所述第一信息中的第六密钥,得到第七密钥;

[0141] 基于所述第四密钥和所述第一信息中的第八密钥,得到第九密钥;

[0142] 将所述随机数、所述第三认证令牌、所述第三预期响应值、所述第七密钥和所述第九密钥作为所述鉴权相关信息。

[0143] 其中,第五密钥AUTN_USIM_ENC_K是AUTN_USIM保护密钥。可选地,基于CK_ME和IK_ME,采用单向函数(f函数)计算得到AUTN_USIM_ENC_K,即,AUTN_USIM_ENC_K=f(CK_ME,IK_ME)。其中,若第二密钥的长度为128bit,第一密钥的长度为256bit,AUTN_USIM_ENC_K是256bit的AUTN_USIM保护密钥,所采用的单向函数比如可以是256bit的摘要函数HASH或者密钥导出函数(Key Derivation Function,KDF)。

[0144] 可选地,所述基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌,包括:

[0145] 将所述第一认证令牌与所述第二认证令牌进行串联,并使用所述第五密钥对串联的结果进行加密,得到所述三认证令牌;或者,

[0146] 使用所述第五密钥对所述第一认证令牌进行加密,并将加密的结果与所述第二认证令牌进行串联,得到所述三认证令牌。

[0147] 也就是说,对于第三认证令牌AUTN_ENC,AUTN_ENC=E(AUTN_USIM_ENC_K,AUTN_USIM||AUTN_ME),或者,AUTN_ENC=E(AUTN_USIM_ENC_K,AUTN_USIM)||AUTN_ME,如此,实现对AUTN_USIM的加密和完整性保护。

[0148] 可选地,所述基于所述第一信息中的第一预期响应值以及所述第二信息中的第二

预期响应值,得到第三预期响应值,包括:

[0149] 将第一预期响应值和第二预期响应值进行串联,并获取串联结果的摘要作为第三预期响应值。

[0150] 这里,获取串联结果的摘要可以采用摘要函数,即,对于第三预期响应值XRES,XRES=HASH(XRES_USIM||XRES_ME)。

[0151] 类似于第三预期响应值,第七密钥和第九密钥都可以采用先串联后获取摘要的方式,则对于第七密钥CK,CK=HASH(CK_USIM||CK_ME);对于第九密钥IK,IK=HASH(IK_USIM||IK_ME)。

[0152] 这样,就能够构造鉴权相关信息AV(RAND,AUTN,XRES,CK,IK)。之后,根据AV(RAND,AUTN,XRES,CK,IK),进一步得到鉴权信息。

[0153] 可选地,所述根据所述鉴权相关信息,得到所述鉴权信息,包括:

[0154] 基于所述第七密钥和所述第九密钥,得到第十密钥;

[0155] 基于所述第三预期响应值,得到第四预期响应值;

[0156] 将所述随机数、所述第三认证令牌、所述第四预期响应值和所述第九密钥作为所述鉴权信息。

[0157] 其中,第十密钥K_{AUSF}是基于CK和IK,通过KDF推衍出的;第四预期响应值XRES*是基于XRES,通过KDF推衍出的。如此,可以得到包括RAND、AUTN、XRES*和K_{AUSF}的鉴权信息。

[0158] 该实施例中,对于采用5G AKA的系统,所得的鉴权信息为5G HE AV。相应的,所述网络侧设备如UDM,可以在鉴权响应(Nudm_UEAuthentication_Get Response)消息中向AUSF返回所请求的5G HE AV,并指示5G HE AV用于5G AKA。若Nudm_UEAuthentication_Get请求中包含SUCI,UDM将在Nudm_UEAuthentication_Get响应中包含SUPI。

[0159] AUSF临时保存XRES*及接收到的SUCI或SUPI,AUSF也可保存K_{AUSF}。AUSF基于从UDM/ARPF接收到的5G HE AV,生成一个5G AV。具体的,从XRES*计算出HXRES*,从K_{AUSF}推衍出K_{SEAF},然后用HXRES*和的K_{SEAF}分别替换5G HE AV中XRES*和K_{AUSF},得到5G AV。然后AUSF移除K_{SEAF},通过认证(Nausf_UEAuthentication_Authenticate)响应把5G SE AV(RAND,AUTN,HXRES*)发送至SEAF。SEAF通过非接入层(Non Access Stratum,NAS)消息(如Auth-Req)向UE发送RAND和AUTN,该消息还包含被UE和AMF用于标识K_{AMF}(即ME和SEAF从K_{SEAF}派生的密钥)和部分原生安全上下文的ngKSI,该消息还包括体系结构之间的返竞标(Anti-Bidding down Between Architectures,ABBA)参数。

[0160] 可选地,该实施例中,所述根据所述封装的第一密钥获得鉴权信息之后,还包括:

[0161] 向所述终端发送所述鉴权信息中的随机数和第三认证令牌。

[0162] 这样,终端能够接收到该随机数和第三认证令牌执行后续鉴权。

[0163] 可选地,所述终端接收所述网络侧设备发送的随机数和第三认证令牌之后,根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌。

[0164] 可选地,所述根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌,包括:

[0165] 基于所述第一密钥和所述随机数,得到第二信息;

[0166] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0167] 使用所述第五密钥对所述第三认证令牌进行解密,得到所述第一认证令牌和第四

