

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 5 月 9 日 (09.05.2019)



(10) 国际公布号
WO 2019/085659 A1

(51) 国际专利分类号:
H04W 60/00 (2009.01) *H04W 76/00* (2018.01)

(21) 国际申请号: PCT/CN2018/105504

(22) 国际申请日: 2018 年 9 月 13 日 (13.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711071266.5 2017 年 11 月 3 日 (03.11.2017) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 唐斌 (TANG, Bin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 于峰 (YU, Feng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 应江威 (YING, Jiangwei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 涂径玄 (TU, Jingxuan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京弘权知识产权代理事务所 (普通合伙) (CHINABLE IP); 中国北京市朝阳区安定路 35 号六层 35-10-2 内 620 室, Beijing 100029 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: INFORMATION INTERACTION METHOD AND DEVICE

(54) 发明名称: 一种信息交互方法及装置

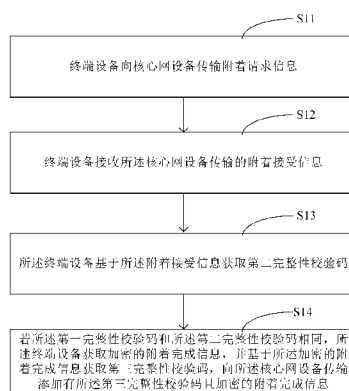


图 2

- S11 A TERMINAL DEVICE TRANSMITS ATTACHMENT REQUEST INFORMATION TO A CORE NETWORK DEVICE
S12 THE TERMINAL DEVICE RECEIVES ATTACHMENT ACCEPTANCE INFORMATION OF THE CORE NETWORK DEVICE
S13 THE TERMINAL DEVICE ACQUIRES A SECOND INTEGRITY CHECK CODE ON THE BASIS OF THE ATTACHMENT ACCEPTANCE INFORMATION
S14 IF THE FIRST INTEGRITY CHECK CODE AND THE SECOND INTEGRITY CHECK CODE ARE THE SAME, THE TERMINAL DEVICE ACQUIRES THE ENCRYPTED ATTACHMENT COMPLETION INFORMATION, AND ACQUIRES A THIRD INTEGRITY CHECK CODE ON THE BASIS OF THE ENCRYPTED ATTACHMENT COMPLETION INFORMATION, AND TRANSMITS THE ENCRYPTED ATTACHMENT COMPLETION INFORMATION WITH THE THIRD INTEGRITY CHECK CODE ADDED TO THE CORE NETWORK DEVICE

(57) Abstract: Disclosed in the present application are an information interaction method and device. The method comprises: the terminal device transmits attachment request information to a core network device, and receives attachment acceptance information of the core network device, wherein the attachment acceptance information comprises a first integrity check code; the terminal device acquires a second integrity check code on the basis of the attachment acceptance information; if the first integrity check code and the second integrity check code are the same, the terminal device acquires a third integrity check code on the basis of encrypted attachment

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

completion information, and transmits the encrypted attachment completion information with the third integrity check code added to the core network device. According to the solution disclosed in the embodiment of the present application, only the attachment request information, the attachment acceptance information, and the attachment completion information are transmitted between the terminal device and the core network device. Therefore, the process of data interaction is reduced, the amount of data of the interactive information is reduced, the time required for the information interaction process between the terminal device and the core network device is reduced, and the power consumption overhead of the terminal device can be reduced.

(57) 摘要: 本申请公开一种信息交互方法及装置。该方法中, 终端设备向核心网设备传输附着请求信息, 接收核心网设备的附着接受信息, 附着接受信息中包括第一完整性校验码; 终端设备基于附着接受信息获取第二完整性校验码; 若第一完整性校验码和第二完整性校验码相同, 终端设备基于加密的附着完成信息获取第三完整性校验码, 向核心网设备传输添加有第三完整性校验码且加密的附着完成信息。通过本申请实施例公开的方案, 终端设备与核心网设备之间只需传输附着请求信息、附着接受信息和附着完成信息, 减少数据交互的流程, 并减少交互的信息的数据量, 减少了终端设备与核心网设备进行信息交互过程的耗时, 并能够减少终端设备的功耗开销。

一种信息交互方法及装置

本申请要求在 2017 年 11 月 3 日提交中国专利局、申请号为 201711071266.5、发明名称为“一种信息交互方法及装置”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，尤其涉及一种信息交互方法及装置。

背景技术

目前一些通信系统中设置有终端设备和核心网设备，并且终端设备和核心网设备之间通常能够进行信息交互。例如，终端设备可将信息传输至无线接入网设备，再由无线接入网设备将该信息传输至核心网设备，实现终端设备与核心网设备的信息交互。

另外，为了保障通信系统的安全，终端设备与核心网设备之间在进行信息交互时，需要对对方进行身份认证，并对交互的信息进行数据保护。现有技术中，为了实现身份认证和数据保护，在终端设备首次接入核心网设备时，通常需要终端设备和核心网设备互相向对方传输自身的身份认证信息。这种情况下，终端设备会根据核心网设备的身份认证信息对核心网设备进行身份认证，以及核心网设备根据终端设备的身份认证信息对终端设备进行身份认证。在终端设备和核心网设备均通过身份认证后，核心网设备选择用于数据保护的完整性算法和加解密算法，并将选择的完整性算法和加解密算法传输至终端设备。终端设备确认是否支持核心网设备选择的完整性算法和加解密算法，并在确定支持后，终端设备向核心网设备发出相应的反馈。核心网设备在接收到反馈后，确认终端设备接入核心网设备。通过上述步骤，终端设备和核心网设备均对方身份进行认证，并且完成完整性算法和加密算法的协商。之后终端设备与核心网设备进行信息时，交互的信息均进行完整性保护和加密保护，从而提高了通信系统的安全性。

但是，发明人在本申请的研究过程中发现，现有技术虽然能够保障通信系统的安全，但终端设备与核心网设备之间进行多次信息交互才能完成身份认证，以及确定用于数据保护的完整性算法和加解密算法，信息交互次数较多，并且交互的信息数据量较大，导致现有技术中存在信息交互过程耗时长，以及终端设备功耗开销高的问题。

发明内容

现有技术中，为了保障通信系统的安全，需要终端设备与核心网设备之间进行多次信息交互，且交互的信息数据量较大，导致现有技术存在信息交互过程耗时长，以及终端设备功耗开销高的问题。为了解决现有技术中的问题，本申请实施例公开一种信息交互方法及装置。

在本申请的第一方面，公开一种信息交互方法，包括：终端设备向核心网设备传输附着请求信息；所述终端设备接收所述核心网设备传输的附着接受信息，所述附着接受信息中包括所述核心网设备的第一完整性校验码；所述终端设备基于所述附着接受信息获取第

二完整性校验码；若所述第一完整性校验码和所述第二完整性校验码相同，所述终端设备获取加密的附着完成信息，并基于所述加密的附着完成信息获取第三完整性校验码，向所述核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息。

通过该信息交互方法，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

结合第一方面，在第一方面第一种可能的实现方式中，所述终端设备基于所述附着接受信息获取第二完整性校验码，包括：所述终端设备基于预设的第一根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第一密钥生成算法生成第一终端密钥；所述终端设备基于所述第一终端密钥和所述附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码。

通过上述步骤，能够使终端获取第二完整性校验码，以便后续过程中，终端根据第二完整性校验码与第一完整性校验码是否相同，确定核心网身份的合法性。

结合第一方面，在第一方面第二种可能的实现方式中，所述终端设备获取加密的附着完成信息，包括：所述终端设备基于预设的第二根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第二密钥生成算法生成第二终端密钥；所述终端设备在生成附着完成信息后，基于所述第二终端密钥，通过预设的第一加解密算法对所述附着完成信息进行加密。

通过上述步骤，能够使终端对附着完成信息进行加密，以便后续过程中，核心网根据是否能够对接收到的附着完成信息进行解密，确定终端是否能够接入核心网。

结合第一方面第一种可能的实现方式，或结合第一方面第二种可能的实现方式，在第一方面第三种可能的实现方式中，所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。其中，终端设备身份标识能够区分不同终端设备，并且终端随机数不易被仿冒，从而提高终端设备参数的安全性。

结合第一方面第一种可能的实现方式，或结合第一方面第二种可能的实现方式，在第一方面第四种可能的实现方式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。其中，核心网设备身份标识能够区分不同核心网设备，并且核心网随机数不易被仿冒，从而提高核心网设备参数的安全性。

在本申请的第二方面，公开一种信息交互方法，包括：核心网设备接收终端设备传输的附着请求信息；所述核心网设备在生成附着接受信息后，基于所述附着接受信息，获取第一完整性校验码，并向所述终端设备传输添加有所述第一完整性校验码的附着接受信息；所述核心网设备接收所述终端设备传输的加密的附着完成信息，所述附着完成信息中包含所述终端设备的第三完整性校验码；所述核心网设备基于所述加密的附着完成信息，获取第四完整性校验码；若所述第三完整性校验码与所述第四完整性校验码相同，所述核心网设备对所述加密的附着完成信息进行解密，并在解密成功后，确定所述终端设备接入核心网设备。

通过该信息交互方法，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

结合第二方面，在第二方面第一种可能的实现方式中，所述基于所述附着接受信息，获取第一完整性校验码，包括：所述核心网设备基于预设的第三根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第三密钥生成算法生成第一核心网密钥；所述核心网设备基于所述第一核心网密钥和所述附着接受信息，通过预设的第二完整性算法，获取所述第一完整性校验码。

通过上述步骤，能够使核心网设备获取第一完整性校验码，以便后续过程中，终端设备根据第二完整性校验码与第一完整性校验码是否相同，确定核心网身份的合法性。

结合第二方面，在第二方面第二种可能的实现方式中，所述核心网设备对所述加密的附着完成信息进行解密，包括：所述核心网设备基于预设的第四根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第四密钥生成算法生成第二核心网密钥；所述核心网设备基于所述第二核心网密钥，通过预设的第二加解密算法对所述加密的附着完成信息进行解密。

通过上述步骤，核心网设备能够根据是否对接收到的附着完成信息解密成功，确定终端设备是否能够接入核心网设备。

结合第二方面第一种可能的实现方式，或结合第二方面第二种可能的实现方式，在第二方面第三种可能的实现方式中，所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。

其中，终端设备身份标识能够区分不同终端设备，并且终端随机数不易被仿冒，从而提高终端设备参数的安全性。

结合第二方面第一种可能的实现方式，或结合第二方面第二种可能的实现方式，在第二方面第四种可能的实现方式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。

其中，核心网设备身份标识能够区分不同核心网设备，并且核心网随机数不易被仿冒，从而提高核心网设备参数的安全性。

在本申请的第三方面，公开一种信息交互装置，包括：第一发送模块、第一接收模块和第一处理模块；所述第一发送模块用于向核心网设备传输附着请求信息；所述第一接收模块用于接收所述核心网设备传输的附着接受信息，所述附着接受信息中包括所述核心网设备的第一完整性校验码；所述第一处理模块用于基于所述附着接受信息获取第二完整性校验码，若所述第一完整性校验码和所述第二完整性校验码相同，所述第一处理模块用于获取加密的附着完成信息，并基于所述加密的附着完成信息获取第三完整性校验码，并触发所述第一发送模块向所述核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息。

通过该信息交互装置，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

结合第三方面，在第三方面第一种可能的实现方式中，所述第一处理模块具体用于基于预设的第一根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第一密钥生成算法生成第一终端密钥，并基于所述第一终端密钥和所述附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码。

结合第三方面，在第三方面第二种可能的实现方式中，所述第一处理模块具体用于基于预设的第二根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第二密钥生成算法生成第二终端密钥，并在生成附着完成信息后，基于所述第二终端密钥，通过预设的第一加解密算法对所述附着完成信息进行加密。

5 结合第三方面第一种可能的实现方式，或结合第三方面第二种可能的实现方式，在第三方面第三种可能的实现方式中，所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。其中，终端设备身份标识能够区分不同终端设备，并且终端随机数不易被仿冒，从而提高终端设备参数的安全性。

10 结合第三方面第一种可能的实现方式，或结合第三方面第二种可能的实现方式，在第三方面第四种可能的实现方式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。其中，核心网设备身份标识能够区分不同核心网设备，并且核心网随机数不易被仿冒，从而提高核心网设备参数的安全性。

在本申请的第四方面，公开一种信息交互装置，包括：第二接收模块、第二发送模块和第二处理模块，

15 所述第二接收模块用于接收终端设备传输的附着请求信息；所述第二处理模块用于在生成附着接受信息后，基于所述附着接受信息，获取第一完整性校验码，并触发所述第二发送模块向所述终端设备传输添加有所述第一完整性校验码的附着接受信息；所述第二接收模块还用于接收所述终端设备传输的加密的附着完成信息，所述附着完成信息中包含所述终端设备的第三完整性校验码；所述第二处理模块还用于基于所述加密的附着完成信息，
20 获取第四完整性校验码，若所述第三完整性校验码与所述第四完整性校验码相同，所述第二处理模块对所述加密的附着完成信息进行解密，并在解密成功后，确定所述终端设备接入核心网设备。

