

(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
2025 年 6 月 12 日 (12.06.2025)



(10) 国际公布号
WO 2025/119355 A1

(51) 国际专利分类号:
H04W 12/037 (2021.01) **H04W 12/03** (2021.01)

(21) 国际申请号: PCT/CN2024/137563

(22) 国际申请日: 2024 年 12 月 6 日 (06.12.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311673987.9 2023 年 12 月 7 日 (07.12.2023) CN

(71) 申请人: 维沃移动通信有限公司(VIVO MOBILE COMMUNICATION CO., LTD.) [CN/CN]; 中国广东省东莞市长安镇维沃路 1 号 523863 (CN)。

(72) 发明人: 谢振华(XIE, Zhenhua); 中国广东省东莞市长安镇维沃路 1 号 523863 (CN)。林志鹏(LIN, Zhipeng); 中国广东省东莞市长安镇维沃路 1 号

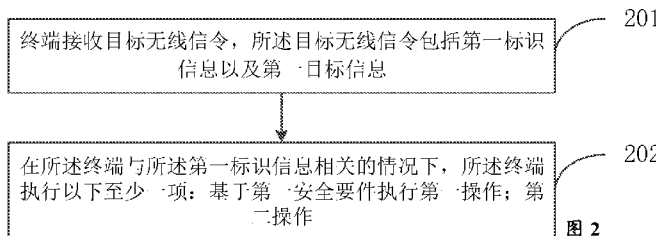
523863 (CN)。姜炜(JIANG, Wei); 中国广东省东莞市长安镇维沃路 1 号 523863 (CN)。

(74) 代理人: 北京励诚知识产权代理有限公司(BEIJING LISENG IP ATTORNEYS, CO., LTD.); 中国北京市丰台区汽车博物馆东路 1 号院诺德中心 6 号楼 702 100160 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) Title: INTERACTION METHOD, APPARATUS AND SYSTEM, TERMINAL AND NETWORK SIDE DEVICE

(54) 发明名称: 交互方法、装置、系统、终端及网络侧设备



- 201 A terminal receives target wireless signaling, wherein the target wireless signaling comprises first identification information and first target information
- 202 When the terminal is associated with the first identification information, the terminal performs at least one of the following: performing a first operation on the basis of a first security element, and a second operation

(57) Abstract: The present application relates to the technical field of communications, and discloses an interaction method, apparatus and system, a terminal and a network side device. The interaction method of an embodiment of the present application comprises: a terminal receiving target wireless signaling, wherein the target wireless signaling comprises first identification information and first target information, and the first target information comprises at least one of encrypted information and integrity protection information; and when the terminal is associated with the first identification information, executing at least one of the following: decrypting the encrypted information, performing confidentiality processing on the encrypted information, performing confidentiality processing on the first target information, checking or verifying the integrity protection information, performing security processing on the first target information, performing integrity checking or integrity processing on the first target information, performing integrity checking or integrity processing on the basis of the integrity protection information, generating a second security element, sending first information to an access network node, sending to an access network node first information carrying a third security parameter, and receiving second information from an access network node.



(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

(57) 摘要: 本申请公开了一种交互方法、装置、系统、终端及网络侧设备, 属于通信技术领域, 本申请实施例的交互方法包括: 终端接收目标无线信令, 目标无线信令包括第一标识信息以及第一目标信息, 第一目标信息包括加密信息与完整性保护信息中的至少一项; 在终端与第一标识信息相关的情况下执行以下至少一项: 解密加密信息; 对加密信息进行机密性处理; 对第一目标信息进行机密性处理; 校验或验证完整性保护信息; 对第一目标信息进行安全处理; 对第一目标信息进行完整性校验或完整性处理; 基于完整性保护信息进行完整性校验或完整性处理; 生成第二安全要件; 向接入网节点发送第一信息; 向接入网节点发送携带第三安全参数的第一信息; 从接入网节点接收第二信息。

交互方法、装置、系统、终端及网络侧设备

相关申请的交叉引用

本申请要求于 2023 年 12 月 07 日提交中国专利局、申请号为 202311673987.9、发明名称为“交互方法、装置、系统、终端及网络侧设备”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

本申请属于通信技术领域，具体涉及一种交互方法、装置、系统、终端及网络侧设备。

背景技术

随着通信技术的发展，在通信系统中，为了提高数据传输的效率，终端可以在不进入连接态的情况下，和网络侧设备进行终端专属数据（UE dedicate data）的收发，即小数据传输（Small Data Transmission, SDT）。目前小数据传输主要包括在终端触发的上行消息 3（Msg3）或者配置授权（Configured Grant, CG）的物理上行共享信道（Physical Uplink Shared Channel, PUSCH）上传输的移动终端发起的小数据传输（Mobile Originated SDT, MO-SDT）或者下行触发的移动终端终止的小数据传输（Mobile Terminated SDT, MT-SDT）。这样，仍然需要终端和网络侧设备进行多次消息交互，才能完成小数据的交互，这样将会导致小数据传输的时延较大。

发明内容

本申请实施例提供一种交互方法、装置、系统、终端及网络侧设备，能够解决小数据传输的时延较大问题。

第一方面，提供了一种交互方法，包括：

终端接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述

述第一目标信息包括加密信息与完整性保护信息中的至少一项；

在所述终端与所述第一标识信息相关的情况下，所述终端执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

向接入网节点发送携带第三安全参数的第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网

相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数；所述第二安全要件包括密钥和密流中的至少一项。

第二方面，提供了一种交互方法，包括：

5 接入网节点发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

其中，所述加密信息和完整性保护信息基于第一安全要件生成，所述第一安全要件包括密钥和密流中的至少一项。

第三方面，提供了一种交互方法，包括：

10 核心网节点向接入网节点发送第三信息或目标数据，所述第三信息包括第二标识信息和第二目标信息；

其中，所述第二目标信息包括以下至少一项：

第一安全要件或第三安全要件；

第一算法信息；

第二安全参数；

15 第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项；所述第一安全要件包括密钥和密流中的至少一项，所述第三安全要件包括密钥和密流中的至少一项，所述第二标识信息指示终端，或由终端标识生成，或指示一组终端。

第四方面，提供了一种交互方法，包括：

20 接入网节点发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项，其中，所述加密信息和完整性保护信息基于第一安全要件生成；

终端接收所述目标无线信令；

在所述终端与所述第一标识信息相关的情况下，所述终端执行以下至少一项：

25 基于第一安全要件执行第一操作；

第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

30 对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

35 基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

向接入网节点发送携带第三安全参数的第一信息；

40 从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信息、和终端接入网上下文中的信息；所述第四派生信息
45 包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信

息、终端接入网上下文中的信息、和所述第三安全参数；所述第二安全要件包括密钥和密流中的至少一项。

第五方面，提供了一种交互装置，包括：

第一接收模块，用于接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

第一执行模块，用于执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息和所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述第二安全要件包括密钥和密流中的至少一项。

第六方面，提供了一种交互装置，包括：

第一发送模块，用于发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

其中，所述加密信息和完整性保护信息基于第一安全要件生成，所述第一安全要件包括密钥和密流中的至少一项。

第七方面，提供了一种交互装置，包括：

第二发送模块，用于向接入网节点发送第三信息或目标数据，所述第三信息包括第二标识信息和第二目标信息；

其中，所述第二目标信息包括以下至少一项：

第一安全要件或第三安全要件；

第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项；所述第一安全要件包括密钥和密流中的至少一项，所述第三安全要件包括密钥和密流中的至少一项，所述第二标识信息指示终端。

第八方面，提供了一种交互系统，包括：接入网节点和终端，其中，

所述接入网节点用于发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项，其中，所述加密信息和完整性保护信息基于第一安全要件生成；

所述终端用于接收所述目标无线信令；并在所述终端与所述第一标识信息相关的情况

下，执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

其中，所述第一操作包括以下至少一项：

5 解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

10 对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

15 向接入网节点发送第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息和所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信息、和终端接入网上下文中的信息；
20 所述第二安全要件包括密钥和密流中的至少一项。

第九方面，提供了一种终端，该终端包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第一方面所述的方法的步骤。

25 第十方面，提供了一种终端，包括处理器及通信接口，其中，所述通信接口用于接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

30 其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

35 对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

40 基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息和所述第四派生信息包括以下至少一项：核心网相关密
45 钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述第二安全要件包括密钥和密流中的至少一项。

第十一方面，提供了一种网络侧设备，该网络侧设备包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第二方面所述的方法的步骤，或实现如第三方面所述的方法的步骤。

第十二方面，提供了一种网络侧设备，包括处理器及通信接口，其中，所述通信接口用于发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；其中，所述加密信息和完整性保护信息基于第一安全要件生成，所述第一安全要件包括秘钥和密流中的至少一项

或者，所述通信接口用于向接入网节点发送第三信息或目标数据，所述第三信息包括第二标识信息和第二目标信息；

其中，所述第二目标信息包括以下至少一项：

第一安全要件或第三安全要件；

第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项；所述第一安全要件包括秘钥和密流中的至少一项，所述第三安全要件包括秘钥和密流中的至少一项，所述第二标识信息指示终端。

第十三方面，提供了一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如第一方面所述的方法的步骤，或者实现如第二方面所述的方法的步骤，或者实现如第三方面所述的方法的步骤。

第十四方面，提供了一种无线通信系统，包括：终端及网络侧设备，所述终端可用于执行如第一方面所述的方法的步骤，所述网络侧设备可用于执行如第二方面和第三方面所述的方法的步骤。

第十五方面，提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如第一方面所述的方法，或实现如第二方面所述的方法，或者实现如第三方面所述的方法的步骤。

第十六方面，提供了一种计算机程序/程序产品，所述计算机程序/程序产品被存储在存储介质中，所述程序/程序产品被至少一个处理器执行以实现如第一方面所述的方法，或实现如第二方面所述的方法，或者实现如第三方面所述的方法的步骤。

本申请实施例通过终端接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；在所述终端与所述第一标识信息相关的情况下，所述终端执行第一操作和第二操作中的至少一项。这样可以基于目标无线信令完成下行数据或信令的传输，或者在目标无线信令之后终端与网络侧设备的第一条交互信息中即可实现数据或信令的传输；因此，本申请实施例降低了数据传输时延。