认证令牌;或者,基于所述第三认证令牌确定第三信息和第四认证令牌,并使用所述第五密钥对所述第三信息进行解密,得到所述第一认证令牌。

[0168] 其中,终端基于K_ME和RAND,可与上述网络侧设备同样采用第一加密算法生成AV_ME,如,终端的ME能够将本地保存的K_ME和接收到的RAND输入到第一加密算法(如MILENAGE-256算法),计算得到AV_ME。之后,基于AV_ME中的CK_ME和IK_ME得到AUTN_USIM_ENC_K。其中,可与上述网络侧设备通过同样的方式得到AUTN_USIM_ENC_K,即AUTN_USIM_ENC_K=f(CK_ME,IK_ME)。然后,针对第三认证令牌的不同生成方式(先串联后加密,或者,先加密后串联),逆处理得到AUTN_USIM和AUTN_ME。

[0169] 其中,若第三认证令牌的生成是先串联后加密,则逆处理为先解密后截取,使用AUTN_USIM_ENC_K解密AUTN_ENC,得到AUTN_USIM和第四认证令牌AUTN_ME的串联信息,由于已知认证令牌长度,即可截取出AUTN_USIM和AUTN_ME;若第三认证令牌的生成是先加密后串联,则逆处理为先截取后解密,由于已知认证令牌长度,截取出AUTN_ME和第三信息(加密的AUTN_USIM),使用AUTN_USIM_ENC_K解密该第三信息,得到AUTN_USIM。

[0170] 可选地,所述终端执行的步骤还包括:

[0171] 根据所述第二信息中的第二认证令牌验证所述第四认证令牌。

[0172] 也就是说,终端在通过上述先解密后截取的方式获得第四认证令牌之后,还可以基于K_ME和RAND,采用第一加密算法验证第四认证令牌的合法性。具体的,将K_ME、RAND输入到第一加密算法(如MILENAGE-256)之后,将计算所得AUTN_ME与第四认证令牌(先解密后截取所得到的AUTN_ME)进行一致性比较。

[0173] 需要说明的是,该实施例中,终端的ME执行上述步骤获得AUTN_USIM,将接收到的RAND和所得到的AUTN_USIM转发给USIM。

[0174] 可选地,所述根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌之后,还包括:

[0175] 根据所述第一认证令牌进行验证;

[0176] 在验证通过的情况下确定第一响应值;

[0177] 向所述网络侧设备发送所述第一响应值。

[0178] 这样,终端在基于接收的第三认证令牌得到AUTN_USIM后,会根据该AUTN_USIM进行验证,并且在验证通过的情况下确定第一响应值RES*,向网络侧设备发送RES*。

[0179] 其中,终端的USIM执行上述步骤,对AUTN_USIM进行验证,检查AUTN_USIM是否被接受。ME在验证通过的情况下确定第二响应值RES,并从RES计算RES*。

[0180] 可选地,所述在验证通过的情况下确定第一响应值,包括:

[0181] 根据第二加密算法和所述第二密钥得到第一信息;

[0182] 基于所述第一信息中的第一预期响应值和第二信息中的第二预期响应值,得到所述第一响应值。

[0183] 即,终端的USIM将K_USIM输入到第二加密算法,计算得到AV_USIM,之后,ME基于AV_USIM中的XRES_USIM以及AV_ME中的XRES_ME,先得到第二响应值RES。具体的,将XRES_USIM和XRES_ME串联之后,采用摘要函数对串联结果进行计算,得到RES,即RES=HASH(XRES_USIM||XRES_ME)。这样,ME可从RES计算RES*。USIM会将AV_USIM中的XRES_USIM、CK_USIM、IK_USIM发送给ME。

[0184] 可选地,所述终端执行的步骤还包括:

[0185] 基于第一信息中的第六密钥和第二信息中的第三密钥,得到第七密钥;

[0186] 基于所述第一信息中的第八密钥和所述第二信息中的第四密钥,得到第九密钥。

[0187] 因此,ME由USIM发送的CK_USIM和本地保存的CK_ME计算CK;由USIM发送的IK_USIM和本地保存的IK_ME计算IK。

[0188] 其中,终端确定第七密钥CK和第九密钥IK的方式是与上述网络侧设备相同,CK=HASH(CK_USIM||CK_ME);IK=HASH(IK_USIM||IK_ME)。

[0189] 可选地,ME可以从CK和IK推衍出K_{AUSF},从K_{AUSF}推衍出K_{SEAF}。

[0190] 该实施例中,终端向网络侧设备发送RES*,可以是终端在NAS消息认证响应中将RES*返回给SEAF。之后,SEAF从RES*计算HRES*,并比较HRES*和HXRES*。若两值一致,SEAF从服务网的角度认为认证成功;若不一致,SEAF认为认证失败,并向AUSF指示失败。SEAF通过Nausf_UEAuthentication_Authenticate Request消息向AUSF发送RES*,还会将来自UE的相应SUCI或SUPI通过Nausf_UEAuthentication_Authenticate Request消息发送给AUSF。当接收到包含RES*的Nausf_UEAuthentication_Authenticate Request消息时,AUSF可验证鉴权信息是否已到期。若鉴权信息已过期,AUSF可从归属网络的角度认为认证不成功。AUSF应将接收到的RES*与存储的XRES*进行比较,若RES*和XRES*一致,AUSF应从归属网络的角度认为认证成功。

[0191] AUSF通过Nausf_UEAuthentication_Authenticate Response向SEAF指示认证是否成功。若认证成功,则AUSF通过Nausf_UEAuthentication_Authenticate Response将K_{SEAF}发送至SEAF。若AUSF在启动认证时从SEAF接收到SUCI且认证成功,AUSF还应在Nausf_UEAuthentication_Authenticate Response中包含SUPI。

[0192] 若认证成功,SEAF应把从Nausf_UEAuthentication_Authenticate Response消息中接收到密钥K_{SEAF}作为锚密钥。然后SEAF应从K_{SEAF}、ABBA参数和SUPI推衍出K_{AMF},并向AMF提供ngKSI和K_{AMF}。如果SUCI用于此认证,SEAF应仅在接收到包含SUPI的Nausf_UEAuthentication_Authenticate Response消息后才向AMF提供ngKSI和K_{AMF};在服务网获知SUPI之前,不会向UE提供通信服务。