25 通过该信息交互装置，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

结合第四方面，在第四方面第一种可能的实现方式中，所述第二处理模块具体用于基于预设的第三根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第三密钥生成算法生成第一核心网密钥，并基于所述第一核心网密钥和所述附着接受信息，通过预设的第二完整性算法，获取所述第一完整性校验码。

30 结合第四方面，在第四方面第二种可能的实现方式中，所述第二处理模块具体用于基于预设的第四根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第四密钥生成算法生成第二核心网密钥，并基于所述第二核心网密钥，通过预设的第二加解密算法对所述加密的附着完成信息进行解密。

35 结合第四方面第一种可能的实现方式，或结合第四方面第二种可能的实现方式，在第四方面第三种可能的实现方式中，所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。其中，终端设备身份标识能够区分不同终端设备，并且终端随机数不易被仿冒，从而提高终端设备参数的安全性。

结合第四方面第一种可能的实现方式，或结合第四方面第二种可能的实现方式，在第四方面第四种可能的实现方式中，所述核心网设备参数包括：核心网设备身份标识和所述

核心网设备产生的核心网随机数。其中，核心网设备身份标识能够区分不同核心网设备，并且核心网随机数不易被仿冒，从而提高核心网设备参数的安全性。

在本申请的第五方面，公开一种终端设备，包括：收发端口、处理器和与所述处理器相连接的存储器；其中，所述收发端口用于和核心网设备之间进行信息的收发，并将从所述核心网设备接收的信息传输至处理器；所述存储器存储有可被所述处理器执行的指令；所述处理器用于获取所述收发端口传输的报文，并通过执行所述存储器中所存储的程序或指令，实现本申请的第一方面所述的信息交互方法。

在本申请的第六方面，公开一种核心网设备，包括：收发端口、处理器和与所述处理器相连接的存储器；其中，所述收发端口用于和终端设备之间进行信息的收发，并将从所述终端设备接收的信息传输至处理器；所述存储器存储有可被所述处理器执行的指令；所述处理器用于获取所述收发端口传输的报文，并通过执行所述存储器中所存储的程序或指令，实现本申请的第二方面所述的信息交互方法。

在本申请的第七方面，本申请实施例还提供了一种计算机程序产品，包括指令，当指令在计算机上运行时，使得计算机执行本申请第一方面的方法。

在本申请的第八方面，本申请实施例还提供了一种计算机程序产品，包括指令，当指令在计算机上运行时，使得计算机执行本申请第二方面的方法。

在本申请的第九方面，本申请实施例还提供了一种计算机存储介质，该计算机存储介质可存储有程序，该程序执行时可实现第一方面提供的信息交互方法的各实施例中的部分或全部步骤。

在本申请的第十方面，本申请实施例还提供了一种计算机存储介质，该计算机存储介质可存储有程序，该程序执行时可实现第二方面提供的信息交互方法的各实施例中的部分或全部步骤。

在本申请的第十一方面，本申请实施例还提供了一种芯片，所述芯片装置包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时，实现本申请第一方面所述的方法。

在本申请的第十二方面，本申请实施例还提供了一种芯片，所述芯片装置包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时，实现本申请第二方面所述的方法。

在本申请的第十三方面，本申请实施例还提供了一种终端设备，包括：处理器和存储器；所述存储器用于存储计算机执行指令，当所述终端设备运行时，所述处理器执行所述存储器存储的该计算机执行指令，以使所述终端设备执行如前述第一方面或第一方面各实现方式所述的信息交互方法。

在本申请的第十四方面，本申请实施例还提供了一种核心网设备，包括：处理器和存储器；所述存储器用于存储计算机执行指令，当所述核心网设备运行时，所述处理器执行所述存储器存储的该计算机执行指令，以使所述核心网设备执行如前述第二方面或第二方面各实现方式所述的信息交互方法。

通过本申请实施例公开的方案，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。与现有技术相比，本申请实施例公开的方案，在保障了通信系统的

安全性的前提下，减少数据交互的流程，并且减少终端设备与核心网设备之间交互的信息的数据量，从而减少了终端设备与核心网设备进行信息交互过程的耗时，并能够减少终端设备的功耗开销。

附图说明

- 5 图 1 为现有技术公开的一种通信系统的结构示意图；
图 2 为本申请实施例公开的一种信息交互方法的工作流程示意图；
图 3 为现有技术公开的一种通信系统中信息交互流程示意图；
图 4 为本申请实施例公开的一种通信系统中信息交互流程示意图；
图 5 为本申请实施例公开的一种应用于通信系统中的完整性算法的示意图；
10 图 6 为本申请实施例公开的又一种信息交互方法的工作流程示意图；
图 7 为本申请实施例公开的一种信息交互装置的结构示意图；
图 8 为本申请实施例公开的又一种信息交互装置的结构示意图。

具体实施方式

- 15 为了保障通信系统的安全，现有技术需要终端设备与核心网设备之间进行多次信息交互，且交互的信息数据量较大，导致现有技术存在信息交互过程耗时长，以及终端设备功耗开销高的问题。为了解决现有技术中的问题，本申请实施例公开一种信息交互方法及装置。

- 图 1 是本申请的实施例应用的通信系统的架构示意图。如图 1 所示，该通信系统包括核心网设备 110、无线接入网设备 120 和至少一个终端设备（如图 1 中的终端设备 130 和终端设备 140）。终端设备通过无线的方式与无线接入网设备 120 相连，无线接入网设备 120 通过无线或有线方式与核心网设备 110 连接。核心网设备与无线接入网设备可以是独立的不同的物理设备，也可以是将核心网设备的功能与无线接入网设备的逻辑功能集成在同一个物理设备上，还可以是一个物理设备上集成了部分核心网设备的功能和部分的无线接入网设备的功能。终端设备可以是固定位置的，也可以是可移动的。图 1 只是示意图，
20 该通信系统中还可以包括其它网络设备，如还可以包括无线中继设备和无线回传设备，在图 1 中未画出。本申请的实施例对该通信系统中包括的核心网设备、无线接入网设备和终端设备的数量不做限定。

- 无线接入网设备是终端设备通过无线方式接入到该通信系统中的接入设备，可以是基站 NodeB、演进型基站 eNodeB、5G 移动通信系统中的基站、未来移动通信系统中的基站或
30 WiFi 系统、LTE-U 或其他免授权频谱无线系统中的接入节点等，本申请的实施例对无线接入网设备所采用的具体技术和具体设备形态不做限定。

- 终端设备也可以称为终端(Terminal)、用户设备(user equipment, UE)、移动台(mobile station, MS)、移动终端(mobile terminal, MT)等。终端设备可以是手机(mobile phone)、平板电脑(Pad)、带无线收发功能的电脑、虚拟现实(virtual reality, VR)终端设备、
35 增强现实(Augmented Reality, AR)终端设备、工业控制(industrial control)中的无线终端、无人驾驶(self-driving)中的无线终端、远程手术(remote medical surgery)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、智慧家庭(smart home)中的无

线终端、具有无线通信功能的智能电表、智能水表、环境感应器、设备标签、定位标签等等。

本申请实施例中，终端设备能够将信息传输至无线接入网设备，再由无线接入网设备将信息传输至核心网设备，并且，核心网设备还能够将信息传输至无线接入网设备，再由无线接入网设备将信息传输至终端设备。也就是说，终端设备与核心网设备之间能够通过无线接入网设备实现信息交互。

本申请实施例公开的方案能够应用于多种通信系统，具体的，可以应用于对终端设备功耗有限制的通信系统中，以通过本申请实施例公开的方案减少对终端设备的功耗。例如，可以应用于 4.5G 移动通信技术中的基于蜂窝网络的窄带物联网 (narrow band internet of things, NB-IoT) 中。这种情况下，终端设备、无线接入网设备和核心网设备即分别为 NB-IoT 系统中的终端设备、无线接入网设备和核心网设备，并根据本申请实施例公开的方案实现终端设备与核心网设备之间的信息交互。

当然本申请实施例还可以应用于其他具备终端设备和核心网设备，且终端设备与核心网设备之间能够进行信息交互的通信系统中，本申请实施例对此不做限定。

以下通过多个实施例对本申请公开的方案进行介绍。其中，在本申请公开的第一实施例中，公开一种信息交互方法，该方法应用于终端设备，该终端设备能够通过无线接入网设备与核心网设备之间进行信息交互。

参见图 2 所示的工作流程示意图，本申请第一实施例公开的所述信息交互方法包括以下步骤：

步骤 S11、终端设备向核心网设备传输附着请求信息。

该步骤中，终端设备将附着请求信息传输至无线接入网设备，再由无线接入网设备传输至核心网设备，以使核心网设备能够接收到所述附着请求信息。

另外，在该附着请求信息中，可以包括终端设备参数。其中，所述终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。所述终端设备身份标识能够对不同的终端设备起到区分作用，例如可以为终端设备国际移动用户标志 (international mobile subscriber identity, IMSI)。

步骤 S12、所述终端设备接收所述核心网设备传输的附着接受信息，所述附着接受信息中包括所述核心网设备的第一完整性校验码。

其中，所述核心网设备接收到所述附着请求信息后，生成附着接受信息，并对所述附着接受信息进行计算，获取第一完整性校验码，将所述第一完整性校验码添加至附着接受信息中，再将添加有第一完整性校验码的附着接受信息传输至无线接入网设备。无线接入网设备会将添加有第一完整性校验码的附着接受信息传输至终端设备，从而使终端设备获取到所述附着接受信息。

步骤 S13、所述终端设备基于所述附着接受信息获取第二完整性校验码。

该步骤中，终端设备通过对附着接受信息进行计算，获取第二完整性校验码。其中，终端设备在对附着接受信息进行计算时，通常根据预先设定的第一完整性算法进行计算。

另外，核心网设备通过预先设定的第二完整性算法对附着接受信息进行计算，获取第一完整性校验码，这种情况下，若允许终端设备接入核心网设备，则预先设定第一完整性算法与第二完整性算法相同。也就是说，终端设备与核心网设备采用相同的完整性算法进

行完整性验证。

步骤 S14、若所述第一完整性校验码和所述第二完整性校验码相同，所述终端设备获取加密的附着完成信息，并基于所述加密的附着完成信息获取第三完整性校验码，向所述核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息。

5 该步骤中，若所述第一完整性校验码和第二完整性校验码相同，则终端设备确定核心网设备的身份合法。也就是说，在本申请实施例中，终端设备通过完整性校验码对核心网设备进行身份认证。

10 在确定核心网设备的身份合法（即第一完整性校验码和第二完整性校验码相同）后，所述终端设备会生成附着完成信息，再对所述附着完成信息进行加密，从而获取加密的附着完成信息。然后，终端设备使用第一完整性算法对加密的附着完成信息进行计算，获取第三完整性校验码，再将所述第三完整性校验码添加至所述加密的附着完成信息中。

15 这种情况下，核心网设备在接收到附着完成信息后，能够根据第二完整性算法对附着完成信息进行计算，获取第四完整性校验码。并且，核心网设备若确定第三完整性校验码与第四完整性校验码相同，则可确定终端设备的身份合法。也就是说，核心网设备通过所述附着完成信息中包含的第三完整性校验码实现对终端设备的身份认证。其中，第一完整性算法与第二完整性算法相同。

20 另外，终端设备对附着完成信息进行了加密处理，以提高附着完成信息的安全性。并且，终端设备通常采用预设的第一加解密方法对附着完成信息进行加密，而核心网设备接收到附着完成信息后，采用预设的第二加解密方法对附着完成信息进行解密。若终端设备允许接入核心网设备，则预先设定第一加解密方法与第二加解密方法相同。这种情况下，在根据完整性校验码确定终端设备的身份合法后，若核心网设备能够根据第二加解密方法对附着完成信息进行解密，说明终端设备与核心网设备之间交互的信息能够互相进行加解密，则确定终端设备接入核心网设备。

25 进一步的，终端设备在接入核心网设备之后，终端设备与核心网设备之间能够继续进行信息交互，例如，终端设备将获取到的检测数据通过无线接入网设备传输至核心网设备，核心网设备向通过无线接入网设备向终端设备传输指令信息等。这种情况下，每次信息交互时，信息的发送端可在交互的信息中添加根据该信息计算得到的完整性校验码，以及对该信息进行加密。接收到该信息的接收端对该信息进行计算，获取相应的完整性校验，若计算获取的完整性校验码与该信息中添加的完整性校验码相同，则接收端可确定接收到的信息完整，并在确定接收到的信息完整之后，可根据预设的加解密算法进行解密，从而提高了通信系统的安全性。