附图说明

图1是本申请实施例可应用的一种无线通信系统的框图；

图2是本申请实施例提供的交互方法流程图之一；

图3是本申请实施例提供的交互方法流程图之二；

图4是本申请实施例提供的交互方法流程图之三；

图5是本申请实施例提供的交互方法流程图之四；

图6是本申请实施例提供的交互方法流程图之五；

图7是本申请实施例提供的交互装置结构示意图之一；

图8是本申请实施例提供的交互装置结构示意图之二；

图9是本申请实施例提供的交互装置结构示意图之三；

图 10 是本申请实施例提供的通信设备的结构示意图；

图 11 是本申请实施例提供的终端的结构示意图；

图 12 是本申请实施例提供的一种网络侧设备的结构示意图；

图 13 是本申请实施例提供的另一种网络侧设备的结构示意图。

5

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本申请保护的范围。

10 本申请的术语“第一”、“第二”等是用于区别类似的对象，而不用来描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，以便本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施，且“第一”、“第二”所区别的对象通常为

15 一类，并不限定对象的个数，例如第一对象可以是一个，也可以是多个。此外，本申请中的“或”表示所连接对象的至少其中之一。例如“A 或 B”涵盖三种方案，即，方案一：包括 A 且不包括 B；方案二：包括 B 且不包括 A；方案三：既包括 A 又包括 B。字符“/”一般表示前后

20 值得指出的是，本申请实施例所描述的技术不限于长期演进型（Long Term Evolution, LTE）/LTE 的演进（LTE-Advanced, LTE-A）系统，还可用于其他无线通信系统，诸如码分多址（Code Division Multiple Access, CDMA）、时分多址（Time Division Multiple Access, TDMA）、频分多址（Frequency Division Multiple Access, FDMA）、正交频分多址（Orthogonal Frequency Division Multiple Access, OFDMA）、单载波频分多址（Single-carrier Frequency Division Multiple Access, SC-FDMA）或其他系统。本申请的术语“系统”和“网络”常被可互

25 换地使用，所描述的技术既可用于以上提及的系统 and 无线电技术，也可用于其他系统和无线电技术。以下描述出于示例目的描述了新空口（New Radio, NR）系统，并且在以下大部分描述中使用 NR 术语，但是这些技术也可应用于 NR 系统应用以外的系统，如第 6 代（6th Generation, 6G）通信系统。

图 1 示出本申请实施例可应用的一种无线通信系统的框图。无线通信系统包括终端 11 和网络侧设备 12。其中，终端 11 可以是手机、平板电脑（Tablet Personal Computer）、膝上型电脑（Laptop Computer）、笔记本电脑、个人数字助理（Personal Digital Assistant, PDA）、掌上电脑、上网本、超级移动个人计算机（Ultra-mobile Personal Computer, UMPC）、移动上网装置（Mobile Internet Device, MID）、增强现实（Augmented Reality, AR）、虚拟现实（Virtual Reality, VR）设备、机器人、可穿戴式设备（Wearable Device）、飞行器（flight vehicle）、车载设备（Vehicle User Equipment, VUE）、船载设备、行人终端（Pedestrian User Equipment, PUE）、智能家居（具有无线通信功能的家居设备，如冰箱、电视、洗衣机或者家具等）、游戏机、个人计算机（Personal Computer, PC）、柜员机或者自助机等终端侧设备。可穿戴式设备包括：智能手表、智能手环、智能耳机、智能眼镜、智能首饰（智能手镯、智能手链、智能戒指、智能项链、智能脚镯、智能脚链等）、智能腕带、智能服装等。其中，车载设备也可以称为车载终端、车载控制器、车载模块、车载部件、车载芯片或车载单元等。需要说明的是，在本申请实施例并不限定终端 11 的具体类型。网络侧设备 12 可以包括接入网系统或核心网设备，其中，接入网系统也可以称为无线接入网（Radio Access Network, RAN）设备、无线接入网功能或无线接入网单元。接入网系统可以包括基站、无线局域网（Wireless Local Area Network, WLAN）接入点（Access Point, AP）或无线保真（Wireless Fidelity, WiFi）节点等。其中，基站可被称为节点 B（Node B, NB）、演进节点 B（Evolved Node B, eNB）、下一代节点 B（the next generation Node B, gNB）、新空口节点 B（New Radio Node B, NR Node B）、接入点、中继站（Relay Base Station, RBS）、服务基站（Serving Base Station, SBS）、基收发机站（Base Transceiver Station,

30

35

40

45

BTS)、无线电基站、无线电收发机、基本服务集(Basic Service Set, BSS)、扩展服务集(Extended Service Set, ESS)、家用B节点(home Node B, HNB)、家用演进型B节点(home evolved Node B)、发送接收点(Transmission Reception Point, TRP)或所属领域中其他某个合适的术语,只要达到相同的技术效果,所述基站不限于特定技术词汇,需要说明的是,在本申请实施例中仅以NR系统中的基站为例进行介绍,并不限定基站的具体类型。

核心网设备可以包含但不限于如下至少一项:核心网节点、核心网功能、移动管理实体(Mobility Management Entity, MME)、接入移动管理功能(Access and Mobility Management Function, AMF)、会话管理功能(Session Management Function, SMF)、用户平面功能(User Plane Function, UPF)、策略控制功能(Policy Control Function, PCF)、策略与计费规则功能单元(Policy and Charging Rules Function, PCRF)、边缘应用服务发现功能(Edge Application Server Discovery Function, EASDF)、统一数据管理(Unified Data Management, UDM)、统一数据仓储(Unified Data Repository, UDR)、归属用户服务器(Home Subscriber Server, HSS)、集中式网络配置(Centralized network configuration, CNC)、网络存储功能(Network Repository Function, NRF)、网络开放功能(Network Exposure Function, NEF)、本地NEF(Local NEF, 或 L-NEF)、绑定支持功能(Binding Support Function, BSF)、应用功能(Application Function, AF)等。需要说明的是,在本申请实施例中仅以NR系统中的核心网设备为例进行介绍,并不限定核心网设备的具体类型。

为了方便理解,以下对本申请实施例涉及的一些内容进行说明:

一、小数据传输(Small Data Transmission, SDT)。

高效小数据传输的特点是针对非无线资源控制(Radio Resource Control, RRC)连接态的终端(UE),避免因此引起的RRC状态转换和RRC连接建立过程的造成过多信令开销,通过极简单的信令过程即完成小数据传输的目的。其中,非RRC连接态可以包括空闲态(IDLE)和非激活(INACTIVE)态。

小数据传输方案的特点是UE当前数据无线承载(Data Radio Bearer, DRB)都是处于挂起的状态,而不是释放的状态。因而,UE在发送恢复请求(ResumeRequest)消息前可以先恢复DRB,然后再用RRC信令来捎带小数据,这时和连接(CONNECTED)态UE一样可以在DRB上传输数据。从而避免进行状态转换,以较小的信令开销达到高效小数据传输的目的。

小数据传输由于使用的是DRB传输,接入层面(Attached Storage, AS)安全已经激活,因此小数据传输可以对数据进行必要的安全保护,例如数据加密和完整性保护等操作。从安全角度,由于UE在挂起状态有可能已经移动到其它的基站下,因此此时UE重新发包所使用的安全密钥是需要更新的。更新的方法就按照UE在进入挂起状态时,网络侧设备提供给它的用于计算下一跳密钥的参数,进行下一个密钥的更新操作。

小数据传输的待传数据在专用业务信道(Dedicated Traffic Channel, DTCH)上承载,与上行RRCConnectionResumeRequest消息进行复用之后进行传输。类似的,如果有回复的下行消息,也可以在DTCH上承载,与下行RRCConnectionRelease消息复用传输。上下行的数据都是加密的,使用更新后的下一个密钥进行加密操作。

可选地,可以基于4步(4-step)随机接入信道(Random Access Channel, RACH)过程中的Msg3 PUSCH上传输小数据。小数据还可以在2-step RACH过程中MsgA PUSCH上传输,或者在RRC inactive状态下配置的配置授权(configured grant, CG)调度的PUSCH资源上传输。在2-step RACH和4-step RACH过程中的小数据传输称之为基于RACH(RACH based)小数据传输,基于configured grant调度的PUSCH的小数据传输称为CG based小数据传输。

二、移动终止的早期数据传输(Mobile Terminated Early Data Transmission, MT-EDT)。

在LTE系统中,网络(Network, NW)会通过寻呼(paging)消息携带MT-EDT触发

消息,随后 UE 发起 EDT 过程, NW 在接收到 UE 的请求消息(携带 MT-EDT 的原因值)后,把 RRC 响应消息串接上 DRB 数据,一并成一个协议数据单元,发送给 UE,最终实现下行业务的接收。

Idle 态或 inactive 态下的数据传输是一种特殊的传输机制,其允许 UE 在不进入连接态的情况下,和 NW 侧进行 UE 专属数据(UE dedicate data)收发。目前小数据传输主要在终端促发的上行 Msg3 或者 CG PUSCH 上传输的 MO-SDT,或者下行促发的 MT-SDT。如何在寻呼消息中数据传输或者调度数据传输尚未有对应的方案。为此,提出了本申请的交互方法,即通过 paging 等 UE 能接收到的第一条广播信号,直接将数据或数据传输资源递交给 UE,减少了消息交互过程。

下面结合附图,通过一些实施例及其应用场景对本申请实施例提供的交互方法进行详细地说明。

参照图 2,本申请实施例提供了一种交互方法,如图 2 所示,该交互方法包括:

步骤 201,终端接收目标无线信令,所述目标无线信令包括第一标识信息以及第一目标信息,所述第一目标信息包括加密信息与完整性保护信息中的至少一项;

步骤 202,在所述终端与所述第一标识信息相关的情况下,所述终端执行以下至少一项:

基于第一安全要件执行第一操作;

第二操作;

其中,所述第一操作包括以下至少一项:

解密所述加密信息;

对所述加密信息进行机密性处理;

对所述第一目标信息进行机密性处理;

校验或验证所述完整性保护信息;

对所述第一目标信息进行安全处理;

对所述第一目标信息进行完整性校验或完整性处理;

基于所述完整性保护信息,对以下至少一项进行完整性校验或完整性处理:所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果;

其中,所述第二操作包括以下至少一项:

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件;

向接入网节点发送第一信息;

向接入网节点发送携带第三安全参数的第一信息;

从接入网节点接收第二信息;

其中,所述第一安全要件基于第一派生信息生成,所述第一安全要件包括密钥和密流中的至少一项;所述第一派生信息包括以下至少一项:核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥;所述第四派生信息包括以下至少一项:核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数;所述第二安全要件包括密钥和密流中的至少一项。