[0193] 下面,结合图2说明本发明实施例的方法在5G AKA的整体流程:

[0194] ME检查USIM是否为新卡,若否,获取USIM归属网的公钥PK_HN。ME随机生成256bit的K_ME,将K_ME加密封装为K_ME_ENC。通过初始化注册请求发送K_ME_ENC、SUCI给UDM/HSS。

[0195] UDM/HSS获得为K_ME_ENC之后,解密K_ME_ENC得到K_ME;基于128bit的K_USIM计算得到AV_USIM;通过RAND和K_ME计算得到AV_ME;计算AUTN_USIM_ENC_K;对AUTN_USIM进行加密保护,得到AUTN_ENC;构造5G HE AV。通过认证请求告知终端RAND和AUTN_ENC。

[0196] ME获得RAND和AUTN_ENC之后,通过K_ME和RAND计算CK_ME、IK_ME和XRES_ME;计算AUTN_USIM_ENC_K;通过AUTN_USIM_ENC_K从AUTN_ENC中解密得到AUTN_USIM。向USIM发送RAND和AUTN_USIM。

[0197] USIM获得RAND和AUTN_USIM之后,验证AUTN_USIM;计算XRES_USIM、CK_USIM、IK_USIM。向ME发送XRES_USIM、CK_USIM和IK_USIM。

[0198] ME通过接收到的XRES_USIM、CK_USIM和IK_USIM,以及本地保存的XRES_ME、CK_ME、IK_ME,计算RES*、CK、IK。终端向UDM/HSS发送认证响应,包括RES*。

[0199] 综上,在终端USIM不支持第一加密算法的场景,本发明实施例的方法可以基于提供的第一密钥完成鉴权,该第一密钥的长度大于USIM存储的密钥的长度,提升了系统的安全性;且,由于无需修改其他网元和相关接口,改动成本较低,与原协议兼容性较高。

[0200] 需要说明的是,该实施例中,判断USIM是否支持第一加密算法,若USIM支持第一加密算法,则终端可以直接加密封装第二密钥,将封装的第二密钥与SUCI发送给网络侧设备,网络侧设备与终端基于该第二密钥完成鉴权。

[0201] 还需要说明的是,本发明实施例的方法不仅适用于3G、4G和5G的AKA协议,也适用于对应的EAP-AKA,上述实施例中主要以5G AKA进行说明。

[0202] 如图3所示,本发明实施例的一种鉴权处理方法,由终端执行,包括:

[0203] 步骤31,判断通用用户身份模块USIM是否支持第一加密算法;

[0204] 步骤32,在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

[0205] 这样,网络侧设备能够通过获取终端发送的SUCI以及封装的第一密钥,在对SUCI进行解密得到SUPI之后,由SUPI确定所述终端的USIM是否支持第一加密算法,从而针对所述终端的USIM不支持第一加密算法的情况,由封装的第一密钥来获得鉴权信息。其中,由于第一密钥的长度大于USIM的密钥的长度,因此即使USIM不支持第一加密算法,所获得的鉴权信息也增强了抵御量子计算的能力,提升了鉴权过程的安全性。

[0206] 可选地,所述向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥之前,还包括:

[0207] 获取所述USIM对应的归属网的公钥;

[0208] 生成所述第一密钥,并使用所述公钥对所述第一密钥进行封装,得到所述封装的第一密钥。

[0209] 可选地,所述向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥之后,还包括:

[0210] 接收所述网络侧设备发送的随机数和第三认证令牌;

[0211] 根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌。

[0212] 可选地,所述根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌之后,还包括:

[0213] 根据所述第一认证令牌进行验证;

[0214] 在验证通过的情况下确定第一响应值;

[0215] 向所述网络侧设备发送所述第一响应值。

[0216] 可选地,所述根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌,包括:

[0217] 基于所述第一密钥和所述随机数,得到第二信息;

[0218] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0219] 使用所述第五密钥对所述第三认证令牌进行解密,得到所述第一认证令牌和第四认证令牌;或者,基于所述第三认证令牌确定第三信息和第四认证令牌,并使用所述第五密钥对所述第三信息进行解密,得到所述第一认证令牌。

[0220] 可选地,所述方法还包括:

[0221] 根据所述第二信息中的第二认证令牌验证所述第四认证令牌。

[0222] 可选地,所述在验证通过的情况下确定第一响应值,包括:

[0223] 根据第二加密算法和所述第二密钥得到第一信息;

[0224] 基于所述第一信息中的第一预期响应值和第二信息中的第二预期响应值,得到所述第一响应值。

[0225] 可选地,所述方法还包括:

[0226] 基于第一信息中的第六密钥和第二信息中的第三密钥,得到第七密钥;

[0227] 基于所述第一信息中的第八密钥和所述第二信息中的第四密钥,得到第九密钥。

[0228] 需要说明的是,该方法是与上述由网络侧设备执行的方法配合实现的,上述方法实施例的实现方式适用于该方法,也能达到相同的技术效果。

[0229] 如图4所示,本发明的实施例提供一种鉴权处理装置,包括:

[0230] 第一接收模块410,用于获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM的密钥;

[0231] 第一处理模块420,用于对所述SUCI进行解密得到用户永久标识符SUPI;