30 本申请实施例公开一种信息交互方法，该方法中，终端设备向核心网设备传输附着请求信息；核心网设备接收到附着请求信息后，生成附着接受信息，基于该附着接受信息获取第一完整性校验码，并将该第一完整性校验码添加至附着接受信息中；终端设备接收所述核心网设备传输的附着接受信息，并基于所述附着接受信息获取第二完整性校验码；若所述第一完整性校验码和所述第二完整性校验码相同，终端设备确定核心网设备的身份合法，也就是说，终端设备通过附着接受信息中包含的第一完整性校验码实现对核心网的身份认证，并在确认核心网设备的身份合法后，终端设备生成附着完成信息并对所述附着完成信息进行加密，然后基于加密的附着完成信息获取第三完整性校验码，将所述第三完整

性校验码添加至加密的附着完成信息中，再向核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息；核心网设备接收到附着完成信息后，基于该附着完成信息获取第四完整性校验码，若第三完整性校验码与第四完整性校验码相同，核心网设备确定终端设备的身份合法，也就是说，核心网设备通过附着完成信息中包含的第四完整性校验码实现5 对终端设备的身份认证，然后，核心网设备对附着完成信息进行解密，若解密成功，则确定终端设备接入核心网设备。

通过本申请实施例公开的信息交互方法，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

10 与现有技术相比，本申请实施例公开的方案，在保障通信系统安全性的前提下，减少数据交互的流程，并且减少终端设备与核心网设备之间交互的信息的数据量，从而减少了终端设备与核心网设备进行信息交互的耗时，以及减少终端设备的功耗开销。

进一步的，为了明确本申请实施例公开的方案的优势，以下对现有技术中通常采用的信息交互方法进行介绍。参见图 3 所示的现有技术的信息交互流程示意图，在现有技术中，15 终端设备首次接入核心网设备时，通常包括以下信息交互的流程：

步骤 1：终端设备产生携带有终端 IMSI 的附着请求信息，并通过无线接入网设备将该附着请求信息传输至核心网设备。

步骤 2：核心网设备在接收到终端设备发出的附着请求信息之后，获取其中包含的 IMSI，再通过无线接入网设备向该终端设备发送用户身份验证请求信息，所述用户身份验证请求20 信息中包括核心网认证码及核心网设备产生的核心网随机数。

步骤 3：终端设备在接收到核心网设备发出的用户身份验证请求信息后，根据其中包括的核心网认证码对核心网进行身份认证，若确定核心网设备的身份合法，终端设备通过预先设置的根密钥、终端设备自身产生的终端随机数及核心网随机数，生成用于对后续信息进行加密的密钥。然后，终端设备生成用户身份验证响应信息，并通过无线接入网设备25 向核心网设备传输所述用户身份验证响应信息，所述用户身份验证响应信息中包括终端认证码和终端随机数。也就是说，通过该步骤，终端设备能够对核心网设备进行身份认证，以及生成用于加密的密钥。

步骤 4：核心网设备接收到终端设备发出的用户身份验证响应信息后，根据其中包括的终端认证码对终端设备进行身份认证。若确定终端设备的身份合法，核心网设备通过预30 置的根密钥、终端随机数和核心网随机数，生成用于对后续信息进行加密的密钥。其中，若允许终端设备接入核心网设备，核心网中预置的根密钥与终端中预置的根密钥相同，核心网生成密钥的方式与终端生成密钥的方式相同，这种情况下，核心网设备生成的密钥与终端设备生成的密钥相同。生成密钥后，核心网设备选择完整性算法和加密算法，并生成安全模式命令信息，所述安全模式命令信息中包括核心网设备选择的完整性算法和加密算35 法，并在使用完整性算法对该安全模式命令信息进行完整性保护后，通过无线接入网设备将其传输至终端。也就是说，通过该步骤，核心网设备能够对终端进行身份认证，以及生成用于加密的密钥。

步骤 5：终端设备接收到核心网设备传输的安全模式命令信息后，确认自身是否支持核心网设备选择的完整性算法和加密算法。若支持，终端设备对所述安全模式命令信息进

行完整性验证，若该信息通过完整性验证，则终端设备通过无线接入网设备向核心网设备传输经过完整性保护和加密的安全模式完成信息。

步骤 6：核心网设备接收到终端设备传输的安全模式完成信息后，首先对该信息进行完整性验证，若该信息通过完整性验证，再解密该信息。然后，核心网设备产生附着接受信息，并通过无线接入网设备将所述附着接受信息传输至终端设备。

步骤 7：终端设备接收到核心网设备传输的附着接受信息后，确认自身是否能够接入核心网设备，若是，则通过无线接入网设备向核心网设备发送经过完整性保护和加密处理后的附着完成信息。核心网设备接收到终端传输的附着完成信息后，对附着完成信息进行完整性验证和解密，若该附着完成信息能够通过完整性验证及解密，则允许终端设备接入核心网设备，完成终端设备接入核心网设备的流程。

通过上述步骤，终端设备和核心网设备均对对方进行了身份认证，并且，完成完整性算法和加密算法的协商，之后终端设备与核心网设备之间再进行信息交互时，交互的信息都将做完整性保护和加密保护，从而提高通信系统的安全性。

但是，根据对上述步骤的描述以及图 3 所示的信息交互流程图可知，通过现有技术虽然能够保障通信系统的安全，但终端设备与核心网设备之间至少需要进行七次信息交互，信息交互的次数较多，且交互的信息数据量较大，导致现有技术中存在信息交互耗时长，以及终端设备功耗开销高的问题。

而采用本申请实施例公开的方案时，参见图 4 所示的信息交互流程示意图，终端设备与核心网设备进行信息交互时，首先由终端设备向核心网设备传输附着请求信息。接收到附着请求信息的核心网设备生成附着接受信息，并基于所述附着接受信息获取第一完整性校验码，将第一完整性校验码添加至附着接受信息后，向终端设备传输该附着接受信息。终端设备接收到附着接受信息后，基于所述附着接受信息，获取第二完整性校验码，在第一完整性校验码和第二完整性校验码相同的情况下，生成附着完成信息并加密。然后，终端设备基于加密的附着完成信息获取第三完整性校验码，并在加密的附着完成信息中添加第三完整性校验码，将添加有第三完整性校验码且加密的附着完成信息传输至核心网设备，以便核心网设备根据接收到的附着完成信息确定是否允许终端设备接入核心网设备。

根据图 4 可知，本申请实施例公开的方案中，只需要在终端设备与核心网设备之间传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需终端设备与核心网设备之间进行三次信息交互即可。与现有技术相比，减少了信息交互的次数，并且减少交互信息的数据量，从而减少了终端设备与核心网设备进行信息交互的耗时，且有效的减少了终端设备的功耗开销。

进一步的，在步骤 S13 中，公开了所述终端设备基于所述附着接受信息获取第二完整性校验码的操作，该操作通常包括以下步骤：

首先，所述终端设备基于预设的第一根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第一密钥生成算法生成第一终端密钥。

然后，所述终端设备基于所述第一终端密钥和所述附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码。

在本申请实施例中，在终端设备中预先设置第一根密钥，并且在附着接受信息中包含

核心网设备参数。接收到附着接受信息后，终端设备根据第一根密钥、终端设备参数及附着接受信息中包含的核心网设备参数，以及第一密钥生成算法生成第一终端密钥，所述第一终端密钥用于生成完整性校验码。

另外，在核心网设备中预先设置有第三根密钥，并且在接收到终端设备传输的附着请求信息后，核心网设备能够根据第三根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第三密钥生成算法生成第一核心网密钥，所述第一核心网密钥用于生成完整性校验码。

这种情况下，若终端设备允许接入核心网设备，则根据预先的设置，第一根密钥与第三根密钥相同，第一密钥生成算法与第二密钥生成算法相同，并且，由于计算第一终端密钥与计算第一核心网密钥的过程中，均依据终端设备参数及核心网设备参数，因此，计算得到的第一终端密钥与第一核心网密钥相同。

进一步的，在终端设备中预先设置第一完整性算法，通过第一完整性算法和第一终端密钥对附着接受信息进行计算，能够得到第二完整性校验码。在核心网设备中预先设置第二完整性算法，通过第二完整性算法和第一核心网密钥对附着接受信息进行计算，能够得到第一完整性校验码。若终端设备允许接入核心网设备，则预先设置第一完整性算法与第二完整性算法相同。

由于第一终端密钥与第一核心网密钥相同，第一完整性算法与第二完整性算法相同，并且，计算第一完整性校验码与计算第二完整性校验码的过程中，均对附着接受信息进行计算，因此，在核心网设备身份合法的情况下，第一完整性校验码与第二完整性校验码相同。这种情况下，终端设备通过比较第一完整性校验码与第二完整性校验码是否相同，即可判定核心网设备的身份是否合法。

另外，本申请实施例中，终端设备根据第一根密钥、终端设备参数及核心网设备参数生成第一终端密钥。其中，终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。所述终端设备身份标识能够对不同的终端设备起到区分作用，因此不同终端设备的终端设备身份标识不同，不同终端设备生成的第一终端密钥不同，从而能够区分不同终端设备生成的第一终端密钥。

所述终端设备身份标识可以采用终端设备国际移动用户标志（international mobile subscriber identity, IMSI），当然，还可以采用其他能够区分不同终端设备的参数作为终端设备身份标识，本申请实施例对此不做限定。

另外，终端随机数为终端设备随机生成的一个数据，将终端随机数作为终端设备参数，能够保障终端设备参数不易被仿冒，从而提高终端设备参数的安全性，进一步提高获取第一终端密钥的安全性。

其中，核心网设备参数可包括多种形式，在其中一种形式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。所述核心网设备身份标识用于对不同的核心网设备起到区分作用，因此终端设备在与不同的核心网设备进行信息交互时，核心网设备参数中的核心网设备身份标识不同，导致终端设备生成的第一终端密钥不同，从而能够区分终端设备与不同核心网设备进行信息交互时生成的第一终端密钥。

在本申请实施例中，可预先为各个核心网设备分配一个不同的核心网标签，通过核心网标签区分各个核心网设备，这种情况下，可将该核心网标签作为核心网设备身份标识。

当然，还可以采用其他能够区分不同核心网设备的参数作为核心网设备身份标识，本申请实施例对此不做限定。

另外，核心网随机数为核心网设备随机生成的一个数据，不易通过多次抓取数据被攻击，将核心网随机数作为核心网设备参数，能够保证核心网设备参数不易被仿冒，从而提高核心网设备参数的安全性，进一步提高获取第一终端密钥的安全性。

本申请实施例中，终端设备采用第一密钥生成算法生成第一终端密钥。其中，第一密钥生成算法可以为多种形式的密钥生成算法。例如，第一密钥生成算法可以为 HMAC-SHA-256 算法。其中，HMAC-SHA-256 算法包含以下公式：

$$\text{Derived Key} = \text{HMAC-SHA-256}(\text{RootKey}, S) \quad \text{公式 (1)};$$

$$S = \text{FC} \parallel \text{Algorithm Type Distinguisher} \parallel L0 \parallel \text{NET ID} \parallel L1 \parallel \text{NET Rand} \parallel L2 \parallel \text{IMSI} \parallel L3 \parallel \text{UE Rand} \parallel L4 \quad \text{公式 (2)}。$$

若在计算第一终端密钥时采用 HMAC-SHA-256 算法，则在公式 (1) 中，Derived Key 为第一终端密钥，RootKey 为终端设备中的第一根密钥，S 为密钥计算参数。该公式输出的字符长度通常为 256bit，在本申请实施例中，可以使用其中的低 128 位作为第一终端密钥。

另外，用于获取密钥计算参数 S 的公式 (2) 中，FC 为预设值，通常情况下，FC=0x015，当然，也可将 FC 设置为其他数值；Algorithm Type Distinguisher 为预设值，例如，在计算第一终端密钥时，可设置 Algorithm Type Distinguisher = 0x02；NET ID 是作为核心网设备身份标识的核心网标签；L0 为 Algorithm Type Distinguisher 的字节长度；L1 为 NET ID 的字节长度；NET Rand 为核心网随机数；L2 为核心网随机数 NET Rand 的字节长度；IMSI 是作为终端设备身份标识的终端设备国际移动用户标志；L3 为 IMSI 的字节长度；UE Rand 为终端随机数；L4 为终端随机数 UE Rand 的字节长度。

这种情况下，可通过公式 (2) 获取 S 的值，然后将 S 的值带入至公式 (1)，计算得到第一终端密钥。

当然，还可以采用其他形式的密钥生成算法，本申请实施例对此不作限定。

另外，终端设备基于第一终端密钥和附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码，该第一完整性算法可为多种形式，例如，第一完整性算法可采用 AES-128-CMAC，其算法示意图如图 5 所示。该算法中，根据信息计数、信息、信息方向、固定数值参数以及用于完整性保护的密钥，计算得到完整性校验码。其中，信息为计算完整性校验码时所应用的信息，在计算第二完整性校验码时，信息即为附着接受信息；另外，若应用的信息的信息方向为上行，则信息方向通常取值为 0，若应用的信息的信息方向为下行，则信息方向通常取值为 1；固定数值参数通常取值为 0。