本申请实施例中,上述第一标识信息可以理解为目标标识或对目标标识截取的一部分标识,该目标标识可以包括用户标识、组标识、连接标识、承载标识、事物标识和交互标识中的至少一项。

可选地,上述加密信息可以理解为对待传输的内容中的至少部分内容进行安全性处理后得到的信息,上述完整性保护信息可以理解为与待传输的内容关联的完保信息,为媒体接入控制(Medium Access Control, MAC)值。在第一目标信息包括加密信息与完整性保护信息时,可以理解对传输的内容即进行安全处理,又进行了完整性处理,最终得到第一目标信息。

可选地，所述终端与所述第一标识信息相关可以理解为所述终端的相关标识与第一标识信息关联，例如，目标无线信令包括用户标识，在目标无线信令中包含的用户标识包括终端的用户标识的情况下，可以认为所述终端与所述第一标识信息相关，此时终端可以执行上述第一操作。

5 应理解，在所述终端与所述第一标识信息不相关的情况下，所述终端可以丢弃接收到的第一目标信息。

需要说明的是，上述目标无线信令可以理解为终端在空闲态或非激活态能够接收到的无线信令。在一些实施例中，在所述终端与所述第一标识信息相关的情况下，所述终端基于第一安全要件执行第一操作，这样无需其他交互信息即可实现下行数据或信令的传输，
10 从而可以降低数据传输时延。与此同时，由于第一目标信息包括加密信息与完整性保护信息中的至少一项，由终端第一安全要件执行第一操作，从而提高传输的安全性，在一些实施例中，在所述终端与所述第一标识信息相关的情况下，终端执行第二操作，从而可以在后续终端与网络侧设备的第一条交互信息中即可实现数据或信令的传输，从而可以降低数据传输时延。

15 可选地，解密所述加密信息后，可以获得接入网节点传输的内容，具体可以包括信令或数据。

可选地，上述密流（KeyStream）可以为基于密钥及其他参数生成的字符串。

可选地，上述核心网相关密钥可以包括长期密钥（Long Term Key）、认证相关密钥（Kausf）、安全及认证相关密钥（Kseaf）、AMF 密钥（Kamf）、移动管理实体（Mobility
20 Management Entity, MME）密钥（Kasme）等。

NAS 层相关密钥可以包括 NAS 加密密钥（Knas_enc）、NAS 完保密钥（Knas_int）等。

接入网相关密钥可以包括基站密钥（如 Kenb、Kgnb、NH、Kenb*、Kgnb*、Ks-enb、Ks-gnb 等）。

AS 层相关密钥可以包括信令加密密钥（Krrc_enc）、信令完保密钥（Krrc_int）、数据
25 加密密钥（Kup_enc）、数据完保密钥（Kup_int）等。

终端上下文中的密钥可以包括核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、和接入层面 AS 层相关密钥中的任意一个或至少两个组合成的密钥。

本申请实施例通过终端接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；在所述
30 终端与所述第一标识信息相关的情况下，所述终端执行第一操作和第二操作中的至少一项。这样可以基于目标无线信令完成下行数据或信令的传输，或者在目标无线信令之后终端与网络侧设备的第一条交互信息中即可实现数据或信令的传输；因此，本申请实施例降低了数据传输时延。

需要说明的是，接入网设备发送目标无线信令之前，所述接入网节点从核心网节点接
35 收第三信息或目标数据，所述第三信息包括第三标识信息和第二目标信息；

其中，所述第三信息包括第二标识信息和第二目标信息；

所述第二目标信息包括以下至少一项：

所述第一安全要件或第三安全要件，所述第三安全要件包括密钥和密流中的至少一项；
第一算法信息；

40 第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第二标识信息用于指示终端，或由终端标识生成，或指示一组终端，或与
所述第一标识信息相关。

本申请实施例中，所述接入网节点可以基于所述第二目标信息获知或生成所述第一安
45 全要件，并基于所述第三信息发送所述目标无线信令。

例如，在一些实施例中，所述接入网节点基于第二派生信息和所述安全要件派生算法

中的至少一项生成所述第一安全要件。其中，所述第二派生信息包括以下至少一项：接入网相关密钥、AS层相关密钥、终端上下文中的密钥、所述第一安全辅助信息中的至少部分内容、所述第二安全辅助信息中的至少部分内容、第一标识信息、和终端接入网上下文中的信息。

5 可选地，第二标识信息可以为全局用户临时标识（Globally Unique Temporary Identifier, GUTI），第一标识信息可以是 RNTI；或者第二标识信息是 GUTI，第一标识信息是短期移动用户识别标识（Short Term Mobile Subscriber Identity, S-TMSI）；或者第二标识信息和第一标识信息都是 S-TMSI。

10 可选地，上述目标数据可以理解为待传输数据，在一些实施例中，上述第三信息还可以包括上述目标数据。上述目标数据与上述加密信息或完整性保护信息关联，即接入网设备可以基于目标数据中的至少部分数据生成加密信息以及完整性保护信息。也就是说，通过目标无线信令可以传输部分数据，剩余部分的数据与第二信息关联，即可以基于剩余部分的数据生成第二信息。当然在一些实施例中，也可以不在目标无线信令中携带待传输数据，例如，上述加密信息为加密的资源信息，上述第二信息为加密的目标数据（或者为基于目标数据生成的加密数据）。

本申请实施例中，上述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

至少一对第二标识信息与第二目标信息；

其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

20 或者，所述第二标识信息与所述第二目标信息为一到零或一映射；

或者，K个第二标识信息与所有第二目标信息存在对应关系，且K小于或等于所述第三信息中包含的第二标识信息的数量。

25 本申请实施例中，第二目标信息与第二标识信息为一到一或多映射可以理解为：第二目标信息可以与第二标识信息存在一到一的映射关系，或者存在一到多的映射关系。例如，所有的第二目标信息与第二标识信息均为一到一映射；或所有的第二目标信息与第二标识信息均为一到多映射；或部分第二目标信息与第二标识信息为一到一映射，部分第二目标信息与第二标识信息为一到多映射。

30 第二标识信息与第二目标信息为一到零或一映射可以理解为：第二标识信息可以与第二目标信息存在一到一的映射关系，或者存在一到零的映射关系，其中一到零的映射关系表示第二标识信息不存在与之映射的第二目标信息。例如，所有的第二标识信息与第二目标信息均为一到一映射；或部分第二标识信息与第二目标信息为一到一映射，部分第二标识信息与第二目标信息为一到零映射。

35 可选地，对于K个第二标识信息与所有第二目标信息存在对应关系，在K等于所述目标无线信令包含的第二标识信息的数量的情况下，可以理解为所有的第二标识信息存在映射的第二目标信息；在K小于所述目标无线信令包含的第二标识信息的数量的情况下，可以理解为仅部分第二标识信息存在映射的第二目标信息，部分第二标识信息不存在映射的第二目标信息。其中，第二目标信息与第二标识信息的映射关系可以包括以下至少一项：一到一的映射关系；一到多的映射关系。

40 可选地，在一些实施例中，所述第二标识信息用于指示终端，或由终端标识生成，或指示一组终端，或与所述第一标识信息相关。

可选地，在一些实施例中，所述接入网节点执行以下至少一项：

基于安全要件派生算法生成所述第一安全要件；

基于第二派生信息生成所述第一安全要件；

基于机密性算法生成所述加密信息；

45 基于完整性算法生成所述完整性保护信息；

基于第一计算参数生成所述加密信息与所述完整性保护信息中的至少一项；

第三操作；

其中，所述第一计算参数包括以下至少一项：

终端接入网上下文中的信息；

所述第一标识信息；

5 第一安全辅助信息中的至少部分内容；

第二安全辅助信息中的至少部分内容；

第一算法信息；

所述第二派生信息包括以下至少一项：

接入网相关密钥；

10 接入层面 AS 层相关密钥；

终端上下文中的密钥；

第三安全要件；

终端接入网上下文中的信息；

所述第一标识信息；

15 第一安全辅助信息中的至少部分内容；

第二安全辅助信息中的至少部分内容；

第一算法信息；

所述第三操作包括以下至少一项：

20 基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件，所述第二安全要件包括密钥和密流中的至少一项，所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、AS 层相关密钥、和终端上下文中的密钥；

从终端接收第一信息；

向终端发送第二信息。

25 可选地，在接入网节点接收到第一信息后，可以对第一信息的至少部分内容进行安全处理，并上报给核心网节点。

可选地，核心网节点向接入网节点发送第一安全要件或第三安全要件之前，还可以基于第三派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件或所述第三安全要件；

30 其中，所述第三派生信息包括以下至少一项：核心网相关密钥、NAS 层相关密钥、终端上下文中的密钥、所述第一算法信息、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

35 需要说明的是，在本申请实施例中，上述核心网节点可以理解或替换为具有核心网功能的设备或系统，即可以称之为核心网设备或核心网系统，也可以称之为核心网功能。上述接入网节点可以理解为具有接入网功能的设备或系统，即可以称之为接入网设备或系统，也可以称之为基站或接入网功能。

可选地，在一些实施例中，所述第一目标信息还包括第一安全辅助信息；

其中，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项；

40 所述第一算法信息包括以下至少一项：

安全要件派生算法，所述第一安全要件还基于所述安全要件派生算法生成；

机密性算法和完整性算法中至少一项，所述第一操作还基于所述机密性算法和完整性算法中至少一项执行。

45 本申请实施例中，上述机密性算法可以包括加密算法和解密算法，上述完整性算法可以包括生成校验码的算法、或者包括校验或验证校验码的算法。

可选地，所述第一安全参数用于表示 NAS 的计数信息，例如下行 NAS 信令次数，或

上行 NAS 信令次数,或 NAS 信令次数(下行 NAS 信令次数与上行 NAS 信令次数的和值);
所述第二安全参数用于表示接入网信令的计数信息或数据报文的计数信息,例如第二安全
参数可以为下行接入网信令次数、上行接入网信令次数、或接入网信令次数(即下行接入
网信令次数与上行接入网信令次数的和值),也可以为下行数据报文数、上行数据报文数、
或数据报文数(即下行数据报文数和上行数据报文数)。上述第三安全参数可以理解为用
于表示接入网信令的计数信息或数据报文的计数信息,例如第二安全参数可以为下行接入
网信令次数、上行接入网信令次数、或接入网信令次数(即下行接入网信令次数与上行接
入网信令次数的和值),也可以为下行数据报文数、上行数据报文数、或数据报文数(即
下行数据报文数和上行数据报文数)。可选地,在一些实施例中,该第三安全参数与第二
安全参数不同。