[0232] 第二处理模块430,用于在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

[0233] 该装置能够通过获取终端发送的SUCI以及封装的第一密钥,在对SUCI进行解密得到SUPI之后,由SUPI确定所述终端的USIM是否支持第一加密算法,从而针对所述终端的USIM不支持第一加密算法的情况,由封装的第一密钥来获得鉴权信息。其中,由于第一密钥的长度大于USIM的密钥的长度,因此即使USIM不支持第一加密算法,所获得的鉴权信息也增强了抵御量子计算的能力,提升了鉴权过程的安全性。

[0234] 可选地,所述第二处理模块还用于:

[0235] 对所述封装的第一密钥进行解封装,得到所述第一密钥,并将所述第一密钥和所述SUPI进行关联存储;

[0236] 根据所述第一密钥和所述第二密钥,得到所述鉴权信息。

[0237] 可选地,所述第二处理模块还用于:

[0238] 根据第二加密算法和所述第二密钥得到第一信息;

[0239] 根据所述第一加密算法、所述第一密钥和所述第一信息中的随机数,得到第二信息;

[0240] 根据所述第一信息和所述第二信息,得到鉴权相关信息;

[0241] 根据所述鉴权相关信息,得到所述鉴权信息。

[0242] 可选地,所述第二处理模块还用于:

[0243] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0244] 基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌;

[0245] 基于所述第一信息中的第一预期响应值以及所述第二信息中的第二预期响应值,得到第三预期响应值;

[0246] 基于所述第三密钥和所述第一信息中的第六密钥,得到第七密钥;

[0247] 基于所述第四密钥和所述第一信息中的第八密钥,得到第九密钥;

[0248] 将所述随机数、所述第三认证令牌、所述第三预期响应值、所述第七密钥和所述第九密钥作为所述鉴权相关信息。

[0249] 可选地,所述第二处理模块还用于:

[0250] 将所述第一认证令牌与所述第二认证令牌进行串联,并使用所述第五密钥对串联的结果进行加密,得到所述三认证令牌;或者,

[0251] 使用所述第五密钥对所述第一认证令牌进行加密,并将加密的结果与所述第二认证令牌进行串联,得到所述三认证令牌。

[0252] 可选地,所述第二处理模块还用于:

[0253] 基于所述第七密钥和所述第九密钥,得到第十密钥;

[0254] 基于所述第三预期响应值,得到第四预期响应值;

[0255] 将所述随机数、所述第三认证令牌、所述第四预期响应值和所述第九密钥作为所述鉴权信息。

[0256] 可选地,所述装置还包括:

[0257] 第二发送模块,用于向所述终端发送所述鉴权信息中的随机数和第三认证令牌。

[0258] 可选地,装置还包括:

[0259] 第二接收模块,用于接收所述终端发送的第一响应值;

[0260] 第四处理模块,用于根据所述第一响应值,确定认证是否成功。

[0261] 需要说明的是,该装置是应用了上述由网络侧设备执行的方法的装置,上述方法实施例的实现方式适用于该装置,也能达到相同的技术效果。

[0262] 如图5所示,本发明的实施例提供一种鉴权处理装置,包括:

[0263] 第三处理模块510,用于判断通用用户身份模块USIM是否支持第一加密算法;

[0264] 第一发送模块520,用于在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

[0265] 该装置使得网络侧设备能够通过获取终端发送的SUCI以及封装的第一密钥,在对SUCI进行解密得到SUPI之后,由SUPI确定所述终端的USIM是否支持第一加密算法,从而针对所述终端的USIM不支持第一加密算法的情况,由封装的第一密钥来获得鉴权信息。其中,由于第一密钥的长度大于USIM的密钥的长度,因此即使USIM不支持第一加密算法,所获得的鉴权信息也增强了抵御量子计算的能力,提升了鉴权过程的安全性。

[0266] 可选地,所述装置还包括:

[0267] 获取模块,用于获取所述USIM对应的归属网的公钥;

[0268] 第五处理模块,用于生成所述第一密钥,并使用所述公钥对所述第一密钥进行封装,得到所述封装的第一密钥。

[0269] 可选地,所述装置还包括:

[0270] 第三接收模块,用于接收所述网络侧设备发送的随机数和第三认证令牌;

[0271] 第六处理模块,用于根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌。

[0272] 可选地,所述装置还包括:

[0273] 第七处理模块,用于根据所述第一认证令牌进行验证;

[0274] 第八处理模块,用于在验证通过的情况下确定第一响应值;

[0275] 第三发送模块,用于向所述网络侧设备发送所述第一响应值。

[0276] 可选地,所述第六处理模块还用于:

[0277] 基于所述第一密钥和所述随机数,得到第二信息;

[0278] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0279] 使用所述第五密钥对所述第三认证令牌进行解密,得到所述第一认证令牌和第四认证令牌;或者,基于所述第三认证令牌确定第三信息和第四认证令牌,并使用所述第五密钥对所述第三信息进行解密,得到所述第一认证令牌。

[0280] 可选地,所述装置还包括:

[0281] 第九处理模块,用于根据所述第二信息中的第二认证令牌验证所述第四认证令牌。

[0282] 可选地,所述第八处理模块还用于:

[0283] 根据第二加密算法和所述第二密钥得到第一信息;

[0284] 基于所述第一信息中的第一预期响应值和第二信息中的第二预期响应值,得到所述第一响应值。

[0285] 可选地,所述装置还包括:

[0286] 第十处理模块,用于基于第一信息中的第六密钥和第二信息中的第三密钥,得到第七密钥;

[0287] 第十一处理模块,用于基于所述第一信息中的第八密钥和所述第二信息中的第四密钥,得到第九密钥。

[0288] 需要说明的是,该装置是应用了上述由终端执行的方法的装置,上述方法实施例的实现方式适用于该装置,也能达到相同的技术效果。

[0289] 如图6所示,本发明实施例的一种终端600,包括处理器610和收发器620,其中,

[0290] 所述处理器用于:判断通用用户身份模块USIM是否支持第一加密算法;