当然，还可以采用其他的完整性算法，本申请实施例对此不作限定。

在本申请实施例的步骤 S14 中，公开终端设备获取加密的附着完成信息的操作。其中，所述终端设备获取加密的附着完成信息，包括以下步骤：

首先，所述终端设备基于预设的第二根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第二密钥生成算法生成第二终端密钥；然后，所述终端设备在生成附着完成信息后，基于所述第二终端密钥，通过预设的第一加解密算法对所述附着完成信息进行加密。

本申请实施例中，在终端设备中预先设置第二根密钥，并且在附着接受信息中包含核心网设备参数。接收到附着接受信息后，终端设备获取核心网设备参数，然后根据第二根密钥、终端设备参数及核心网设备参数，以及第二密钥生成算法生成第二终端密钥，所述第二终端密钥用于对交互的信息进行加密保护。

5 另外，在核心网设备中，预先设置第四根密钥，并且在接收到终端设备传输的附着请求信息后，核心网设备根据第四根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第四密钥生成算法生成第二核心网密钥，所述第二核心网密钥用于对交互的信息进行加密保护。

10 这种情况下，若允许终端设备接入核心网设备，则预先设置第二根密钥与第四根密钥相同，第二密钥生成算法与第四密钥生成算法相同，并且，由于计算第二终端密钥与计算第二核心网密钥的过程中，均依据终端设备参数及核心网设备参数，因此，第二终端密钥与第二核心网密钥相同。

15 进一步的，在终端设备中预先设置第一加解密算法，以便通过第一加解密算法对附着完成信息进行加密。在核心网设备中预先设置第二加解密算法，以便通过第二加解密算法对附着完成信息进行解密。其中，若允许终端设备接入核心网设备，则预先设置第一加解密算法与第二加解密算法相同，以便核心网设备能够对终端设备加密的信息进行解密。

20 另外，本申请实施例中，终端设备根据第二根密钥、终端设备参数及核心网设备参数生成第二终端密钥。其中，终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。所述终端设备身份标识能够对不同的终端设备起到区分作用，不同终端设备的终端设备身份标识不同，因此不同终端设备生成的第二终端密钥不同，从而能够区分不同终端设备生成的第二终端密钥。

所述终端设备身份标识可以采用终端设备国际移动用户标志（international mobile subscriber identity, IMSI），当然，还可以采用其他能够区分不同终端设备的参数作为终端设备身份标识，本申请实施例对此不做限定。

25 另外，终端随机数为终端设备随机生成的一个数据，将终端随机数作为终端设备参数，能够保障终端设备参数不易被仿冒，从而提高终端设备参数的安全性，进一步提高获取第二终端密钥的安全性。

30 其中，核心网设备参数可包括多种形式，在其中一种形式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。所述核心网设备身份标识用于对不同的核心网设备起到区分作用，因此终端设备在与不同的核心网设备进行信息交互时，核心网设备参数中的核心网设备身份标识不同，导致终端设备生成的第二终端密钥不同，从而能够区分终端设备与不同核心网设备进行信息交互时生成的第二终端密钥。

35 在本申请实施例中，可预先为各个核心网设备分配一个不同的核心网标签，通过核心网标签区分各个核心网设备，这种情况下，可将该核心网标签作为核心网设备身份标识。当然，还可以采用其他能够区分不同核心网设备的参数作为核心网设备身份标识，本申请实施例对此不做限定。

另外，核心网随机数为核心网设备随机生成的一个数据，不易通过多次抓取数据被攻击，将核心网随机数作为核心网设备参数，能够保证核心网设备参数不易被仿冒，从而提高核心网设备参数的安全性，进一步提高获取第二终端密钥的安全性。

终端设备采用第二密钥生成算法生成第二终端密钥。其中，第二密钥生成算法可采用多种形式的密钥生成算法，例如，第二密钥生成算法也可以为 HMAC-SHA-256 算法。也就是说，可以通过公式（1）与公式（2）计算第二终端密钥。

Derived Key 为第二终端密钥，RootKey 为终端设备中的第一根密钥，S 为密钥计算参数。该公式输出的字符长度通常为 256bit，在本申请实施例中，可以使用其中的低 128 位作为第二终端密钥。

另外，用于获取密钥计算参数 S 的公式（2）中，FC 为预设值，通常情况下，FC=0x015，当然，也可将 FC 设置为其他数值；Algorithm Type Distinguisher 为预设值，例如，在计算第二终端密钥时，可设置 Algorithm Type Distinguisher = 0x01；NET ID 是作为核心网设备身份标识的核心网标签；L0 为 Algorithm Type Distinguisher 的字节长度；L1 为 NET ID 的字节长度；NET Rand 为核心网随机数；L2 为核心网随机数 NET Rand 的字节长度；IMSI 是作为终端设备身份标识的终端设备国际移动用户标志；L3 为 IMSI 的字节长度；UE Rand 为终端随机数；L4 为终端随机数 UE Rand 的字节长度。

当然，还可以采用其他形式的密钥生成算法，本申请实施例对此不作限定。

进一步的，为了提高通信系统的安全性，预先设置在终端设备中的第一根密钥和第二根密钥可经过加密处理，当需要时，终端设备再对其进行解密，然后分别通过解密后的第一根密钥生成第一终端密钥，通过解密后的第二根密钥生成第二终端密钥。第一根密钥和第二根密钥的加解密方式可以相同，也可以不同，本申请实施例对此不做限定。

另外，第一根密钥和第二根密钥可为同一根密钥，即终端设备通过相同的根密钥生成第一终端密钥和第二终端密钥，或者第一根密钥和第二根密钥分别为不同的根密钥，本申请实施例对此不做限定。

在本申请实施例中，附着接受信息和附着完成信息中均包含完整性校验码，这种情况下，附着接受信息和附着完成信息的部分信息结构可如下表所示：

8	7	6	5	4	3	2	1	
Sec Hdr Type		Reserved						Oct 1
MAC								Oct 2
MAC								Oct 3
MAC								Oct 4
MAC								Oct 5
Sequence number								Oct 6

其中，“Sec Hdr Type”用于表示该条信息的安全类型，在本申请实施例中，若在“Sec Hdr Type”字段中设置有预设值（例如 11），则表示该条信息经过完整性保护，该条信息中设置有完整性校验码；“Reserved”为预留字段；“MAC”字段构成 32 位的完整性校验码；Sequence number 为信息计数。

相应的，本申请通过第二实施例公开一种信息交互方法，该方法应用于核心网设备，该核心网设备可通过无线接入网设备与终端设备之间进行信息交互，该终端设备能够执行本申请第一实施例公开的信息交互方法，因此，核心网设备在执行本申请第二实施例公开的信息交互方法时，终端设备所执行的操作可参见本申请第一实施例公开的内容。

参见图 6 所示的工作流程示意图，本申请实施例公开的所述信息交互方法包括：

步骤 S21、核心网设备接收终端设备传输的附着请求信息。

当终端设备需要接入核心网设备时，终端设备会产生附着请求信息，将附着请求信息传输至无线接入网设备，再由无线接入网设备传输至核心网设备，以使核心网设备能够接收到所述附着请求信息。

5 另外，在该附着请求信息中，可以包括终端设备参数。其中，所述终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。所述终端设备身份标识能够对不同的终端设备起到区分作用，可以为终端设备国际移动用户标志（international mobile subscriber identity, IMSI）。

10 步骤 S22、所述核心网设备在生成附着接受信息后，基于所述附着接受信息，获取第一完整性校验码，并向所述终端设备传输添加有所述第一完整性校验码的附着接受信息。

核心网设备中预先设置有第二完整性算法。在接收到附着请求信息后，核心网设备能够根据预先设定的第二完整性算法对附着接受信息进行计算，获取相应的第一完整性校验码。然后，所述核心网设备将所述第一完整性校验码添加至所述附着接受信息中，并将添加所述第一完整性校验码的附着接受信息通过无线接入网设备传输至所述终端设备。

15 步骤 S23、所述核心网设备接收所述终端设备传输的加密的附着完成信息，所述附着完成信息中包含所述终端设备的第三完整性校验码。

20 终端设备接收到附着接受信息后，对所述附着接受信息进行计算，获取第二完整性校验码。其中，终端设备在对附着接受信息进行计算时，通常根据预先设定的第一完整性算法进行计算。另外，核心网设备通过预先设定的第二完整性算法对附着接受信息进行计算，获取第一完整性校验码。若允许终端设备接入核心网设备，则预先设定第一完整性算法与第二完整性算法相同。也就是说，终端设备与核心网设备采用相同的完整性算法进行完整性验证。

25 这种情况下，若所述第一完整性校验码和第二完整性校验码相同，则终端设备确定核心网设备的身份合法。也就是说，本申请实施例中，终端设备通过完整性校验码对核心网设备进行身份认证。

在确定核心网设备的身份合法（即第一完整性校验码和第二完整性校验码相同）后，所述终端设备会生成附着完成信息，再对所述附着完成信息进行加密，从而获取加密的附着完成信息。然后，终端设备使用第一完整性算法对加密的附着完成信息进行计算，获取第三完整性校验码，再将所述第三完整性校验码添加至所述加密的附着完成信息中，通过无线接入网设备将添加有所述第三完整性校验码的附着完成信息传输至核心网设备。

30 步骤 S24、所述核心网设备基于所述加密的附着完成信息，获取第四完整性校验码。

该步骤中，核心网设备在接收到附着完成信息后，能够根据第二完整性算法对附着完成信息进行计算，获取第四完整性校验码。

35 步骤 S25、若所述第三完整性校验码与所述第四完整性校验码相同，所述核心网设备对所述加密的附着完成信息进行解密，并在解密成功后，确定所述终端设备接入核心网设备。

核心网设备若确定第三完整性校验码与第四完整性校验码相同，则可确定终端设备的身份合法。也就是说，核心网设备通过所述附着完成信息中包含的第三完整性校验码实现对终端设备的身份认证。

另外，终端设备对附着完成信息进行了加密处理，以提高附着完成信息的安全性。并且，终端设备通常采用预设的第一加解密方法对附着完成信息进行加密，而核心网设备接收到附着完成信息后，采用预设的第二加解密方法对附着完成信息进行解密。若终端设备允许接入核心网设备，则预先设定第一加解密方法与第二加解密方法相同。

5 这种情况下，在根据确定终端设备的身份合法后，若核心网设备能够根据第二加解密方法对附着完成信息进行解密，说明终端设备与核心网设备之间交互的信息能够进行加解密，则确定终端设备接入核心网设备。

进一步的，终端设备在接入核心网设备之后，终端设备与核心网设备之间能够继续进行信息交互，例如，终端设备将获取到的检测数据通过无线接入网设备传输至核心网设备，
10 核心网设备向通过无线接入网设备向终端设备传输指令信息等。这种情况下，每次信息交互时，信息的发送端可在交互的信息中添加根据该信息计算得到的完整性校验码，以及对
15 该信息进行加密。接收到该信息的接收端对该信息进行计算，获取相应的完整性校验，若
计算获取的完整性校验码与该信息中添加的完整性校验码相同，则接收端可确定接收到的
信息完整，并在确定接收到的信息完整之后，可根据预设的加解密算法进行解密，从而提
15 高了通信系统的安全性。

本申请实施例公开一种信息交互方法，该方法中，核心网设备在接收到终端设备传输
的附着请求信息之后，生成附着接受信息，基于该附着接受信息获取第一完整性校验码，
并将该第一完整性校验码添加至附着接受信息中，然后将附着接受信息传输至终端设备；
终端设备接收所述核心网设备传输的附着接受信息，并基于所述附着接受信息获取第二完
20 整性校验码；若所述第一完整性校验码和所述第二完整性校验码相同，终端设备确定核心
网设备的身份合法，也就是说，终端设备通过附着接受信息中包含的第一完整性校验码实
现对核心网的身份认证，这种情况下，终端设备生成附着完成信息并对所述附着完成信息
进行加密，然后基于加密的附着完成信息获取第三完整性校验码，将所述第三完整性校验
码添加至加密的附着完成信息中，再向核心网设备传输添加有所述第三完整性校验码且加
25 密的附着完成信息；核心网设备接收到附着完成信息后，基于该附着完成信息获取第四完
整性校验码，若第三完整性校验码与第四完整性校验码相同核心网设备确定终端设备的身
份合法，也就是说，核心网设备通过附着完成信息中包含的第四完整性校验码实现对终端
设备的身份认证，然后，核心网设备对附着完成信息进行解密，若解密成功，则确定终端
设备接入核心网设备。