应理解,上述下行 NAS 信令可以理解或替换为 NAS 下行信令,下行 NAS 信令可以理
解或替换为 NAS 下行信令。下行接入网信令可以理解或替换为 AS 下行信令,上行接入网
信令可以理解或替换为 AS 上行信令,接入网信令可以理解或替换为 AS 信令。数据报文可
以理解或替换为协议数据报文。

可选地,所述第一安全要件还基于所述安全要件派生算法生成可以理解为,第一安全
要件基于第一派生信息和接入网节点指示的安全要件派生算法生成。在一些实施例中,安
全要件派生算法也可以属于第一派生信息的内容,即所述第一安全要件还基于所述安全要
件派生算法生成可以理解为所述第一安全要件基于第一派生信息中除接入网节点指示的安
全要件派生算法之外的信息和接入网节点指示的安全要件派生算法生成第一安全要件。应
理解,在第一目标信息不包括安全要件派生算法的情况下,生成第一安全要件的安全要件
派生算法可以由协议约定。

可选地,在一些实施例中,所述第一派生信息还包括以下至少一项:

第一安全辅助信息中的至少部分内容;

终端核心网上下文中的信息;

终端接入网上下文中的信息;

所述第一标识信息。

可选地,在一些实施例中,所述终端基于第一安全要件执行第一操作,包括:

所述终端基于所述第一安全要件以及第一计算参数执行所述第一操作,所述第一计算
参数包括以下至少一项:

终端核心网上下文中的信息;

终端接入网上下文中的信息;

所述第一标识信息;

第一安全辅助信息中的至少部分内容。

本申请实施例中,第一计算参数包含的第一安全辅助信息中的至少部分内容可以与第
一派生信息中包含的第一安全辅助信息中的至少部分内容相同或不同,或部分相同。例如,
在一些实施例中,第一安全辅助信息包括两部分信息,其中一部分信息(如第一安全参数)
用于执行所述第一操作,另一部分(如第二安全参数)用于生成安全要件。

可选地,在一些实施例中,所述终端核心网上下文中的信息,包括以下至少一项:

终端的标识信息;

终端的组标识信息;

NAS 信令的计数信息;

NAS 上行信令的计数信息;

NAS 下信令的计数信息;

通过 NAS 传输的协议数据报文的计数信息;

通过 NAS 传输的上行协议数据报文的计数信息;

通过 NAS 传输的下行协议数据报文的计数信息;

或, 所述终端接入网上下文中的信息, 包括以下至少一项:

终端的标识信息;

终端的组标识信息;

AS 信令的计数信息;

5 AS 上行信令的计数信息;

AS 下行信令的计数信息;

协议数据报文的计数信息;

上行协议数据报文的计数信息;

下行协议数据报文的计数信息。

10 可选地, 在一些实施例中, 所述方法包括以下至少一项:

所述终端基于以下至少一项生成所述第二安全要件: 所述第一安全要件、所述第四派生信息、和所述第三安全参数;

所述终端基于以下至少一项, 对所述第一信息或所述第一信息中的部分内容进行安全保护: 所述第一安全要件或所述第二安全要件, 第一计算参数, 和所述第三安全参数;

15 所述终端基于以下至少一项, 对所述第二信息或所述第二信息中的部分内容进行安全处理: 所述第一安全要件或所述第二安全要件, 第一计算参数, 和所述第三安全参数。

在一些实施例中, 在第一信息包括第三安全参数的情况下, 上述第二安全要件基于第三安全参数或第三安全参数与其他相关信息生成, 与此同时安全处理基于第三安全参数或第三安全参数与其他相关信息执行。该第三安全参数可以理解为用于更新安全要件和安全处理的信息, 由于可以基于第三安全参数更新使用的安全要件和安全处理, 从而提高了传输的安全性。

20 在一些实施例中, 第一信息不包括第三安全参数的情况下, 所述终端基于以下至少一项生成所述第二安全要件: 所述第一安全要件, 所述第四派生信息。所述终端基于以下至少一项, 对所述第二信息或所述第二信息中的部分内容进行安全处理: 所述第一安全要件或所述第二安全要件, 第一计算参数。

需要说明的是, 在本申请实施例中, 所述安全保护包括机密性保护、加密、和完整性保护中的至少一项; 所述安全处理包括解密、机密性处理、完整性处理、完整性校验中的至少一项。

可选地, 在一些实施例中, 所述目标无线信令包括以下至少一项:

30 至少一个第一标识信息和至少一个第一目标信息;

至少一对第一标识信息与第一目标信息;

其中, 第一目标信息与第一标识信息为一到一或多映射;

或者, 第一标识信息与第一目标信息为一到零或一映射;

35 或者, N 个第一标识信息与所有第一目标信息存在对应关系, 且 N 小于或等于所述目标无线信令中包含的第一标识信息的数量。

本申请实施例中, 第一目标信息与第一标识信息为一到一或多映射可以理解为: 第一目标信息可以与第一标识信息存在一到一的映射关系, 或者存在一到多的映射关系。例如, 所有的第一目标信息与第一标识信息均为一到一映射; 或所有的第一目标信息与第一标识信息均为一到多映射; 或部分第一目标信息与第一标识信息为一到一映射, 部分第一目标信息

40 信息与第一标识信息为一到多映射。
第一标识信息与第一目标信息为一到零或一映射可以理解为: 第一标识信息可以与第一目标信息存在一到一的映射关系, 或者存在一到零的映射关系, 其中一到零的映射关系表示第一标识信息不存在与之映射的第一目标信息。例如, 所有的第一标识信息与第一目标信息均为一到一映射; 或部分第一标识信息与第一目标信息为一到一映射, 部分第一标识信息

45 信息与第一目标信息为一到零映射。
可选地, 对于 N 个第一标识信息与所有第一目标信息存在对应关系, 在 N 等于所述目

标无线信令包含的第一标识信息的数量的情况下，可以理解为所有的第一标识信息存在映射的第一目标信息；在N小于所述目标无线信令包含的第一标识信息的数量的情况下，可以理解为仅部分第一标识信息存在映射的第一目标信息，部分第一标识信息不存在映射的第一目标信息。其中，第一目标信息与第一标识信息的映射关系可以包括以下至少一项：

一到一的映射关系；一到多的映射关系。

可选地，在一些实施例中，所述终端为空闲态或非激活态，或在发送所述第一信息前为空闲态或非激活态，或在接收所述第二信息前为空闲态或非激活态。

本申请实施例中，空闲态包括核心网空闲态和无线空闲态两种情况，核心网空闲态指终端的一种状态，该状态下核心网不能直接发送以该终端为目标的NAS消息（必须先寻呼），或终端不能直接向核心网发送NAS消息（必须先获得相应的发送资源），也可称终端与核心网间无NAS连接，无线空闲态指终端没有资源向基站发送信令建立终端与基站间的无线点对点连接（有终端的专有无线资源来收发信息，包括专有扰码资源，比如无线网络临时标识（Radio Network Temporary Identifier, RNTI）；非激活态指终端的一种状态，该状态下终端非核心网空闲态，核心网与基站之间有针对性针对终端的连接或隧道，但终端和基站之间没有无线点对点连接。终端的状态还可以使用其他名称定义，终端和基站之间有其他行为，比如终端和基站之间有无线点对点连接，但核心网不能直接发送以终端为目标的NAS消息，这种状态可能会使用新名称，但仍对应于本申请的空闲态（即核心网空闲态）描述，比如终端非核心网空闲态（可以直接发送以终端为目标的NAS消息），终端和基站之间没有无线点对点连接，但核心网和基站之间没有针对性针对终端的连接（比如上行或下行NAS消息基于UE ID标识源或目标，而非基于连接或隧道标识（Tunnel endpoint identifier, TEID）），这种状态可以采用其他名称定义，但仍对应与本申请的非激活态描述。例如，有NAS连接但终端到基站再到核心网之间的连接不完整。

可选地，在本申请实施例中，在终端进入到非激活态后，到接收所述目标无线信令之前，所述终端未向所述接入网系统发送信息。

可选地，在一些实施例中，所述终端接收目标无线信令之前，所述方法还包括：

所述终端向网络侧发送第二算法信息，所述第二算法信息用于指示以下至少一项：所述终端支持的算法、所述终端使用的算法；

其中，所述算法包括安全要件派生算法、机密性算法、和完整性算法中至少一项。

本申请实施例中，所述终端向网络侧发送第二算法信息可以理解为所述终端向核心网节点发送NAS消息，该NAS消息可以包括上述第二算法信息。进一步的，接入网节点转发NAS消息给核心网节点时，可以携带接入网节点支持的算法和接入网节点使用的算法中的至少一项。

可选地，核心网节点接收到第二算法信息后可以向接入网节点指示第一算法信息。

可选地，在一些实施例中，所述第一标识信息指示终端，或者由终端标识生成，或者指示一组终端。

本申请实施例中，在第一标识信息由终端标识生成的情况下，不同终端标识可以生成相同的第一标识信息，例如，一组终端的终端标识可以生成相同的第一标识信息。

可选地，在一些实施例中，所述目标无线信令包括广播信令、寻呼信令、无线短消息、和系统消息中的任一项；

或者，所述目标无线信令通过寻呼信道（Paging Channel, PCH）、多播信道（Multicast Channel, MCH）、广播信道（Broadcast Channel, BCH）和下行共享信道（Downlink Shared Channel, DL-SCH）中的至少一项发送；

或者，所述目标无线信令通过物理下行控制信道（Physical downlink control channel, PDCCH）、物理下行共享信道（Physical downlink shared channel, PDSCH）、物理广播信道（Physical broadcast channel, PBCH）和物理多播信道（Physical Multicast Channel, PMCH）中的至少一项发送。

本申请实施例中,上述目标无线信令可以通过 PCH 发送的新格式的 paging 消息(即包含资源信息和/或数据的 paging 消息),可以是 PCH 中发送的信令,该目标无线信令包含传统的 paging 消息(即不包含资源信息和数据的 paging 消息),以及资源信息和/或数据,还可以是 PCH 中发送传统的 paging 消息,以及通过 PDCCH 发送资源信息和/或 PDSCH 发送数据。

可选地,上述无线短消息可以理解为无线信令涉及的短消息(Short Message),并非是短信服务(Short Messaging/Message Service, SMS)中涉及的短消息。