[0291] 所述收发器用于:在所述USIM不支持所述第一加密算法的情况下,向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为所述USIM存储的密钥。

[0292] 可选地,所述处理器还用于:

[0293] 获取所述USIM对应的归属网的公钥;

[0294] 生成所述第一密钥,并使用所述公钥对所述第一密钥进行封装,得到所述封装的第一密钥。

[0295] 可选地,所述收发器还用于接收所述网络侧设备发送的随机数和第三认证令牌;

[0296] 所述处理器还用于根据所述第一密钥、所述随机数和所述第三认证令牌,得到第一认证令牌。

[0297] 可选地,所述处理器还用于根据所述第一认证令牌进行验证;在验证通过的情况下确定第一响应值;

[0298] 所述收发器还用于向所述网络侧设备发送所述第一响应值。

[0299] 可选地,所述处理器还用于:

[0300] 基于所述第一密钥和所述随机数,得到第二信息;

[0301] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0302] 使用所述第五密钥对所述第三认证令牌进行解密,得到所述第一认证令牌和第四认证令牌;或者,基于所述第三认证令牌确定第三信息和第四认证令牌,并使用所述第五密钥对所述第三信息进行解密,得到所述第一认证令牌。

[0303] 可选地,所述处理器还用于:

[0304] 根据所述第二信息中的第二认证令牌验证所述第四认证令牌。

[0305] 可选地,所述处理器还用于:

[0306] 根据第二加密算法和所述第二密钥得到第一信息;

[0307] 基于所述第一信息中的第一预期响应值和第二信息中的第二预期响应值,得到所述第一响应值。

[0308] 可选地,所述处理器还用于:

[0309] 基于第一信息中的第六密钥和第二信息中的第三密钥,得到第七密钥;

[0310] 基于所述第一信息中的第八密钥和所述第二信息中的第四密钥,得到第九密钥。

[0311] 本发明另一实施例的一种移动终端,如图7所示,包括收发器710、处理器700、存储器720及存储在所述存储器720上并可在所述处理器700上运行的程序或指令;所述处理器700执行所述程序或指令时实现上述应用于终端的鉴权处理方法。

[0312] 所述收发器710,用于在处理器700的控制下接收和发送数据。

[0313] 其中,在图7中,总线架构可以包括任意数量的互联的总线和桥,具体由处理器700代表的一个或多个处理器和存储器720代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口提供接口。收发器710可以是多个元件,即包括发送机和接收机,提供用于在传输介质上与各种其他装置通信的单元。针对不同的用户设备,用户接口730还可以是能够外接内接需要设备的接口,连接的设备包括但不限于小键盘、显示器、扬声器、麦克风、操纵杆等。

[0314] 处理器700负责管理总线架构和通常的处理,存储器720可以存储处理器700在执行操作时所使用的数据。

[0315] 本发明实施例的一种网络侧设备,包括处理器和收发器,

[0316] 所述收发器用于:获取终端发送的用户隐藏标识符SUCI和封装的第一密钥;其中,所述第一密钥的长度大于第二密钥的长度,所述第二密钥为通用用户身份模块USIM的密钥;

[0317] 所述处理器用于:对所述SUCI进行解密得到用户永久标识符SUPI;

[0318] 所述处理器还用于:在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下,根据所述封装的第一密钥获得鉴权信息。

[0319] 可选地,所述处理器还用于:

[0320] 对所述封装的第一密钥进行解封装,得到所述第一密钥,并将所述第一密钥和所述SUPI进行关联存储;

[0321] 根据所述第一密钥和所述第二密钥,得到所述鉴权信息。

[0322] 可选地,所述处理器还用于:

[0323] 根据第二加密算法和所述第二密钥得到第一信息;

[0324] 根据所述第一加密算法、所述第一密钥和所述第一信息中的随机数,得到第二信息;

[0325] 根据所述第一信息和所述第二信息,得到鉴权相关信息;

[0326] 根据所述鉴权相关信息,得到所述鉴权信息。

[0327] 可选地,所述处理器还用于:

[0328] 基于所述第二信息中的第三密钥和第四密钥,得到第五密钥;

[0329] 基于所述第五密钥、所述第一信息中的第一认证令牌、所述第二信息中的第二认证令牌,得到第三认证令牌;

[0330] 基于所述第一信息中的第一预期响应值以及所述第二信息中的第二预期响应值,得到第三预期响应值;

[0331] 基于所述第三密钥和所述第一信息中的第六密钥,得到第七密钥;

[0332] 基于所述第四密钥和所述第一信息中的第八密钥,得到第九密钥;

[0333] 将所述随机数、所述第三认证令牌、所述第三预期响应值、所述第七密钥和所述第九密钥作为所述鉴权相关信息。

[0334] 可选地,所述处理器还用于:

[0335] 将所述第一认证令牌与所述第二认证令牌进行串联,并使用所述第五密钥对串联的结果进行加密,得到所述三认证令牌;或者,

[0336] 使用所述第五密钥对所述第一认证令牌进行加密,并将加密的结果与所述第二认证令牌进行串联,得到所述三认证令牌。

[0337] 可选地,所述处理器还用于:

[0338] 基于所述第七密钥和所述第九密钥,得到第十密钥;

[0339] 基于所述第三预期响应值,得到第四预期响应值;

[0340] 将所述随机数、所述第三认证令牌、所述第四预期响应值和所述第九密钥作为所述鉴权信息。

[0341] 可选地,所述收发器用于:

[0342] 向所述终端发送所述鉴权信息中的随机数和第三认证令牌。

[0343] 可选地,所述收发器用于接收所述终端发送的第一响应值;

[0344] 所述处理器还用于根据所述第一响应值,确定认证是否成功。

[0345] 本发明另一实施例的网络侧设备,如图8所示,包括收发器810、处理器800、存储器820及存储在所述存储器820上并可在所述处理器800上运行的程序或指令;所述处理器800执行所述程序或指令时实现上述应用于网络侧设备的鉴权处理方法。

[0346] 所述收发器810,用于在处理器800的控制下接收和发送数据。

[0347] 其中,在图8中,总线架构可以包括任意数量的互联的总线和桥,具体由处理器800代表的一个或多个处理器和存储器820代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口提供接口。收发器810可以是多个元件,即包括发送机和接收机,提供用于在传输介质上与各种其他装置通信的单

元。处理器800负责管理总线架构和通常的处理,存储器820可以存储处理器800在执行操作时所使用的数据。

[0348] 本发明实施例的一种可读存储介质,其上存储有程序或指令,所述程序或指令被处理器执行时实现如上所述的鉴权处理方法中的步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0349] 其中,所述处理器为上述实施例中所述的终端或网络侧设备中的处理器。所述可读存储介质,包括计算机可读存储介质,如计算机只读存储器(Read-Only Memory,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等。

[0350] 本申请实施例还提供一种计算机程序产品,包括计算机指令,该计算机指令被处理器执行时实现上述图1或图3所示方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0351] 进一步需要说明的是,此说明书中所描述的终端包括但不限于智能手机、平板电脑等,且所描述的许多功能部件都被称为模块,以便更加特别地强调其实现方式的独立性。

[0352] 本发明实施例中,模块可以用软件实现,以便由各种类型的处理器执行。举例来说,一个标识的可执行代码模块可以包括计算机指令的一个或多个物理或者逻辑块,举例来说,其可以被构建为对象、过程或函数。尽管如此,所标识模块的可执行代码无需物理地位于一起,而是可以包括存储在不同位里上的不同的指令,当这些指令逻辑上结合在一起时,其构成模块并且实现该模块的规定目的。

[0353] 实际上,可执行代码模块可以是单条指令或者是许多条指令,并且甚至可以分布在多个不同的代码段上,分布在不同程序当中,以及跨越多个存储器设备分布。同样地,操作数据可以在模块内被识别,并且可以依照任何适当的形式实现并且被组织在任何适当类型的数据结构内。所述操作数据可以作为单个数据集被收集,或者可以分布在不同位置上(包括在不同存储设备上),并且至少部分地可以仅作为电子信号存在于系统或网络上。

[0354] 在模块可以利用软件实现时,考虑到现有硬件工艺的水平,所以可以以软件实现的模块,在不考虑成本的情况下,本领域技术人员都可以搭建对应的硬件电路来实现对应的功能,所述硬件电路包括常规的超大规模集成(VLSI)电路或者门阵列以及诸如逻辑芯片、晶体管之类的现有半导体或者是其它分立的元件。模块还可以用可编程硬件设备,诸如现场可编程门阵列、可编程阵列逻辑、可编程逻辑设备等实现。

[0355] 上述范例性实施例是参考该些附图来描述的,许多不同的形式和实施例是可行而不偏离本发明精神及教示,因此,本发明不应被建构成为在此所提出范例性实施例的限制。更确切地说,这些范例性实施例被提供以使得本发明会是完善又完整,且会将本发明范围传达给那些熟知此项技术的人士。在该些图式中,组件尺寸及相对尺寸也许基于清晰起见而被夸大。在此所使用的术语只是基于描述特定范例性实施例目的,并无意成为限制用。如在此所使用地,除非该内文清楚地另有所指,否则该单数形式“一”、“一个”和“该”是意欲将该些多个形式也纳入。会进一步了解到该些术语“包含”及/或“包括”在使用于本说明书时,表示所述特征、整数、步骤、操作、构件及/或组件的存在,但不排除一或更多其它特征、整数、步骤、操作、构件、组件及/或其族群的存在或增加。除非另有所示,陈述时,一值范围包含该范围的上下限及其间的任何子范围。