30 参见图 4 所示的信息交互流程示意图，通过本申请实施例公开的信息交互方法，终端
设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就
是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

与现有技术相比，本申请实施例公开的方案，在保障通信系统安全性的前提下，减少
数据交互的流程，并且减少终端设备与核心网设备之间交互的信息的数据量，从而减少了
35 终端设备与核心网设备进行信息交互的耗时，以及减少终端设备的功耗开销。

进一步的，在步骤 S22 中，公开核心网设备在生成附着接受信息后，基于所述附着接
受信息，获取第一完整性校验码的操作。其中，所述基于所述附着接受信息，获取第一完
整性校验码，包括以下步骤：

首先，所述核心网设备基于预设的第三根密钥、核心网设备参数及所述附着请求信息

中包含的终端设备参数，通过预设的第三密钥生成算法生成第一核心网密钥；然后，所述核心网设备基于所述第一核心网密钥和所述附着接受信息，通过预设的第二完整性算法，获取所述第一完整性校验码。

本申请实施例中，在终端设备中预先设置第一根密钥，并且在附着接受信息中包含核心网设备参数。接收到附着接受信息后，终端设备根据第一根密钥、终端设备参数及附着接受信息中包含的核心网设备参数，以及第一密钥生成算法生成第一终端密钥，所述第一终端密钥用于生成完整性校验码。

相应的，在核心网设备中预先设置有第三根密钥，并且在接收到终端设备传输的附着请求信息后，核心网设备能够根据第三根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第三密钥生成算法生成第一核心网密钥，所述第一核心网密钥用于生成完整性校验码。

这种情况下，若终端设备允许接入核心网设备，则根据预先的设置，第一根密钥与第三根密钥相同，第一密钥生成算法与第二密钥生成算法相同，并且，由于计算第一终端密钥与计算第一核心网密钥的过程中，均依据终端设备参数及核心网设备参数，因此，计算得到的第一终端密钥与第一核心网密钥相同。

进一步的，在终端设备中预先设置第一完整性算法，通过第一完整性算法对附着接受信息进行计算，能够得到第二完整性校验码。在核心网设备中预先设置第二完整性算法，通过第二完整性算法对附着接受信息进行计算，能够得到第一完整性校验码。若终端设备允许接入核心网设备，则预先设置第一完整性算法与第二完整性算法相同。

由于第一终端密钥与第一核心网密钥相同，第一完整性算法与第二完整性算法相同，并且，计算第一完整性校验码与计算第二完整性校验码的过程中，均对附着接受信息进行计算，因此，在核心网设备身份合法的情况下，第一完整性校验码与第二完整性校验码相同。这种情况下，终端设备通过比较第一完整性校验码与第二完整性校验码是否相同，即可判定核心网设备的身份是否合法。

另外，本申请实施例中，核心网设备根据第三根密钥、核心网设备参数及终端设备参数生成第一核心网密钥。其中，终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。所述终端设备身份标识能够对不同的终端设备起到区分作用，不同终端设备的终端设备身份标识不同，因此能够区分核心网设备在与不同终端设备进行信息交互时，生成的第一核心网密钥。

所述终端设备身份标识可以采用终端设备国际移动用户标志（international mobile subscriber identity, IMSI），当然，还可以采用其他能够区分不同终端设备的参数作为终端设备身份标识，本申请实施例对此不做限定。

另外，终端随机数为终端设备随机生成的一个数据，将终端随机数作为终端设备参数，能够保障终端设备参数不易被仿冒，从而提高终端设备参数的安全性，进一步提高获取第一核心网密钥的安全性。

其中，核心网设备参数可包括多种形式，在其中一种形式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。所述核心网设备身份标识用于对不同的核心网设备起到区分作用，因此不同的核心网设备生成的第一核心网密钥不同，从而能够区分不同核心网设备生成的第一核心网密钥。

在本申请实施例中，可预先为各个核心网设备分配一个不同的核心网标签，通过核心网标签区分各个核心网设备，这种情况下，可将该核心网标签作为核心网设备身份标识。当然，还可以采用其他能够区分不同核心网设备的参数作为核心网设备身份标识，本申请实施例对此不做限定。

5 另外，核心网随机数为核心网设备随机生成的一个数据，不易通过多次抓取数据被攻击，将核心网随机数作为核心网设备参数，能够保证核心网设备参数不易被仿冒，从而提高核心网设备参数的安全性，进一步提高获取第一核心网密钥的安全性。

本申请实施例中，核心网设备采用第三密钥生成算法生成第一核心网密钥。其中，第三密钥生成算法可以为多种形式的密钥生成算法。例如，第三密钥生成算法可以为
10 HMAC-SHA-256 算法。也就是说，核心网设备能够根据公式（1）和公式（2）生成第一核心网密钥。

其中，核心网设备在计算第一核心网密钥时采用 HMAC-SHA-256 算法，则在公式（1）中，Derived Key 为第一核心网密钥，RootKey 为核心网设备中的第三根密钥，S 为密钥计算参数。公式（1）输出的字符长度通常为 256bit，在本申请实施例中，可以使用其中的
15 低 128 位作为第一核心网密钥。并且，用于获取密钥计算参数 S 的公式（2）中，FC 为预设值，通常情况下，FC=0x015，当然，也可将 FC 设置为其他数值；Algorithm Type Distinguisher 的具体数值与计算第一终端密钥时设置的具体数值相同。例如，若在计算第一终端密钥时，Algorithm Type Distinguisher = 0x02，相应的，在计算第一核心网
20 密钥时，Algorithm Type Distinguisher = 0x02。NET ID 是作为核心网设备身份标识的核心网标签；L0 为 Algorithm Type Distinguisher 的字节长度；L1 为核心网标签 NET ID 的字节长度；NET Rand 为核心网随机数；L2 为核心网随机数 NET Rand 的字节长度；IMSI 是作为终端设备身份标识的终端设备国际移动用户标志；L3 为 IMSI 的字节长度；UE Rand 为终端随机数；L4 为终端随机数 UE Rand 的字节长度。

这种情况下，可通过公式（2）获取 S 的值，然后将 S 的值带入至公式（1），计算得
25 到第一核心网密钥。

当然，还可以采用其他形式的密钥生成算法，本申请实施例对此不作限定。

另外，核心网设备基于第一核心网密钥和附着接受信息，通过预设的第二完整性算法获取所述第一完整性校验码，该第二完整性算法可为多种形式，例如，第二完整性算法可采用 AES-128-CMAC，其算法示意图如图 5 所示。该算法中，根据信息计数、信息、信息方向、固定数值参数以及用于完整性保护的密钥，即可计算得到完整性校验码。其中，信息
30 为计算完整性校验码时所应用的信息，其中，在计算第一完整性校验码时，信息即为附着接受信息；另外，若应用的信息的信息方向为上行，则信息方向通常取值为 0，若应用的信息的信息方向为下行，则信息方向通常取值为 1；固定数值参数通常取值为 0。

当然，还可以采用其他的完整性算法，本申请实施例对此不作限定。

35 进一步的，本申请实施例的步骤 S25 中，公开核心网设备对所述加密的附着完成信息进行解密的操作。所述核心网设备对所述加密的附着完成信息进行解密通常包括以下步骤：

首先，所述核心网设备基于预设的第四根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第四密钥生成算法生成第二核心网密钥；然后，所述核心网设备基于所述第二核心网密钥，通过预设的第二加解密算法对所述加密的附着完成

信息进行解密。

本申请实施例中，在终端设备中预先设置第二根密钥，并且在附着请求信息中包含终端设备参数。接收到附着接受信息后，终端设备获取核心网设备参数，然后根据第二根密钥、终端设备参数及核心网设备参数，以及第二密钥生成算法生成第二终端设备密钥，所述第二终端设备密钥用于对交互的信息进行加密保护。

另外，在核心网设备中，预先设置第四根密钥，并且在接收到终端设备传输的附着请求信息后，核心网设备根据第四根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第四密钥生成算法生成第二核心网设备密钥，所述第二核心网设备密钥用于对交互的信息进行加密保护。

这种情况下，若允许终端设备接入核心网设备，则预先设置第二根密钥与第四根密钥相同，第二密钥生成算法与第四密钥生成算法相同，并且，由于计算第二终端设备密钥与计算第二核心网设备密钥的过程中，均依据终端设备参数及核心网设备参数，因此，第二终端设备密钥与第二核心网设备密钥相同。

进一步的，在终端设备中预先设置第一加解密算法，以便通过第一加解密算法对附着完成信息进行加密。在核心网设备中预先设置第二加解密算法，以便通过第二加解密算法对附着完成信息进行解密。其中，若允许终端设备接入核心网设备，则预先设置第一加解密算法与第二加解密算法相同，以便核心网设备能够对终端设备加密的信息进行解密。

另外，本申请实施例中，核心网设备根据第四根密钥、核心网设备参数及终端设备参数生成第二核心网密钥。其中，终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。所述终端设备身份标识能够对不同的终端设备起到区分作用，不同终端设备的终端设备身份标识不同，因此能够区分核心网设备在与不同终端设备进行信息交互时，生成的第二核心网密钥。

所述终端设备身份标识可以采用终端设备国际移动用户标志（international mobile subscriber identity, IMSI），当然，还可以采用其他能够区分不同终端设备的参数作为终端设备身份标识，本申请实施例对此不做限定。

另外，终端随机数为终端设备随机生成的一个数据，将终端随机数作为终端设备参数，能够保障终端设备参数不易被仿冒，从而提高终端设备参数的安全性，进一步提高获取第二核心网密钥的安全性。

其中，核心网设备参数可包括多种形式，在其中一种形式中，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。所述核心网设备身份标识用于对不同的核心网设备起到区分作用，因此不同的核心网设备生成的第二核心网密钥不同，从而能够区分不同核心网设备生成的第二核心网密钥。

在本申请实施例中，可预先为各个核心网设备分配一个不同的核心网标签，通过核心网标签区分各个核心网设备，这种情况下，可将该核心网标签作为核心网设备身份标识。当然，还可以采用其他能够区分不同核心网设备的参数作为核心网设备身份标识，本申请实施例对此不做限定。

另外，核心网随机数为核心网设备随机生成的一个数据，不易通过多次抓取数据被攻击，将核心网随机数作为核心网设备参数，能够保证核心网设备参数不易被仿冒，从而提高核心网设备参数的安全性，进一步提高获取第二核心网密钥的安全性。

上述步骤中，核心网设备采用第四密钥生成算法生成第二核心网密钥。其中，第四密钥生成算法可采用多种形式的密钥生成算法，例如，第四密钥生成算法也可以为 HMAC-SHA-256 算法。也就是说，可以通过公式（1）与公式（2）计算第二核心网密钥。

在通过 HMAC-SHA-256 算法计算第二核心网密钥时，Derived Key 为第二核心网密钥，RootKey 为核心网设备中的第四根密钥，S 为密钥计算参数。该公式输出的字符长度通常为 256bit，在本申请实施例中，可以使用其中的低 128 位作为第二核心网密钥。

另外，用于获取密钥计算参数 S 的公式（2）中，FC 为预设值，通常情况下，FC=0x015，当然，也可将 FC 设置为其他数值；Algorithm Type Distinguisher 为预设值，Algorithm Type Distinguisher 的具体数值与计算第二终端密钥时设置的具体数值相同，例如，若在计算第二终端密钥时，Algorithm Type Distinguisher = 0x01，相应的，在计算第二核心网密钥时，Algorithm Type Distinguisher = 0x01；NET ID 是作为核心网设备身份标识的核心网标签；L0 为 Algorithm Type Distinguisher 的字节长度；L1 为核心网标签 NET ID 的字节长度；NET Rand 为核心网随机数；L2 为核心网随机数 NET Rand 的字节长度；IMSI 是作为终端设备身份标识的终端设备国际移动用户标志；L3 为 IMSI 的字节长度；UE Rand 为终端随机数；L4 为终端随机数 UE Rand 的字节长度。

当然，还可以采用其他形式的密钥生成算法，本申请实施例对此不作限定。

进一步的，为了提高通信系统的安全性，所述第三根密钥和第四根密钥可经过加密处理，当需要时，核心网设备再对其进行解密，然后分别通过解密后的第三根密钥生成第一核心网密钥，通过解密后的第四根密钥生成第二核心网密钥。其中，核心网设备对第三根密钥和第四根密钥进行加解密时，可采用相同的加解密算法，也可采用不同的加解密算法，本申请实施例对此不做限定。

另外，第三根密钥和第四根密钥可为同一根密钥，即核心网设备通过相同的根密钥生成第一核心网密钥和第二核心网密钥。或者，第三根密钥和第四根密钥分别为不同的根密钥，本申请实施例对此不做限定。