为了更好的理解本申请,以下通过一些示例进行详细说明。

实施例一,在终端处于 idle 态下,交互的流程如图 3 所示,具体包括以下步骤:

步骤 31,终端向核心网发送 NAS 消息,接入网节点转发 NAS 消息给核心网节点时,携带终端支持的算法指示信息(即第二算法信息),也可以进一步携带接入网节点支持的算法指示信息,核心网节点可选地保存终端支持的算法指示信息,或终端和接入网节点支持的算法指示信息。

步骤 32,核心网节点向接入网节点发送信息 1,例如可以通过 Paging 消息或激励消息发送。

其中,信息 1 中包括第一用户标识、安全要件(包括秘钥和密流中的至少一项),该安全要件可以基于终端核心网上下文中的密流、第一用户标识和第一安全参数中的至少一项生成。可选地,信息 1 中还可以包括第一安全参数和算法指示中的至少一项,该算法指示用于指示第一算法信息。

可选地,信息 1 中除第一用户标识以外的其他信息中至少部分信息可以与第一用户标识关联,从而可以携带多个第一用户标识关联的其他信息。当然在其他实施例中,也可以设置信息 1 中除第一用户标识以外的其他信息中至少部分信息与第一用户标识。

步骤 33,接入网节点可以基于信息 1 执行操作 1,该操作 1 包括加密操作和完保操作中的至少一项。

对于加密操作:使用秘钥或密流对资源信息(如 SRB 信息、DRB 信息、MAC CE 调度信息、grant 信息等)和其他信元(如目标无线信令中的数据)中的至少一项进行加密(例如使用密流以及约定或指示的算法加密,或使用密流进行异或操作),资源信息可以包括上行资源信息和下行资源信息中的至少一项;其中,在安全要件包括秘钥的情况下,加密的行为可以基于第一用户标识、第二用户标识、第一安全参数和第二安全参数中的至少一项执行。

其中,第二用户标识可以基于第一用户标识生成,例如第一用户标识是核心网节点分配的用户标识(如 TMSI),第二用户标识为接入网节点分配的用户标识(如 RNTI),或者第一用户标识是接入网节点分配的用户标识,第二用户标识为核心网节点分配的用户标识。

对于完保操作:在安全要件包括秘钥的情况下,对资源信息、加密的资源信息和其他信元(如目标无线信令中的数据)中的至少一项进行完保操作;例如使用密流以及约定或指示的算法计算 MAC 值,可选地,完保操作还可以基于第一安全参数和第二安全参数中的至少一项执行,即计算 MAC 值是将第一安全参数和第二安全参数中的至少一项作为算法的输入。

可选地,在一些实施例中,在算法指示不支持的情况下,则不执行步骤 33 以及后续步骤。

步骤 34,接入网节点通过空口广播信息 2,例如通过 Paging 消息、系统消息、或激励消息等进行发送。或者在向终端发送的第一条消息中发送信息 2。

该信息 2 包括第一用户标识或第二用户标识以及以下至少一项:加密的资源信息和 MAC 值。

可选地,上述信息 2 中除用户标识(第一用户标识或第二用户标识)以外的其他信息

可以与用户标识关联,从而可以携带多个用户标识关联的其他信息。当然在其他实施例中,上述信息 2 中除用户标识以外的其他信息可以与用户标识无关。

可选地,信息 2 中还可以包括算法指示、第一安全参数和第二安全参数中的至少一项。这些信息中的至少部分可以与用户标识无关或相关。

5 需要说明的是,上述信息 2 中除用户标识由承载信息 2 的消息携带,其他信息可以是在消息中携带,也可以是在承载消息的信令(如 RLC 层信令、MAC 层信令)中携带。

至此,终端和接入网节点之间完成安全激活,后续的消息和数据交互可以进行安全保护。

10 步骤 35,终端生成安全要件(该安全要件包括密钥或密流中的至少一项,安全要件的生成方式与步骤 32 相同,在此不再赘述)并执行操作 2,操作 2 包括解密操作和完保校验操作中的至少一项。

15 对于解密操作,使用密钥或密流对资源信息进行解密(例如使用密钥以及约定或指示的算法解密,或基于密流进行异或操作)。在安全要件包括密钥的情况下,还可以使用接收到的用户标识、基于接收到的用户标识获得的第三用户标识(比如收到 RNTI 获得 TMSI,或反之)、第一安全参数和第二安全参数执行上述解密操作(即解密时还将相关参数作为输入参数)。

20 对于完保校验操作,在安全要件包括密钥的情况下,对资源信息和/或加密的资源信息进行完保校验(例如使用密钥以及约定或指示的算法计算目标 MAC 值并与接收到的 MAC 进行比较),完保校验还可以使用接收到的用户标识、基于接收到的用户标识获得的第三用户标识、第一安全参数 1 和第二安全参数中的至少一项(即计算目标 MAC 值的过程中还将相关参数作为输入)。

25 可选地,在步骤 35 之后,终端还可以基于终端核心网上行文或接入网上下文中的密钥生成新的安全要件(比如使用相应密钥以及约定的参数和/或接收到的接入网节点发送的信息生成新的安全要件)。终端基于资源信息(比如上行资源信息)向基站发送信令和/或数据,可以基于前述完保校验执行发送信令和/或数据的过程,比如完保校验成功后发送。信令中可以包括以下至少一项:

基于安全要件或新的安全要件中的密钥或密流加密的信令整体或信令中的部分信元(使用密钥以及约定或指示的算法加密,或使用密流进行异或操作);

30 在安全要件或新的安全要件包括密钥的情况下,对信令整体(明文信令整体)、加密的信令整体、信令中的部分信元(明文信元)、或信令中的部分加密信元进行完保操作后的信息(使用密钥以及约定或指示的算法计算出的 MAC 值)。

发送数据可以是基于安全要件或新的安全要件中的密钥或密流加密后的数据,也可以是基于安全要件或新的安全要件中的密钥完保后的数据,也可以是基于安全要件或新的安全要件中的密钥加密和完保后的数据。

35 可选地,在安全要件或新的安全要件包括密钥的情况下,上述加密和/或完保操作还可以基于接收到的用户标识、基于接收到的用户标识获得的第三用户标识、第一安全参数、第二安全参数 2 和第三安全参数中的至少一项执行。

40 在使用了安全参数 3 的情况下,发送的信令或数据可以包括明文的安全参数 3(安全参数 3 作为信令整体的一部分,或数据的一部分,或部分信元中的一个,但不是加密后的信令整体,也不是部分加密信元中的一个)。

可选地,接入网节点可以基于终端接入网上下文中的密钥或从核心网节点收到的安全要件生成新的安全要件(比如使用相应密钥以及约定的参数和/或接入网节点发送给终端的信息生成新的安全要件)。接入网节点基于资源信息(比如上行资源信息)从终端接收信令和/或数据。

45 可选地,接入网节点对信令执行以下至少一项:

基于安全要件或新的安全要件中的密钥或密流解密信令或信令中的部分信元;

基于安全要件或新的安全要件中的密钥对信令整体（密文信令整体）、解密的（明文）信令整体、信令中的部分信元（密文信元）、和/或信令中的部分解密信元（明文信元）进行完保校验（使用密钥以及约定或指示的算法计算出的目标 MAC 值并比较接收到的 MAC 值）；

5 向核心网节点发送解密后的信令整体或信令中的部分解密信元。

可选地，接入网节点对接收到的数据执行以下至少一项：

基于安全要件或新的安全要件中的密钥或密流解密数据；

基于安全要件或新的安全要件中的密钥对数据进行完保校验；

向核心网节点发送数据或解密后的数据（明文数据）。

10 可选地，接入网节点可以基于对接收到的信令的完保校验执行上述对数据的操作，比如成功则处理。上述完保校验和/或解密操作还可以基于发送的用户标识、基于发送的用户标识获得的第三用户标识、第一安全参数、第二安全参数和第三安全参数执行（即计算 XMAC 值的过程中、解密的过程中，还将相应参数作为输入）。

在完成上述操作流程后，接入网节点和终端可以继续执行后续的信令和数据传输流程。

15 例如，终端基于资源信息向接入网节点发送信令和/或数据中的至少一项，接入网节点基于上行资源信息接收到的终端发送的信息后，可以向核心网节点上报相关信息。具体的加密操作和完保操作可以参照上述实施例的描述，在此不再赘述。

例如，接入网节点从核心网节点接收到信令或数据，基于下行资源信息向终端发送信令和/或数据，具体的过程可以参照上述实施例，在此不再赘述。

20 实施例二，在终端处于 INACTIVE 态下，与实施例一的区别在于：

1、核心网节点与接入网节点之间的数据交互是基于用户面执行的。

2、接入网节点基于终端接入网上下文中的密钥生成安全要件的情况下，该安全要件中的密钥就是终端接入网上下文中的密钥。

25 3、第一安全参数不参与交互流程，即实施例一中交互过程中的发送的信息、用于生成安全密钥，执行安全操作、加密操作等信息或行为都不包含第一安全参数。例如，信息 2 中不包含第一安全参数，不基于第一安全参数生成安全要件等。

参照图 4，本申请实施例还提供了一种交互方法，如图 4 所示，该交互方法包括：

步骤 401，接入网节点发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

30 其中，所述加密信息和完整性保护信息基于第一安全要件生成，所述第一安全要件包括密钥和密流中的至少一项。

可选地，所述接入网节点发送目标无线信令之前，所述方法还包括：

所述接入网节点从核心网节点接收第三信息或目标数据；

其中，所述第三信息包括第二标识信息和第二目标信息；

35 所述第二目标信息包括以下至少一项：

所述第一安全要件或第三安全要件，所述第三安全要件包括密钥和密流中的至少一项；第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

40 其中，所述第二标识信息用于指示终端，或由终端标识生成，或指示一组终端，或与所述第一标识信息相关；所述第一算法信息包括以下至少一项：

安全要件派生算法、机密性算法、和完整性算法。

可选地，所述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

45 至少一对第二标识信息与第二目标信息；

其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

或者, 所述第二标识信息与所述第二目标信息为一到零或一映射;

或者, K 个第二标识信息与所有第二目标信息存在对应关系, 且 K 小于或等于所述第三信息中包含的第二标识信息的数量。

可选地, 所述第一目标信息还包括以下至少一项:

第一安全辅助信息, 所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项。

可选地, 所述方法包括:

所述接入网节点执行以下至少一项:

基于第二派生信息和安全要件派生算法中的至少一项生成所述第一安全要件;

还基于机密性算法生成所述加密信息;