[0356] 以上所述是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员

来说,在不脱离本发明所述原理的前提下,还可以作出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

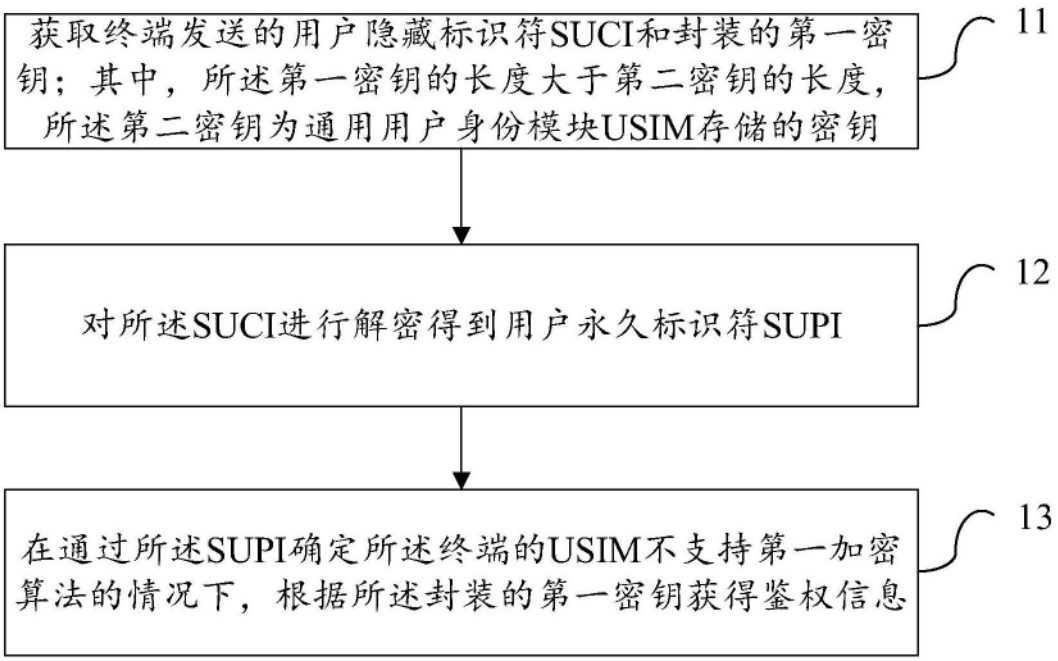

获取终端发送的用户隐藏标识符SUCI和封装的第一密钥；其中，所述第一密钥的长度大于第二密钥的长度，所述第二密钥为通用用户身份模块USIM存储的密钥
11
对所述SUCI进行解密得到用户永久标识符SUPI
12
在通过所述SUPI确定所述终端的USIM不支持第一加密算法的情况下，根据所述封装的第一密钥获得鉴权信息
13

图1


终端
USIM
ME
UDM/HSS
检查USIM是否为新卡;
若否，获取USIM归属网的公钥PK_HN;
随机生成256bit的K_ME，将K_ME加密封装为K_ME_ENC
初始化注册请求
解密K_ME_ENC得到K_ME;
基于128bit的K_USIM计算得到AV_USIM;
通过RAND和K_ME计算得到AV_ME；计算AUTN_USIM_ENC_K;
对AUTN_USIM进行加密保护，得到AUTN_ENC;
构造5G HE AV
认证请求
通过K_ME和RAND计算CK_ME、IK_ME和XRES_ME;
计算AUTN_USIM_ENC_K;
通过AUTN_USIM_ENC_K从AUTN_ENC中解密得到AUTN_USIM
RAND和AUTN_USIM
验证AUTN_USIM;
计算XRES_USIM、CK_USIM、IK_USIM
XRES_USIM、CK_USIM和IK_USIM
计算RES*、CK、IK
认证响应

图2

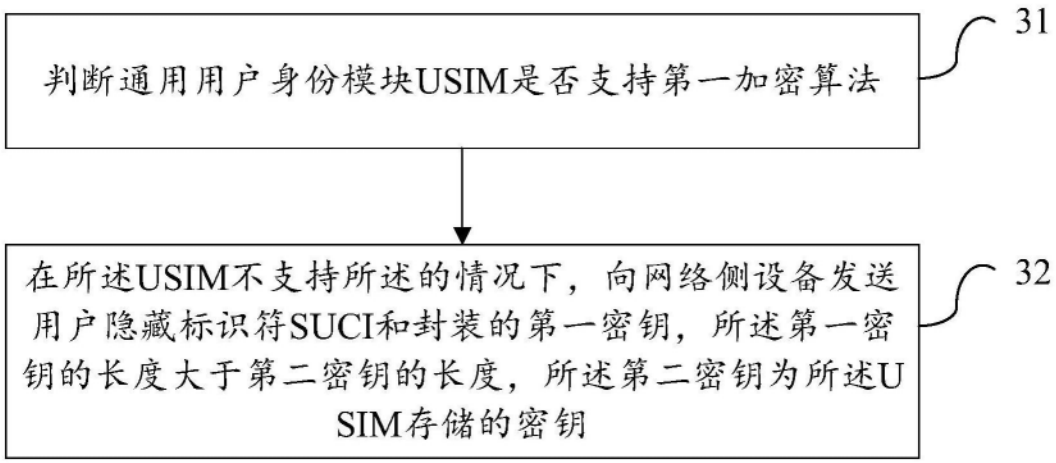

判断通用用户身份模块USIM是否支持第一加密算法
31
在所述USIM不支持所述的情况下，向网络侧设备发送用户隐藏标识符SUCI和封装的第一密钥，所述第一密钥的长度大于第二密钥的长度，所述第二密钥为所述USIM存储的密钥
32