下述为本申请装置实施例，可以用于执行本申请方法实施例。对于本申请装置实施例中未披露的细节，请参照本申请方法实施例。

本申请通过第三实施例公开一种信息交互装置。该装置应用于图 1 中的终端设备，该终端设备能够通过无线接入网设备与核心网设备之间进行信息交互，并执行本申请第一实施例公开的信息交互方法。

参见图 7 所示的结构示意图，本申请实施例公开的信息交互装置包括：第一发送模块 100、第一接收模块 200 和第一处理模块 300。

其中，所述第一发送模块 100 用于向核心网设备传输附着请求信息。在该附着请求信息中，可以包括终端设备参数。其中，所述终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数。

所述第一接收模块 200 用于接收所述核心网设备传输的附着接受信息，所述附着接受信息中包括所述核心网设备的第一完整性校验码。

核心网设备接收到所述附着请求信息后，生成附着接受信息，并对所述附着接受信息进行计算，获取第一完整性校验码，将所述第一完整性校验码添加至附着接受信息中，再通过无线接入设备将添加有第一完整性校验码的附着接受信息传输至终端设备。

所述第一处理模块 300 用于基于所述附着接受信息获取第二完整性校验码，若所述第一完整性校验码和所述第二完整性校验码相同，所述第一处理模块用于获取加密的附着完成信息，并基于所述加密的附着完成信息获取第三完整性校验码，并触发所述第一发送模块向所述核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息。

5 其中，第一处理模块 300 通常根据预先设定的第一完整性算法进行计算，获取第二完整性校验码。另外，核心网设备通过预先设定的第二完整性算法对附着接受信息进行计算，获取第一完整性校验码，这种情况下，若允许终端设备接入核心网设备，则预先设定第一完整性算法与第二完整性算法相同。

10 若所述第一完整性校验码和第二完整性校验码相同，则终端设备确定核心网设备的身份合法。在确定核心网设备的身份合法后，第一处理模块 300 生成附着完成信息，再对所述附着完成信息进行加密，从而获取加密的附着完成信息，然后使用第一完整性算法对加密的附着完成信息进行计算，获取第三完整性校验码，再将所述第三完整性校验码添加至所述加密的附着完成信息中。

15 这种情况下，核心网设备在接收到附着完成信息后，能够根据第二完整性算法对附着完成信息进行计算，获取第四完整性校验码。并且，核心网设备若确定第三完整性校验码与第四完整性校验码相同，则可确定终端设备的身份合法。也就是说，核心网设备通过所述附着完成信息中包含的第三完整性校验码实现对终端设备的身份认证。其中，第一完整性算法与第二完整性算法相同。

20 另外，第一处理模块对附着完成信息进行了加密处理，并且通常采用预设的第一加解密方法对附着完成信息进行加密，而核心网设备接收到附着完成信息后，采用预设的第二加解密方法对附着完成信息进行解密。若终端设备允许接入核心网设备，则预先设定第一加解密方法与第二加解密方法相同。这种情况下，在根据完整性校验码确定终端设备的身份合法后，若核心网设备能够根据第二加解密方法对附着完成信息进行解密，说明终端设备与核心网设备之间交互的信息能够互相进行加解密，则确定终端设备接入核心网设备。

25 通过本申请实施例公开的信息交互装置，终端设备与核心网设备之间只需要传输附着请求信息、附着接受信息和附着完成信息，也就是说，只需要进行三次信息交互，即可实现对对方身份的认证及数据保护。

30 与现有技术相比，本申请实施例公开的方案，在保障通信系统安全性的前提下，减少数据交互的流程，并且减少终端设备与核心网设备之间交互的信息的数据量，从而减少了终端设备与核心网设备进行信息交互的耗时，以及减少终端设备的功耗开销。

进一步的，所述第一处理模块具体用于基于预设的第一根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第一密钥生成算法生成第一终端密钥，并基于所述第一终端密钥和所述附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码。

35 在本申请实施例中，在终端设备中预先设置第一根密钥，并且在附着接受信息中包含核心网设备参数。接收到附着接受信息后，终端设备根据第一根密钥、终端设备参数及附着接受信息中包含的核心网设备参数，以及第一密钥生成算法生成第一终端密钥，所述第一终端密钥用于生成完整性校验码。

另外，在核心网设备中预先设置有第三根密钥，并且在接收到终端设备传输的附着请

求信息后，核心网设备能够根据第三根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第三密钥生成算法生成第一核心网密钥，所述第一核心网密钥用于生成完整性校验码。

5 这种情况下，若终端设备允许接入核心网设备，则根据预先的设置，第一根密钥与第三根密钥相同，第一密钥生成算法与第二密钥生成算法相同，并且，由于计算第一终端密钥与计算第一核心网密钥的过程中，均依据终端设备参数及核心网设备参数，因此，计算得到的第一终端密钥与第一核心网密钥相同。

10 进一步的，在终端设备中预先设置第一完整性算法，通过第一完整性算法和第一终端密钥对附着接受信息进行计算，能够得到第二完整性校验码。在核心网设备中预先设置第二完整性算法，通过第二完整性算法和第一核心网密钥对附着接受信息进行计算，能够得到第一完整性校验码。若终端设备允许接入核心网设备，则预先设置第一完整性算法与第二完整性算法相同。

15 由于第一终端密钥与第一核心网密钥相同，第一完整性算法与第二完整性算法相同，并且，计算第一完整性校验码与计算第二完整性校验码的过程中，均对附着接受信息进行计算，因此，在核心网设备身份合法的情况下，第一完整性校验码与第二完整性校验码相同。这种情况下，终端设备通过比较第一完整性校验码与第二完整性校验码是否相同，即可判定核心网设备的身份是否合法。

20 进一步的，所述第一处理模块具体用于基于预设的第二根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第二密钥生成算法生成第二终端密钥，并在生成附着完成信息后，基于所述第二终端密钥，通过预设的第一加解密算法对所述附着完成信息进行加密。

25 本申请实施例中，在终端设备中预先设置第二根密钥，并且在附着接受信息中包含核心网设备参数。接收到附着接受信息后，终端设备获取核心网设备参数，然后根据第二根密钥、终端设备参数及核心网设备参数，以及第二密钥生成算法生成第二终端密钥，所述第二终端密钥用于对交互的信息进行加密保护。

30 另外，在核心网设备中，预先设置第四根密钥，并且在接收到终端设备传输的附着请求信息后，核心网设备根据第四根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第四密钥生成算法生成第二核心网密钥，所述第二核心网密钥用于对交互的信息进行加密保护。

35 这种情况下，若允许终端设备接入核心网设备，则预先设置第二根密钥与第四根密钥相同，第二密钥生成算法与第四密钥生成算法相同，并且，由于计算第二终端密钥与计算第二核心网密钥的过程中，均依据终端设备参数及核心网设备参数，因此，第二终端密钥与第二核心网密钥相同。

进一步的，在终端设备中预先设置第一加解密算法，以便通过第一加解密算法对附着完成信息进行加密。在核心网设备中预先设置第二加解密算法，以便通过第二加解密算法对附着完成信息进行解密。其中，若允许终端设备接入核心网设备，则预先设置第一加解密算法与第二加解密算法相同，以便核心网设备能够对终端设备加密的信息进行解密。

另外，在本申请实施例中，所述终端设备参数通常包括：终端设备身份标识和所述终端设备产生的终端随机数，所述核心网设备参数包括：核心网设备身份标识和所述核心网

设备产生的核心网随机数。

相应的，本申请通过第四实施例公开一种信息交互装置，该装置应用于核心网设备，该核心网设备可通过无线接入网设备与终端设备之间进行信息交互，并执行本申请第二实施例公开的信息交互方法。

5 参见图 8 所示的结构示意图，本申请实施例公开的信息交互装置包括：第二接收模块 400、第二发送模块 500 和第二处理模块 600。

其中，所述第二接收模块 400 用于接收终端设备传输的附着请求信息。

10 其中，当终端设备需要接入核心网设备时，终端设备会产生附着请求信息，并通过无线接入网设备将其传输至第二接收模块 400。在该附着请求信息中，可以包括终端设备参数。

所述第二处理模块 600 用于在生成附着接受信息后，基于所述附着接受信息，获取第一完整性校验码，并触发所述第二发送模块 500 向所述终端设备传输添加有所述第一完整性校验码的附着接受信息。

15 核心网设备中预先设置有第二完整性算法。在接收到附着请求信息后，第二处理模块 600 能够根据预先设定的第二完整性算法对附着接受信息进行计算，获取相应的第一完整性校验码。然后，所述第二处理模块 600 将所述第一完整性校验码添加至所述附着接受信息中，并将添加所述第一完整性校验码的附着接受信息通过无线接入网设备传输至所述终端设备。

20 所述第二接收模块 400 还用于接收所述终端设备传输的加密的附着完成信息，所述附着完成信息中包含所述终端设备的第三完整性校验码。

25 终端设备接收到附着接受信息后，对所述附着接受信息进行计算，获取第二完整性校验码。其中，终端设备在对附着接受信息进行计算时，通常根据预先设定的第一完整性算法进行计算。另外，核心网设备通过预先设定的第二完整性算法对附着接受信息进行计算，获取第一完整性校验码。若允许终端设备接入核心网设备，则预先设定第一完整性算法与第二完整性算法相同。也就是说，终端设备与核心网设备采用相同的完整性算法进行完整性验证。这种情况下，若所述第一完整性校验码和第二完整性校验码相同，则终端设备确定核心网设备的身份合法。

30 在确定核心网设备的身份合法后，所述终端设备会生成附着完成信息，再对所述附着完成信息进行加密，从而获取加密的附着完成信息。然后，终端设备使用第一完整性算法对加密的附着完成信息进行计算，获取第三完整性校验码，再将所述第三完整性校验码添加至所述加密的附着完成信息中，通过无线接入网设备将添加有所述第三完整性校验码的附着完成信息传输至核心网设备，以便核心网设备通过第二接收模块 500 获取该附着完成信息。

35 所述第二处理模块 600 还用于基于所述加密的附着完成信息，获取第四完整性校验码，若所述第三完整性校验码与所述第四完整性校验码相同，所述第二处理模块 600 对所述加密的附着完成信息进行解密，并在解密成功后，确定所述终端设备接入核心网设备。

其中，第二处理模块 600 能够根据第二完整性算法对附着完成信息进行计算，获取第四完整性校验码。若确定第三完整性校验码与第四完整性校验码相同，则可确定终端设备的身份合法。

另外，终端设备对附着完成信息进行了加密处理，以提高附着完成信息的安全性。并且，终端设备通常采用预设的第一加解密方法对附着完成信息进行加密，而核心网设备接收到附着完成信息后，采用预设的第二加解密方法对附着完成信息进行解密。若终端设备允许接入核心网设备，则预先设定第一加解密方法与第二加解密方法相同。

5 这种情况下，在根据确定终端设备的身份合法后，若核心网设备能够根据第二加解密方法对附着完成信息进行解密，说明终端设备与核心网设备之间交互的信息能够进行加解密，则确定终端设备接入核心网设备。

与现有技术相比，本申请实施例公开的方案，在保障通信系统安全性的前提下，减少数据交互的流程，并且减少终端设备与核心网设备之间交互的信息的数据量，从而减少了
10 终端设备与核心网设备进行信息交互的耗时，以及减少终端设备的功耗开销。

进一步的，在本申请实施例中，所述第二处理模块具体用于基于预设的第三根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第三密钥生成算法生成第一核心网密钥，并基于所述第一核心网密钥和所述附着接受信息，通过预设的第二完整性算法，获取所述第一完整性校验码。

15 本申请实施例中，在终端设备中预先设置第一根密钥，并且在附着接受信息中包含核心网设备参数。接收到附着接受信息后，终端设备根据第一根密钥、终端设备参数及附着接受信息中包含的核心网设备参数，以及第一密钥生成算法生成第一终端密钥，所述第一终端密钥用于生成完整性校验码。

相应的，在核心网设备中预先设置有第三根密钥，并且在接收到终端设备传输的附着
20 请求信息后，核心网设备能够根据第三根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第三密钥生成算法生成第一核心网密钥，所述第一核心网密钥用于生成完整性校验码。

这种情况下，若终端设备允许接入核心网设备，则根据预先的设置，第一根密钥与第三根密钥相同，第一密钥生成算法与第二密钥生成算法相同，并且，由于计算第一终端密
25 钥与计算第一核心网密钥的过程中，均依据终端设备参数及核心网设备参数，因此，计算得到的第一终端密钥与第一核心网密钥相同。

进一步的，在终端设备中预先设置第一完整性算法，通过第一完整性算法对附着接受信息进行计算，能够得到第二完整性校验码。在核心网设备中预先设置第二完整性算法，通过第二完整性算法对附着接受信息进行计算，能够得到第一完整性校验码。若终端设备
30 允许接入核心网设备，则预先设置第一完整性算法与第二完整性算法相同。