还基于完整性算法生成所述完整性保护信息;

还基于第一计算参数生成所述加密信息与所述完整性保护信息中的至少一项;

第三操作;

其中, 所述第一计算参数包括以下至少一项:

终端接入网上下文中的信息;

所述第一标识信息;

第一安全辅助信息中的至少部分内容;

第二安全辅助信息中的至少部分内容;

其中, 所述第二派生信息包括以下至少一项:

接入网相关密钥;

接入层面 AS 层相关密钥;

终端上下文中的密钥;

第三安全要件;

终端接入网上下文中的信息;

所述第一标识信息;

第一安全辅助信息中的至少部分内容;

第二安全辅助信息中的至少部分内容;

所述第三操作包括以下至少一项:

从终端接收第一信息;

从终端接收携带第三安全参数的第一信息;

向终端发送第二信息;

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件, 所述第二安全要件包括密钥和密流中的至少一项, 所述第四派生信息包括以下至少一项: 核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数。

可选地, 所述方法包括以下至少一项:

所述接入网节点基于以下至少一项, 对所述第一信息或所述第一信息中的部分内容进行安全处理: 所述第一安全要件或所述第二安全要件, 所述第一计算参数, 和所述第三安全参数;

所述接入网节点基于以下至少一项, 对所述第二信息或所述第二信息中的部分内容进行安全保护: 所述第一安全要件或所述第二安全要件, 所述第一计算参数, 和所述第三安全参数。

可选地, 所述安全保护包括机密性保护、加密、和完整性保护中的至少一项; 所述安全处理包括解密、机密性处理、完整性处理、完整性校验中的至少一项。

可选地, 所述终端为空闲态或非激活态, 或在发送所述第一信息前为空闲态或非激活态, 或在接收所述第二信息前为空闲态或非激活态。

可选地，所述目标无线信令包括以下至少一项：

至少一个第一标识信息和至少一个第一目标信息；

至少一对第一标识信息与第一目标信息；

其中，第一目标信息与第一标识信息为一到一或多映射；

5 或者，第一标识信息与第一目标信息为一到零或一映射；

或者，N个第一标识信息与所有第一目标信息存在对应关系，且N小于或等于所述目标无线信令包含的第一标识信息的数量。

可选地，所述第一标识信息指示终端，或者由终端标识生成，或者指示一组终端。

10 可选地，所述目标无线信令为广播信令、寻呼信令、无线短消息、系统消息中的任一项；

或者，所述目标无线信令通过寻呼信道PCH、多播信道MCH、广播信道BCH和下行共享信道DL-SCH中的至少一项发送；

或者，所述目标无线信令通过物理下行控制信道PDCCH、物理下行共享信道PDSCH、物理广播信道PBCH和物理多播信道PMCH中的至少一项发送。

15 参照图5，本申请实施例还提供了一种交互方法，如图5所示，该交互方法包括：

步骤501，核心网节点向接入网节点发送第三信息或目标数据，所述第三信息包括第二标识信息和第二目标信息；

其中，所述第二目标信息包括以下至少一项：

第一安全要件或第三安全要件；

20 第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

25 其中，所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项；所述第一安全要件包括密钥和密流中的至少一项，所述第三安全要件包括密钥和密流中的至少一项，所述第二标识信息指示终端，或由终端标识生成，或指示一组终端。

可选地，所述方法还包括：

所述核心网节点基于第三派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件或所述第三安全要件；

30 其中，所述第三派生信息包括以下至少一项：核心网相关密钥、NAS层相关密钥、终端上下文中的密钥、所述第一算法信息、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

可选地，所述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

至少一对第二标识信息与第二目标信息；

35 其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

或者，所述第二标识信息与所述第二目标信息为一到零或一映射；

或者，K个第二标识信息与所有第二目标信息存在对应关系，且K小于或等于第二标识信息的数量。

可选地，所述方法还包括：

40 所述核心网节点从所述终端接收第二算法信息，所述第二算法信息用于指示以下至少一项：所述终端支持的算法、所述终端使用的算法；

其中，所述第一算法信息基于所述第二算法信息生成。

参照图6，本申请实施例还提供了一种交互方法，如图6所示，该交互方法包括：

45 步骤601，接入网节点发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项，其中，所述加密信息和完整性保护信息基于第一安全要件生成；

步骤 602, 终端接收所述目标无线信令;

步骤 603, 在所述终端与所述第一标识信息相关的情况下, 所述终端执行以下至少一项:

基于第一安全要件执行第一操作;

第二操作;

其中, 所述第一操作包括以下至少一项:

解密所述加密信息;

对所述加密信息进行机密性处理;

对所述第一目标信息进行机密性处理;

校验或验证所述完整性保护信息;

对所述第一目标信息进行安全处理;

对所述第一目标信息进行完整性校验或完整性处理;

基于所述完整性保护信息, 对以下至少一项进行完整性校验或完整性处理: 所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果;

其中, 所述第二操作包括以下至少一项:

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件;

向接入网节点发送第一信息;

向接入网节点发送携带第三安全参数的第一信息;

从接入网节点接收第二信息;

其中, 所述第一安全要件基于第一派生信息生成, 所述第一安全要件包括秘钥和密流中的至少一项; 所述第一派生信息包括以下至少一项: 核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信息、和终端接入网上下文中的信息; 所述第四派生信息包括以下至少一项: 核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信息、终端接入网上下文中的信息、和所述第三安全参数; 所述第二安全要件包括密钥和密流中的至少一项。

可选地, 所述方法还包括:

核心网节点向接入网节点发送第三信息或目标数据, 所述第三信息包括第二标识信息和第二目标信息;

所述接入网节点基于所述第二目标信息获知或生成所述第一安全要件, 并基于所述第三信息发送所述目标无线信令;

其中, 所述第二目标信息包括以下至少一项: 所述第一安全要件或第三安全要件、第一算法信息、第二安全参数、和第二安全辅助信息; 所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项;

其中, 所述第二安全辅助信息包括终端核心网上下文中的信息, 所述第三安全要件包括秘钥和密流中的至少一项, 所述第二标识信息指示终端, 或由终端标识生成, 或指示一组终端, 或与所述第一标识信息相关。

可选地, 所述接入网节点基于所述第二目标信息生成所述第一安全要件包括:

所述接入网节点基于第二派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件;

其中, 所述第二派生信息包括以下至少一项: 接入网相关密钥、AS 层相关密钥、终端上下文中的密钥、所述第一安全辅助信息中的至少部分内容、所述第二安全辅助信息中的至少部分内容、第一标识信息、和终端接入网上下文中的信息。

可选地, 所述方法还包括:

所述核心网节点基于第三派生信息和所述安全要件派生算法中的至少一项生成所述第

一安全要件或所述第三安全要件；

其中，所述第三派生信息包括以下至少一项：核心网相关密钥、NAS 层相关密钥、终端上下文中的密钥、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

可选地，所述目标无线信令包括第一安全辅助信息；

5 和/或，所述第一派生信息包括第一安全辅助信息中的至少部分内容；

其中，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项。

本申请实施例中，上述终端还可以执行上述图 2 实施例中终端的各个步骤，上述接入网节点还可以执行上述图 4 实施例中接入网节点各个步骤，核心网节点还可以执行上述图 5 中核心网节点执行的各个步骤，详情可参照上述实施例的描述，为了避免重复在此不再赘述。

本申请实施例提供的交互方法，执行主体可以为交互装置或交互系统。本申请实施例中以交互装置执行交互方法的方法为例，说明本申请实施例提供的交互装置和交互系统。

参照图 7，本申请实施例还提供了一种交互装置，如图 7 所示，该交互装置 700 包括：

15 第一接收模块 701，用于接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

第一执行模块 702，用于执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

20 其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

25 对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

30 基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息和所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述第二安全要件包括密钥和密流中的至少一项。

可选地，所述第一目标信息还包括第一安全辅助信息；

其中，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项；

40 所述第一算法信息包括以下至少一项：

安全要件派生算法，所述第一安全要件还基于所述安全要件派生算法生成；

机密性算法和完整性算法中至少一项，所述第一操作还基于所述机密性算法和完整性算法中至少一项执行。

可选地，所述第一派生信息还包括以下至少一项：

45 第一安全辅助信息中的至少部分内容；

终端核心网上下文中的信息；

终端接入网上下文中的信息；
所述第一标识信息。

可选地，所述第一执行模块 702 具体用于基于所述第一安全要件以及第一计算参数执行所述第一操作，所述第一计算参数包括以下至少一项：

5 终端核心网上下文中的信息；
终端接入网上下文中的信息；
所述第一标识信息；
第一安全辅助信息中的至少部分内容。

可选地，所述终端核心网上下文中的信息，包括以下至少一项：

10 终端的标识信息；
终端的组标识信息；
NAS 信令的计数信息；
NAS 上行信令的计数信息；
NAS 下行信令的计数信息；

15 通过 NAS 传输的协议数据报文的计数信息；
通过 NAS 传输的上行协议数据报文的计数信息；
通过 NAS 传输的下行协议数据报文的计数信息；
或，所述终端接入网上下文中的信息，包括以下至少一项：

20 终端的标识信息；
终端的组标识信息；
AS 信令的计数信息；
AS 上行信令的计数信息；
AS 下行信令的计数信息；
协议数据报文的计数信息；

25 上行协议数据报文的计数信息；
下行协议数据报文的计数信息。

可选地，所述第一执行模块 702 还用于执行以下至少一项：

基于以下至少一项，对所述第一信息或所述第一信息中的部分内容进行安全保护：所述第一安全要件或所述第二安全要件，第一计算参数，和所述第三安全参数；

30 基于以下至少一项，对所述第二信息或所述第二信息中的部分内容进行安全处理：所述第一安全要件或所述第二安全要件，第一计算参数，和所述第三安全参数。

可选地，所述安全保护包括机密性保护、加密、和完整性保护中的至少一项；所述安全处理包括解密、机密性处理、完整性处理、完整性校验中的至少一项。

可选地，所述目标无线信令包括以下至少一项：

35 至少一个第一标识信息和至少一个第一目标信息；
至少一对第一标识信息与第一目标信息；

其中，第一目标信息与第一标识信息为一到一或多映射；

或者，第一标识信息与第一目标信息为一到零或一映射；

40 或者，N 个第一标识信息与所有第一目标信息存在对应关系，且 N 小于或等于所述目标无线信令中包含的第一标识信息的数量。

可选地，所述终端为空闲态或非激活态，或在发送所述第一信息前为空闲态或非激活态，或在接收所述第二信息前为空闲态或非激活态。

可选地，所述第一执行模块 702 还用于：向网络侧发送第二算法信息，所述第二算法信息用于指示以下至少一项：所述终端支持的算法、所述终端使用的算法；

45 其中，所述算法包括安全要件派生算法、机密性算法、和完整性算法中至少一项。

可选地，所述第一标识信息指示终端，或者由终端标识生成，或者指示一组终端。

可选地, 所述目标无线信令包括广播信令、寻呼信令、无线短消息、和系统消息中的任一项;