图3

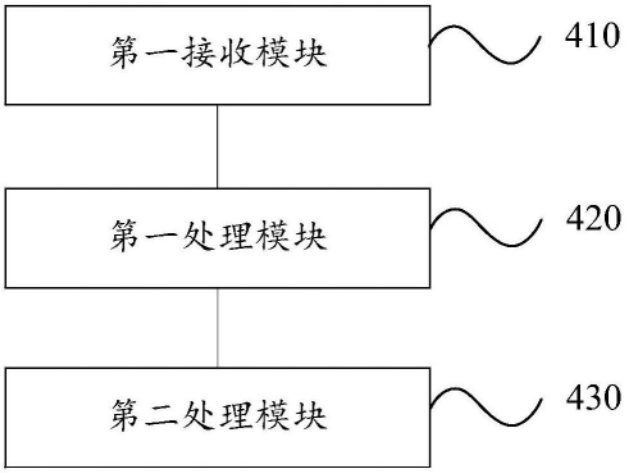

第一接收模块
410
第一处理模块
420
第二处理模块
430

图4

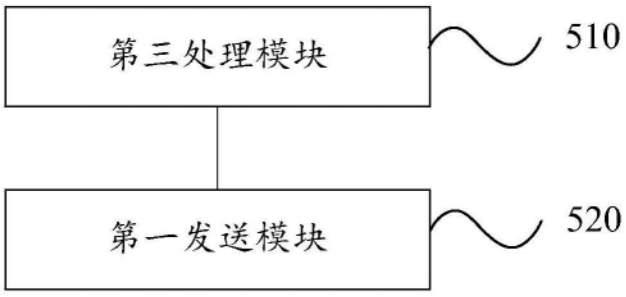

第三处理模块
510
第一发送模块
520

图5

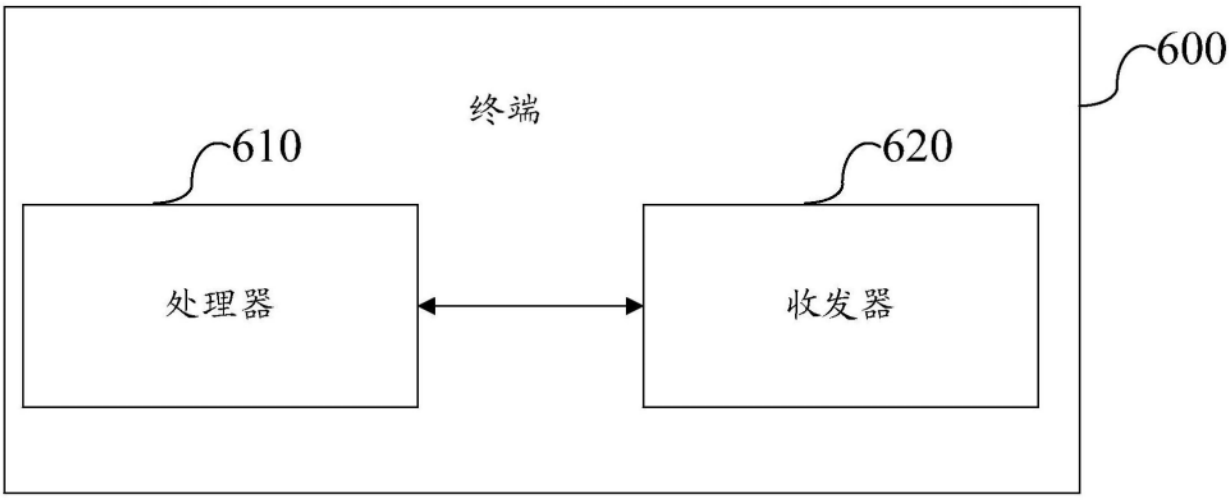

600
终端
610
620
处理器
收发器

图6

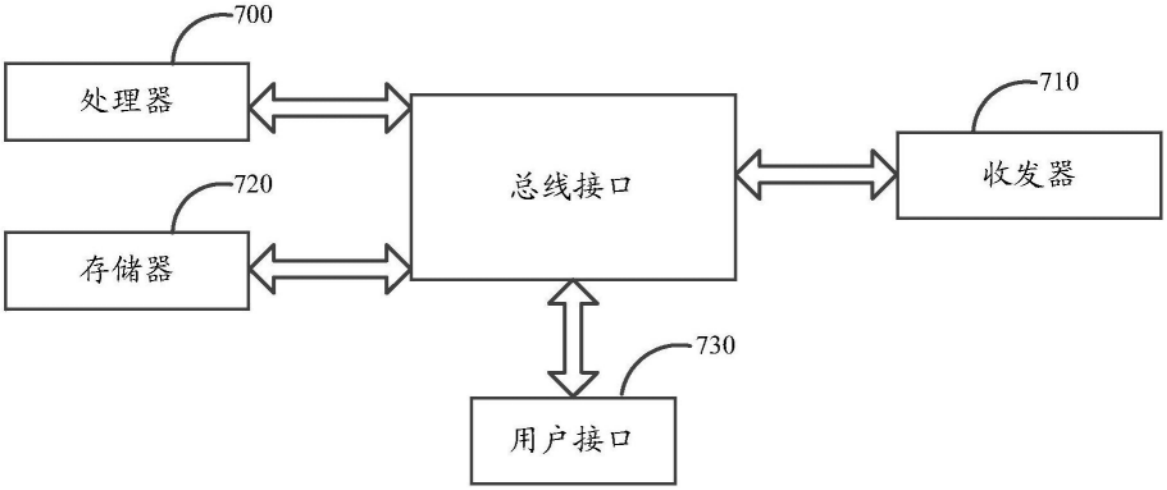

700
处理器
710
总线接口
收发器
720
存储器
730
用户接口

图7

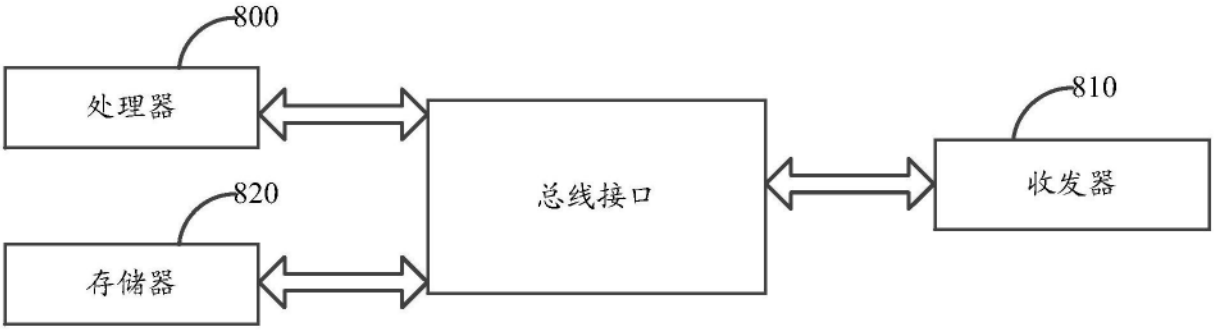

800
处理器
810
总线接口
收发器
820
存储器

图8