由于第一终端密钥与第一核心网密钥相同，第一完整性算法与第二完整性算法相同，并且，计算第一完整性校验码与计算第二完整性校验码的过程中，均对附着接受信息进行计算，因此，在核心网设备身份合法的情况下，第一完整性校验码与第二完整性校验码相同。这种情况下，终端设备通过比较第一完整性校验码与第二完整性校验码是否相同，即
35 可判定核心网设备的身份是否合法。

进一步的，在本申请实施例中，所述第二处理模块具体用于基于预设的第四根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第四密钥生成算法生成第二核心网密钥，并基于所述第二核心网密钥，通过预设的第二加解密算法对所述加密的附着完成信息进行解密。

本申请实施例中，在终端设备中预先设置第二根密钥，并且在附着请求信息中包含终端设备参数。接收到附着接受信息后，终端设备获取核心网设备参数，然后根据第二根密钥、终端设备参数及核心网设备参数，以及第二密钥生成算法生成第二终端设备密钥，所述第二终端设备密钥用于对交互的信息进行加密保护。

5 另外，在核心网设备中，预先设置第四根密钥，并且在接收到终端设备传输的附着请求信息后，核心网设备根据第四根密钥、核心网设备参数及附着请求信息中包含的终端设备参数，利用第四密钥生成算法生成第二核心网设备密钥，所述第二核心网设备密钥用于对交互的信息进行加密保护。

10 这种情况下，若允许终端设备接入核心网设备，则预先设置第二根密钥与第四根密钥相同，第二密钥生成算法与第四密钥生成算法相同，并且，由于计算第二终端设备密钥与计算第二核心网设备密钥的过程中，均依据终端设备参数及核心网设备参数，因此，第二终端设备密钥与第二核心网设备密钥相同。

15 进一步的，在终端设备中预先设置第一加解密算法，以便通过第一加解密算法对附着完成信息进行加密。在核心网设备中预先设置第二加解密算法，以便通过第二加解密算法对附着完成信息进行解密。其中，若允许终端设备接入核心网设备，则预先设置第一加解密算法与第二加解密算法相同，以便核心网设备能够对终端设备加密的信息进行解密。

另外，在本申请实施例中，所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数，所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。

20 相应的，本申请实施例还公开一种终端设备，该终端设备包括：收发端口、处理器和与所述处理器相连接的存储器；其中，所述收发端口用于和核心网设备之间进行信息的交互，并将从所述核心网设备接收的信息传输至处理器；所述存储器存储有可被所述处理器执行的指令；所述处理器用于获取所述收发端口传输的报文，并通过执行所述存储器中所存储的程序或指令，执行本申请第一实施例中所公开的信息交互方法。

25 相应的，本申请实施例还公开一种核心网设备，该核心网设备包括：收发端口、处理器和与所述处理器相连接的存储器；其中，所述收发端口用于和终端设备之间进行信息的交互，并将从所述终端设备接收的信息传输至处理器；所述存储器存储有可被所述处理器执行的指令；所述处理器用于获取所述收发端口传输的报文，并通过执行所述存储器中所存储的程序或指令，执行本申请第二实施例中所公开的信息交互方法。

30 本申请实施例还提供一种计算机程序产品，包括指令，当指令在计算机上运行时，使得计算机执行图 2 所公开的方法实施例中公开的信息交互方法。

本申请实施例还提供一种计算机程序产品，包括指令，当指令在计算机上运行时，使得计算机执行图 6 所公开的方法实施例中公开的信息交互方法。

35 具体实现中，本申请实施例还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时可实现图 2 或图 6 所公开方法实施例中的信息交互方法中的部分或全部步骤。所述的存储介质可为磁碟、光盘、只读存储记忆体（read-only memory, ROM）或随机存储记忆体（random access memory, RAM）等。

本申请实施例还提供了一种芯片，所述芯片装置包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时，实现

本申请第一实施例或第二实施例中所公开的信息交互方法。

需要指出，根据实施的需要，可将本申请实施例中描述的各个部件/步骤拆分为更多部件/步骤，也可将两个或多个部件/步骤或者部件/步骤的部分操作组合成新的部件/步骤，以实现本申请的目的。

- 5 本领域的技术人员可以清楚地了解到本申请实施例中的技术可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请实施例中的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，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，或者网络设备等）执行本申请各个实施例或者实施例的某些部分
- 10 所述的方法。

本说明书中各个实施例之间相同相似的部分互相参见即可。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例中的说明即可。

以上所述的本申请实施方式并不构成对本申请保护范围的限定。

权 利 要 求 书

1、一种信息交互方法，其特征在于，包括：

终端设备向核心网设备传输附着请求信息；

5 所述终端设备接收所述核心网设备传输的附着接受信息，所述附着接受信息中包含所述核心网设备的第一完整性校验码；

所述终端设备基于所述附着接受信息获取第二完整性校验码；

若所述第一完整性校验码和所述第二完整性校验码相同，所述终端设备获取加密的附着完成信息，并基于所述加密的附着完成信息获取第三完整性校验码，向所述核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息。

10 2、根据权利要求1所述的信息交互方法，其特征在于，所述终端设备基于所述附着接受信息获取第二完整性校验码，包括：

所述终端设备基于预设的第一根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第一密钥生成算法生成第一终端密钥；

15 所述终端设备基于所述第一终端密钥和所述附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码。

3、根据权利要求1所述的信息交互方法，其特征在于，所述终端设备获取加密的附着完成信息，包括：

所述终端设备基于预设的第二根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第二密钥生成算法生成第二终端密钥；

20 所述终端设备在生成附着完成信息后，基于所述第二终端密钥，通过预设的第一加解密算法对所述附着完成信息进行加密。

4、根据权利要求2或3所述的信息交互方法，其特征在于，

所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。

5、根据权利要求2或3所述的信息交互方法，其特征在于，

25 所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。

6、一种信息交互方法，其特征在于，包括：

核心网设备接收终端设备传输的附着请求信息；

30 所述核心网设备在生成附着接受信息后，基于所述附着接受信息，获取第一完整性校验码，并向所述终端设备传输添加有所述第一完整性校验码的附着接受信息；

所述核心网设备接收所述终端设备传输的加密的附着完成信息，所述附着完成信息中包含所述终端设备的第三完整性校验码；

所述核心网设备基于所述加密的附着完成信息，获取第四完整性校验码；

35 若所述第三完整性校验码与所述第四完整性校验码相同，所述核心网设备对所述加密的附着完成信息进行解密，并在解密成功后，确定所述终端设备接入核心网设备。

7、根据权利要求6所述的信息交互方法，其特征在于，所述基于所述附着接受信息，获取第一完整性校验码，包括：

所述核心网设备基于预设的第三根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第三密钥生成算法生成第一核心网密钥；

所述核心网设备基于所述第一核心网密钥和所述附着接受信息，通过预设的第二完整性算法，获取所述第一完整性校验码。

8、根据权利要求6所述的信息交互方法，其特征在于，所述核心网设备对所述加密的附着完成信息进行解密，包括：

5 所述核心网设备基于预设的第四根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第四密钥生成算法生成第二核心网密钥；

所述核心网设备基于所述第二核心网密钥，通过预设的第二加解密算法对所述加密的附着完成信息进行解密。

9、根据权利要求7或8所述的信息交互方法，其特征在于，

10 所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。

10、根据权利要求7或8所述的信息交互方法，其特征在于，

所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。

11、一种信息交互装置，其特征在于，包括：

15 第一发送模块、第一接收模块和第一处理模块；

所述第一发送模块用于向核心网设备传输附着请求信息；

所述第一接收模块用于接收所述核心网设备传输的附着接受信息，所述附着接受信息中包括所述核心网设备的第一完整性校验码；

20 所述第一处理模块用于基于所述附着接受信息获取第二完整性校验码，若所述第一完整性校验码和所述第二完整性校验码相同，所述第一处理模块用于获取加密的附着完成信息，并基于所述加密的附着完成信息获取第三完整性校验码，并触发所述第一发送模块向所述核心网设备传输添加有所述第三完整性校验码且加密的附着完成信息。

12、根据权利要求11所述的信息交互装置，其特征在于，

25 所述第一处理模块具体用于基于预设的第一根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第一密钥生成算法生成第一终端密钥，并基于所述第一终端密钥和所述附着接受信息，通过预设的第一完整性算法获取所述第二完整性校验码。

13、根据权利要求11所述的信息交互装置，其特征在于，

30 所述第一处理模块具体用于基于预设的第二根密钥、终端设备参数及所述附着接受信息中包含的核心网设备参数，通过预设的第二密钥生成算法生成第二终端密钥，并在生成附着完成信息后，基于所述第二终端密钥，通过预设的第一加解密算法对所述附着完成信息进行加密。

14、根据权利要求12或13所述的信息交互装置，其特征在于，

35 所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。

15、根据权利要求12或13所述的信息交互装置，其特征在于，

所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。

16、一种信息交互装置，其特征在于，包括：

第二接收模块、第二发送模块和第二处理模块，

所述第二接收模块用于接收终端设备传输的附着请求信息；

所述第二处理模块用于在生成附着接受信息后，基于所述附着接受信息，获取第一完整性校验码，并触发所述第二发送模块向所述终端设备传输添加有所述第一完整性校验码的附着接受信息；

所述第二接收模块还用于接收所述终端设备传输的加密的附着完成信息，所述附着完成信息中包含所述终端设备的第三完整性校验码；

所述第二处理模块还用于基于所述加密的附着完成信息，获取第四完整性校验码，若所述第三完整性校验码与所述第四完整性校验码相同，所述第二处理模块对所述加密的附着完成信息进行解密，并在解密成功后，确定所述终端设备接入核心网设备。

17、根据权利要求 16 所述的信息交互装置，其特征在于，

所述第二处理模块具体用于基于预设的第三根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第三密钥生成算法生成第一核心网密钥，并基于所述第一核心网密钥和所述附着接受信息，通过预设的第二完整性算法，获取所述完整性校验码。

18、根据权利要求 16 所述的信息交互装置，其特征在于，

所述第二处理模块具体用于基于预设的第四根密钥、核心网设备参数及所述附着请求信息中包含的终端设备参数，通过预设的第四密钥生成算法生成第二核心网密钥，并基于所述第二核心网密钥，通过预设的第二加解密算法对所述加密的附着完成信息进行解密。

19、根据权利要求 17 或 18 所述的信息交互装置，其特征在于，

所述终端设备参数包括：终端设备身份标识和所述终端设备产生的终端随机数。

20、根据权利要求 17 或 18 所述的信息交互装置，其特征在于，

所述核心网设备参数包括：核心网设备身份标识和所述核心网设备产生的核心网随机数。

21、一种计算机可读存储介质，其特征在于，包括指令，当其在计算机上运行时，使得计算机执行如权利要求 1 至 5 中任一项所述的方法，或使得计算机执行如权利要求 6 至 10 中任一项所述的方法。

22、一种计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1 至 5 中任一项所述的方法，或使得计算机执行如权利要求 6 至 10 中任一项所述的方法。

23、一种终端设备，其特征在于，包括：处理器和存储器；

所述存储器用于存储计算机执行指令，当所述终端设备运行时，所述处理器执行所述存储器存储的该计算机执行指令，以使所述终端设备执行如权利要求 1 至 5 中任一项所述的信息交互方法。

24、一种核心网设备，其特征在于，包括：处理器和存储器；

所述存储器用于存储计算机执行指令，当所述核心网设备运行时，所述处理器执行所述存储器存储的该计算机执行指令，以使所述核心网设备执行如权利要求 6 至 10 中任一项所述的信息交互方法。