或者, 所述目标无线信令通过寻呼信道 PCH、多播信道 MCH、广播信道 BCH 和下行共享信道 DL-SCH 中的至少一项发送;

5 或者, 所述目标无线信令通过物理下行控制信道 PDCCH、物理下行共享信道 PDSCH、物理广播信道 PBCH 和物理多播信道 PMCH 中的至少一项发送。

参照图 8, 本申请实施例还提供了一种交互装置, 如图 8 所示, 该交互装置 800 包括:

第一发送模块 801, 用于发送目标无线信令, 所述目标无线信令包括第一标识信息以及第一目标信息, 所述第一目标信息包括加密信息与完整性保护信息中的至少一项;

10 其中, 所述加密信息和完整性保护信息基于第一安全要件生成, 所述第一安全要件包括秘钥和密流中的至少一项。

可选地, 所述交互装置还包括:

第二接收模块, 用于从核心网节点接收第三信息或目标数据;

其中, 所述第三信息包括第二标识信息和第二目标信息;

15 所述第二目标信息包括以下至少一项:

所述第一安全要件或第三安全要件, 所述第三安全要件包括秘钥和密流中的至少一项;

第一算法信息;

第二安全参数;

第二安全辅助信息, 所述第二安全辅助信息包括终端核心网上下文中的信息;

20 其中, 所述第二标识信息用于指示终端, 或由终端标识生成, 或指示一组终端, 或与所述第一标识信息相关; 所述第一算法信息包括以下至少一项:

安全要件派生算法、机密性算法、和完整性算法。

可选地, 所述第三信息包括以下至少一项:

至少一个第二标识信息和至少一个第二目标信息;

25 至少一对第二标识信息与第二目标信息;

其中, 所述第二目标信息与所述第二标识信息为一到一或多映射;

或者, 所述第二标识信息与所述第二目标信息为一到零或一映射;

或者, K 个第二标识信息与所有第二目标信息存在对应关系, 且 K 小于或等于所述第三信息中包含的第二标识信息的数量。

30 可选地, 所述第一目标信息还包括以下至少一项:

第一安全辅助信息, 所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项。

可选地, 所述交互装置 800 还包括:

第二执行模块, 用于执行以下至少一项:

35 基于第二派生信息和安全要件派生算法中的至少一项生成所述第一安全要件;

还基于机密性算法生成所述加密信息;

还基于完整性算法生成所述完整性保护信息;

还基于第一计算参数生成所述加密信息与所述完整性保护信息中的至少一项;

第三操作;

40 其中, 所述第一计算参数包括以下至少一项:

终端接入网上下文中的信息;

所述第一标识信息;

第一安全辅助信息中的至少部分内容;

第二安全辅助信息中的至少部分内容;

45 其中, 所述第二派生信息包括以下至少一项:

接入网相关密钥;

接入层面 AS 层相关密钥；
终端上下文中的密钥；
第三安全要件；
终端接入网上下文中的信息；

所述第一标识信息；
第一安全辅助信息中的至少部分内容；
第二安全辅助信息中的至少部分内容；
所述第三操作包括以下至少一项：

从终端接收第一信息；
从终端接收携带第三安全参数的第一信息；
向终端发送第二信息；

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件，所述第二安全要件包括密钥和密流中的至少一项，所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数。

可选地，所述第二执行模块还用于执行以下至少一项：

基于以下至少一项，对所述第一信息或所述第一信息中的部分内容进行安全处理：所述第一安全要件或所述第二安全要件，所述第一计算参数，和所述第三安全参数；

基于以下至少一项，对所述第二信息或所述第二信息中的部分内容进行安全保护：所述第一安全要件或所述第二安全要件，所述第一计算参数，和所述第三安全参数。

可选地，所述安全保护包括机密性保护、加密、和完整性保护中的至少一项；所述安全处理包括解密、机密性处理、完整性处理、完整性校验中的至少一项。

可选地，所述终端为空闲态或非激活态，或在发送所述第一信息前为空闲态或非激活态，或在接收所述第二信息前为空闲态或非激活态。

可选地，所述目标无线信令包括以下至少一项：

至少一个第一标识信息和至少一个第一目标信息；

至少一对第一标识信息与第一目标信息；

其中，第一目标信息与第一标识信息为一到一或多映射；

或者，第一标识信息与第一目标信息为一到零或一映射；

或者，N 个第一标识信息与所有第一目标信息存在对应关系，且 N 小于或等于所述目标无线信令包含的第一标识信息的数量。

可选地，所述第一标识信息指示终端，或者由终端标识生成，或者指示一组终端。

可选地，所述目标无线信令为广播信令、寻呼信令、无线短消息、系统消息中的任一项；

或者，所述目标无线信令通过寻呼信道 PCH、多播信道 MCH、广播信道 BCH 和下行共享信道 DL-SCH 中的至少一项发送；

或者，所述目标无线信令通过物理下行控制信道 PDCCH、物理下行共享信道 PDSCH、物理广播信道 PBCH 和物理多播信道 PMCH 中的至少一项发送。

参照图 9，本申请实施例还提供了一种交互装置，如图 9 所示，该交互装置 900 包括：

第二发送模块 901，用于向接入网节点发送第三信息或目标数据，所述第三信息包括第二标识信息和第二目标信息；

其中，所述第二目标信息包括以下至少一项：

第一安全要件或第三安全要件；

第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项；所述第一安全要件包括秘钥和密流中的至少一项，所述第三安全要件包括秘钥和密流中的至少一项，所述第二标识信息指示终端。

可选地，所述交互装置 900 还包括：

5 第三执行模块，用于基于第三派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件或所述第三安全要件；

其中，所述第三派生信息包括以下至少一项：核心网相关密钥、NAS 层相关密钥、终端上下文中的密钥、所述第一算法信息、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

10 可选地，所述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

至少一对第二标识信息与第二目标信息；

其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

或者，所述第二标识信息与所述第二目标信息为一到零或一映射；

15 或者，K 个第二标识信息与所有第二目标信息存在对应关系，且 K 小于或等于第二标识信息的数量。

可选地，所述交互装置 900 还包括：

第三接收模块，用于从所述终端接收第二算法信息，所述第二算法信息用于指示以下至少一项：所述终端支持的算法、所述终端使用的算法；

20 其中，所述第一算法信息基于所述第二算法信息生成。

本申请实施例中的交互装置可以是电子设备，例如具有操作系统的电子设备，也可以是电子设备中的部件，例如集成电路或芯片。该电子设备可以是终端，也可以为除终端之外的其他设备。示例性的，终端可以包括但不限于上述所列举的终端 11 的类型，其他设备可以为服务器、网络附属存储器（Network Attached Storage，NAS）等，本申请实施例不作具体限定。

本申请实施例提供的交互装置能够实现图 2 至图 5 的方法实施例实现的各个过程，并达到相同的技术效果，为避免重复，这里不再赘述。

本申请实施例还提供了一种交互系统，该交互系统包括：接入网节点和终端，其中，

30 所述接入网节点用于发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项，其中，所述加密信息和完整性保护信息基于第一安全要件生成；

所述终端用于接收所述目标无线信令；并在所述终端与所述第一标识信息相关的情况下，执行以下至少一项：

基于第一安全要件执行第一操作；

35 第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

40 校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

45 其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括秘钥和密流中的至少一项；所述第一派生信息和所述第四派生信息包括以下至少一项：核心网相关密
5 钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文
文中的密钥、终端核心网上下文中的信息、第一标识信息、和终端接入网上下文中的信息；
所述第二安全要件包括密钥和密流中的至少一项。

可选地，所述交互系统还包括核心网节点，所述核心网节点用于向接入网节点发送第
三信息或目标数据，所述第三信息包括第二标识信息和第二目标信息；

10 所述接入网节点基于所述第二目标信息获知或生成所述第一安全要件，并基于所述第
三信息发送所述目标无线信令；

其中，所述第二目标信息包括以下至少一项：所述第一安全要件或第三安全要件、第
一算法信息、第二安全参数、和第二安全辅助信息；所述第一算法信息包安全要件派生算
法、机密性算法、和完整性算法中的至少一项；

15 其中，所述第二安全辅助信息包括终端核心网上下文中的信息，所述第三安全要件包
括秘钥和密流中的至少一项，所述第二标识信息指示终端，或由终端标识生成，或指示一
组终端，或与所述第一标识信息相关。

可选地，所述接入网节点具体用于基于第二派生信息和所述安全要件派生算法中的至
少一项生成所述第一安全要件；

20 其中，所述第二派生信息包括以下至少一项：接入网相关密钥、AS 层相关密钥、终端
上下文中的密钥、所述第一安全辅助信息中的至少部分内容、所述第二安全辅助信息中的
至少部分内容、第一标识信息、和终端接入网上下文中的信息。

可选地，所述核心网节点还用于基于第三派生信息和所述安全要件派生算法中的至少
一项生成所述第一安全要件或所述第三安全要件；

25 其中，所述第三派生信息包括以下至少一项：核心网相关密钥、NAS 层相关密钥、终
端上下文中的密钥、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

可选地，所述目标无线信令包括第一安全辅助信息；

和/或，所述第一派生信息包括第一安全辅助信息中的至少部分内容；

30 其中，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中
的至少一项。

需要说明的是，上述对交互系统的说明仅仅是部分举例，交互系统可以包括前述各个
实施例中的终端、接入网节点以及核心网节点中的至少两项。

如图 10 所示，本申请实施例还提供一种通信设备 1000，包括处理器 1001 和存储器
1002，存储器 1002 上存储有可在所述处理器 1001 上运行的程序或指令，该程序或指令被
35 处理器 1001 执行时实现上述交互方法实施例的各个步骤，且能达到相同的技术效果，为避
免重复，这里不再赘述。