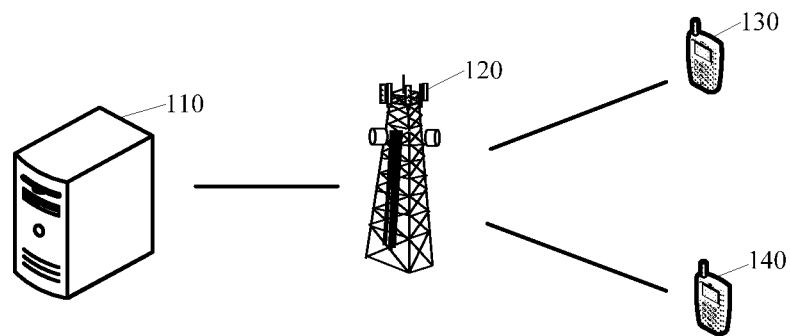


图 1

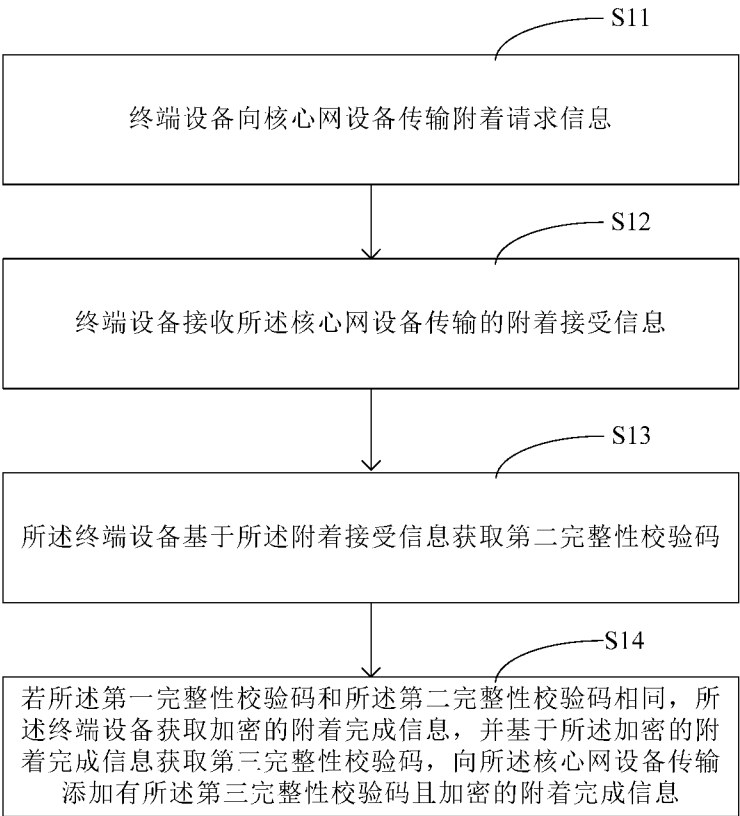


图 2

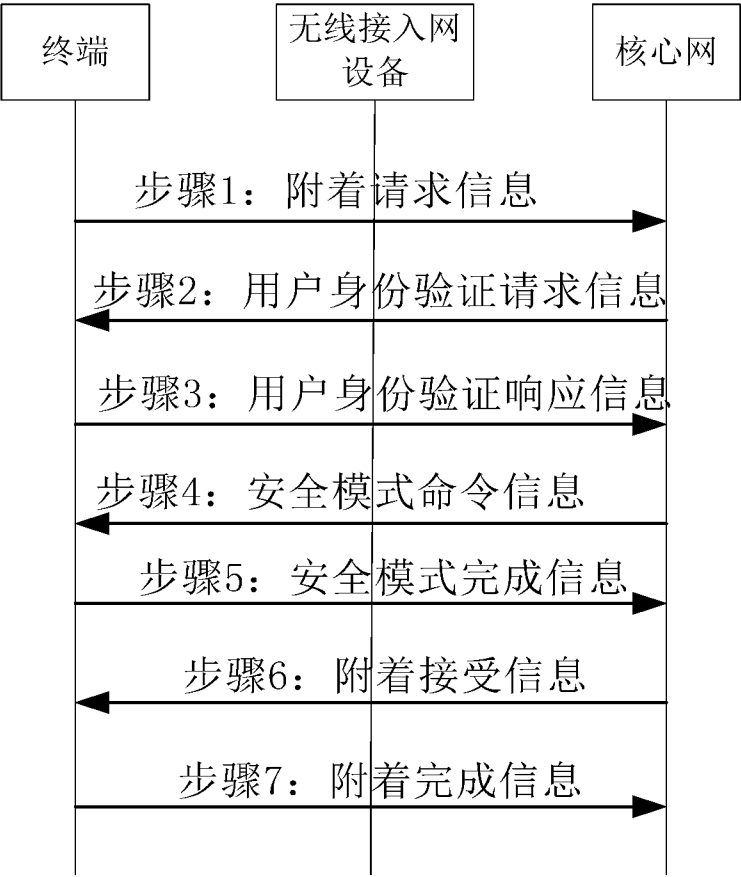


图 3

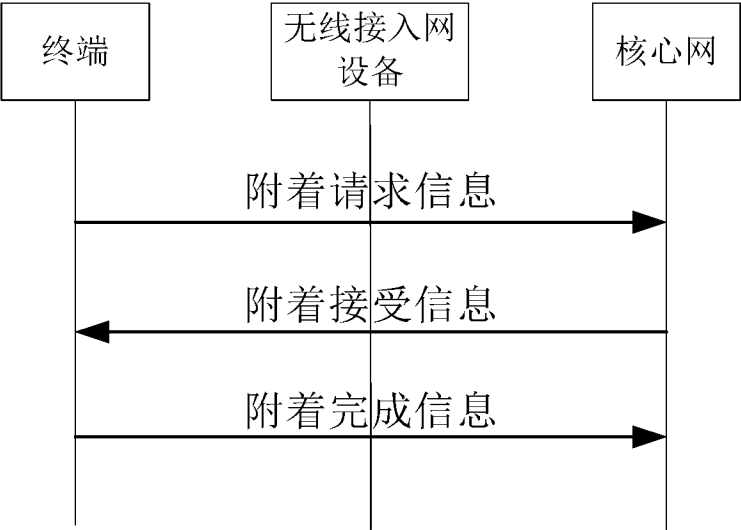


图 4

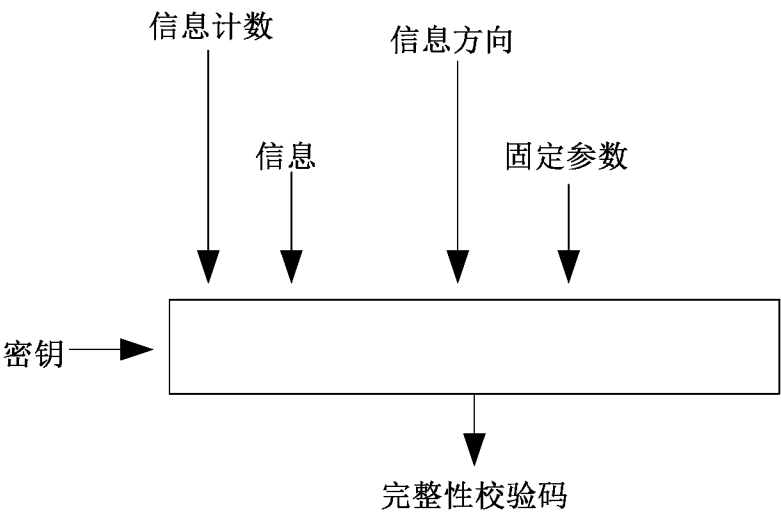


图 5

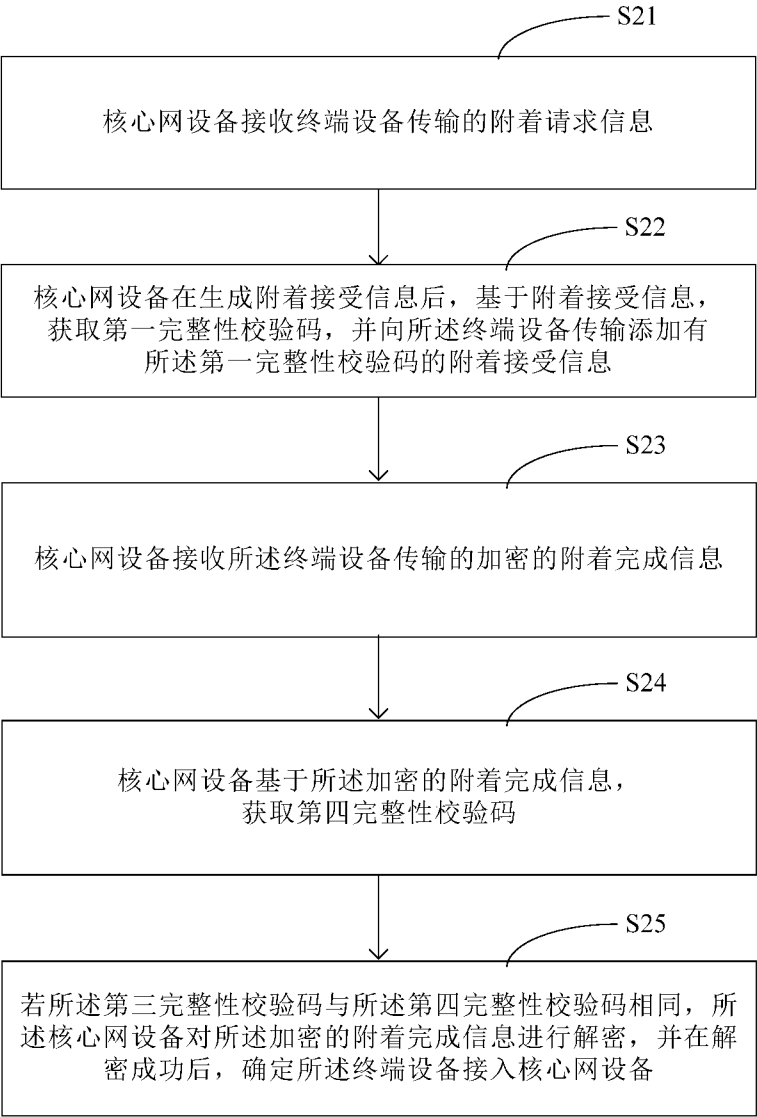


图 6

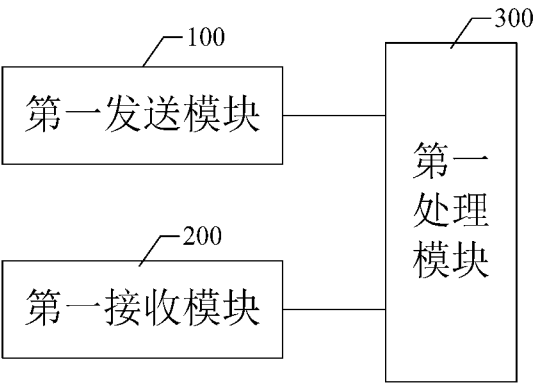


图 7

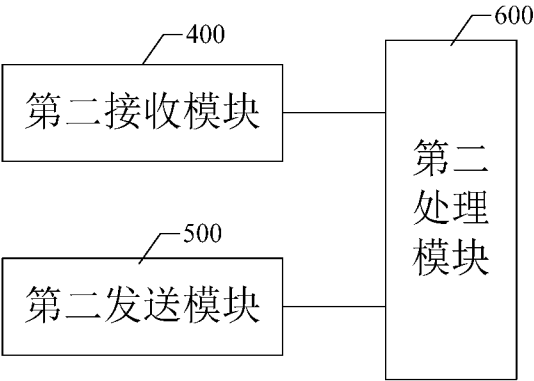


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/105504

A. CLASSIFICATION OF SUBJECT MATTER

H04W 60/00(2009.01)i; H04W 76/00(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 附着, 请求, 接受, 完成, 完整性, 校验, 加密, 密钥, 随机数, 身份, 标识, attach+, request+, complet+, integrity, encrypt+, checkout, decrypt+, key, random number, identity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104852994 A (POTEVIO INSTITUTE TECHNOLOGY CO., LTD.) 19 August 2015 (2015-08-19) description, paragraphs [0065]-[0098]	1-24
A	CN 102333386 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) 25 January 2012 (2012-01-25) entire document	1-24
A	EP 2713664 A1 (ALCATEL LUCENT) 02 April 2014 (2014-04-02) entire document	1-24
A	ERICSSON. "Corrections to EASE" 3GPP TSG-SA WG3 Meeting #84 S3-161180, 29 July 2016 (2016-07-29), entire document	1-24

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

17 November 2018

Date of mailing of the international search report

28 November 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/105504

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	104852994	A	19 August 2015	None	
CN	102333386	A	25 January 2012	None	
EP	2713664	A1	02 April 2014	None	

国际检索报告

国际申请号

PCT/CN2018/105504

A. 主题的分类

H04W 60/00(2009.01)i; H04W 76/00(2018.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W H04L H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPODOC, 3GPP:附着, 请求, 接受, 完成, 完整性, 校验, 加密, 密钥, 随机数, 身份, 标识, attach+, request+, complet+, integrality, encrypt+, checkout, decrypt+, key, random number, identity

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 104852994 A (普天信息技术研究院有限公司) 2015年 8月 19日 (2015 - 08 - 19) 说明书第[0065]-[0098]段	1-24
A	CN 102333386 A (大唐移动通信设备有限公司) 2012年 1月 25日 (2012 - 01 - 25) 全文	1-24
A	EP 2713664 A1 (ALCATEL LUCENT) 2014年 4月 2日 (2014 - 04 - 02) 全文	1-24
A	ERICSSON. "Corrections to EASE" 3GPP TSG-SA WG3 Meeting #84 S3-161180, 2016年 7月 29日 (2016 - 07 - 29), 全文	1-24

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 11月 17日

国际检索报告邮寄日期

2018年 11月 28日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

田琳琳

电话号码 86-(10)-53961736

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/105504

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	104852994	A	2015年 8月 19日	无	
CN	102333386	A	2012年 1月 25日	无	
EP	2713664	A1	2014年 4月 2日	无	