本申请实施例还提供一种终端，包括处理器和通信接口，所述通信接口和所述处理器
耦合，所述处理器用于运行程序或指令，实现如图 2 所示方法实施例中的步骤。该终端实
施例与上述终端侧方法实施例对应，上述方法实施例的各个实施过程和实现方式均可适用
40 于该终端实施例中，且能达到相同的技术效果。具体地，图 11 为实现本申请实施例的一种
终端的硬件结构示意图。

该终端 1100 包括但不限于：射频单元 1101、网络模块 1102、音频输出单元 1103、输
入单元 1104、传感器 1105、显示单元 1106、用户输入单元 1107、接口单元 1108、存储器
1109 以及处理器 1110 等中的至少部分部件。

45 本领域技术人员可以理解，终端 1100 还可以包括给各个部件供电的电源（比如电池），
电源可以通过电源管理系统与处理器 1110 逻辑相连，从而通过电源管理系统实现管理充电、

放电以及功耗管理等功能。图 11 中示出的终端结构并不构成对终端的限定，终端可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置，在此不再赘述。

应理解的是，本申请实施例中，输入单元 1104 可以包括图形处理单元（Graphics Processing Unit, GPU）11041 和麦克风 11042，图形处理器 11041 对在视频捕获模式或图像捕获模式中由图像捕获装置（如摄像头）获得的静态图片或视频的图像数据进行处理。显示单元 1106 可包括显示面板 11061，可以采用液晶显示器、有机发光二极管等形式来配置显示面板 11061。用户输入单元 1107 包括触控面板 11071 以及其他输入设备 11072 中的至少一种。触控面板 11071，也称为触摸屏。触控面板 11071 可包括触摸检测装置和触摸控制器两个部分。其他输入设备 11072 可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆，在此不再赘述。

本申请实施例中，射频单元 1101 接收来自网络侧设备的下行数据后，可以传输给处理器 1110 进行处理；另外，射频单元 1101 可以向网络侧设备发送上行数据。通常，射频单元 1101 包括但不限于天线、放大器、收发信机、耦合器、低噪声放大器、双工器等。

存储器 1109 可用于存储软件程序或指令以及各种数据。存储器 1109 可主要包括存储程序或指令的第一存储区和存储数据的第二存储区，其中，第一存储区可存储操作系统、至少一个功能所需的应用程序或指令（比如声音播放功能、图像播放功能等）等。此外，存储器 1109 可以包括易失性存储器或非易失性存储器。其中，非易失性存储器可以是只读存储器（Read-Only Memory, ROM）、可编程只读存储器（Programmable ROM, PROM）、可擦除可编程只读存储器（Erasable PROM, EPROM）、电可擦除可编程只读存储器（Electrically EPROM, EEPROM）或闪存。易失性存储器可以是随机存取存储器（Random Access Memory, RAM），静态随机存取存储器（Static RAM, SRAM）、动态随机存取存储器（Dynamic RAM, DRAM）、同步动态随机存取存储器（Synchronous DRAM, SDRAM）、双倍数据速率同步动态随机存取存储器（Double Data Rate SDRAM, DDRSDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM, ESDRAM）、同步连接动态随机存取存储器（Synch link DRAM, SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM, DRRAM）。本申请实施例中的存储器 1109 包括但不限于这些和任意其它适合类型的存储器。

处理器 1110 可包括一个或多个处理单元；可选的，处理器 1110 集成应用处理器和调制解调处理器，其中，应用处理器主要处理涉及操作系统、用户界面和应用程序等的操作，调制解调处理器主要处理无线通信信号，如基带处理器。可以理解的是，上述调制解调处理器也可以不集成到处理器 1110 中。

其中，射频单元 1101，用于接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

在终端与所述第一标识信息相关的情况下，执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；
向接入网节点发送第一信息；
向接入网节点发送携带第三安全参数的第一信息；
从接入网节点接收第二信息；

5 其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数；所述
10 第二安全要件包括密钥和密流中的至少一项。可以理解，本实施例中提及的各实现方式的实现过程可以参照终端侧方法实施例的相关描述，并达到相同或相应的技术效果，为避免重复，在此不再赘述。

本申请实施例还提供一种网络侧设备，包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如图 4 所示的方法实施例的步骤。该
15 网络侧设备实施例与上述网络侧设备方法实施例对应，上述方法实施例的各个实施过程和实现方式均可适用于该网络侧设备实施例中，且能达到相同的技术效果。

具体地，本申请实施例还提供了一种网络侧设备。如图 12 所示，该网络侧设备 1200
包括：天线 1201、射频装置 1202、基带装置 1203、处理器 1204 和存储器 1205。天线 1201
与射频装置 1202 连接。在上行方向上，射频装置 1202 通过天线 1201 接收信息，将接收的
20 信息发送给基带装置 1203 进行处理。在下行方向上，基带装置 1203 对要发送的信息进行处理，并发送给射频装置 1202，射频装置 1202 对收到的信息进行处理后经过天线 1201 发送出去。

以上实施例中网络侧设备执行的方法可以在基带装置 1203 中实现，该基带装置 1203
包括基带处理器。

25 基带装置 1203 例如可以包括至少一个基带板，该基带板上设置有多个芯片，如图 12 所示，其中一个芯片例如为基带处理器，通过总线接口与存储器 1205 连接，以调用存储器 1205 中的程序，执行以上方法实施例中所示的网络侧设备操作。

该网络侧设备还可以包括网络接口 1206，该接口例如为通用公共无线接口（Common
Public Radio Interface, CPRI）。

30 具体地，本申请实施例的网络侧设备 1200 还包括：存储在存储器 1205 上并可在处理器 1204 上运行的指令或程序，处理器 1204 调用存储器 1205 中的指令或程序执行图 8 所示各模块执行的方法，并达到相同的技术效果，为避免重复，故不在此赘述。

具体地，本申请实施例还提供了一种网络侧设备。如图 13 所示，该网络侧设备 1300
包括：处理器 1301、网络接口 1302 和存储器 1303。其中，网络接口 1302 例如为通用公共
35 无线接口（common public radio interface, CPRI）。

具体地，本申请实施例的网络侧设备 1300 还包括：存储在存储器 1303 上并可在处理器 1301 上运行的指令或程序，处理器 1301 调用存储器 1303 中的指令或程序执行图 9 所示各模块执行的方法，并达到相同的技术效果，为避免重复，故不在此赘述。

本申请实施例还提供一种可读存储介质，所述可读存储介质上存储有程序或指令，该
40 程序或指令被处理器执行时实现上述交互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。

其中，所述处理器为上述实施例中所述的终端中的处理器。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 ROM、随机存取存储器 RAM、磁碟或者光盘
等。在一些示例中，可读存储介质可以是非瞬态的可读存储介质。

45 本申请实施例另提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现上述交互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。

应理解，本申请实施例提到的芯片还可以称为系统级芯片，系统芯片，芯片系统或片上系统芯片等。

5 本申请实施例另提供了一种计算机程序/程序产品，所述计算机程序/程序产品被存储在存储介质中，所述计算机程序/程序产品被至少一个处理器执行以实现上述交互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。

本申请实施例还提供了一种无线通信系统，包括：终端及网络侧设备，所述终端可用于执行如上所述终端侧的交互方法的步骤，所述网络侧设备可用于执行如上所述接入网节点和核心网节点的交互方法的步骤。

10 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。此外，需要指出的是，本
15 申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能，还可包括根据所涉及的功能按基本同时的方式或按相反的顺序来执行功能，例如，可以按不同于所描述的次序来执行所描述的方法，并且还可以添加、省去、或组合各种步骤。另外，参照某些示例所描述的特征可在其他示例中被组合。

20 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助计算机软件产品加必需的通用硬件平台的方式来实现，当然也可以通过硬件。该计算机软件产品存储在存储介质（如 ROM、RAM、磁碟、光盘等）中，包括若干指令，用以使得终端或者网络侧设备执行本申请各个实施例所述的方法。

上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式的实施方式，这些实施方式均属于本申请的保护之内。

权利要求书

1. 一种交互方法，其中，包括：

终端接收目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述
5 第一目标信息包括加密信息与完整性保护信息中的至少一项；

在所述终端与所述第一标识信息相关的情况下，所述终端执行以下至少一项：

基于第一安全要件执行第一操作；

第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

10 对所述加密信息进行机密性处理；

对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

15 基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一
目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

20 向接入网节点发送携带第三安全参数的第一信息；

从接入网节点接收第二信息；

其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流
中的至少一项；所述第一派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS
层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述
25 第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网
相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数；所述
第二安全要件包括密钥和密流中的至少一项。

2. 根据权利要求 1 所述的方法，其中，所述第一目标信息还包括第一安全辅助信息；

30 其中，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中
的至少一项；

所述第一算法信息包括以下至少一项：

安全要件派生算法，所述第一安全要件还基于所述安全要件派生算法生成；

机密性算法和完整性算法中至少一项，所述第一操作还基于所述机密性算法和完整性
算法中至少一项执行。

35 3. 根据权利要求 1 或 2 所述的方法，其中，所述第一派生信息还包括以下至少一项：

第一安全辅助信息中的至少部分内容；

终端核心网上下文中的信息；

终端接入网上下文中的信息；

所述第一标识信息。

40 4. 根据权利要求 1 至 3 任一项所述的方法，其中，所述终端基于第一安全要件执行第
一操作，包括：

所述终端基于所述第一安全要件以及第一计算参数执行所述第一操作，所述第一计算
参数包括以下至少一项：

终端核心网上下文中的信息；

45 终端接入网上下文中的信息；

所述第一标识信息；

第一安全辅助信息中的至少部分内容。

5. 根据权利要求 3 或 4 所述的方法，其中，所述终端核心网上下文中的信息，包括以下至少一项：

5 终端的标识信息；

终端的组标识信息；

NAS 信令的计数信息；

NAS 上行信令的计数信息；

NAS 下行信令的计数信息；

10 通过 NAS 传输的协议数据报文的计数信息；

通过 NAS 传输的上行协议数据报文的计数信息；

通过 NAS 传输的下行协议数据报文的计数信息；

或，所述终端接入网上下文中的信息，包括以下至少一项：

终端的标识信息；

15 终端的组标识信息；

AS 信令的计数信息；

AS 上行信令的计数信息；

AS 下行信令的计数信息；

协议数据报文的计数信息；

20 上行协议数据报文的计数信息；

下行协议数据报文的计数信息。

6. 根据权利要求 1 至 5 中任一项所述的方法，其中，所述方法包括以下至少一项：

所述终端基于以下至少一项，对所述第一信息或所述第一信息中的部分内容进行安全保护：所述第一安全要件或所述第二安全要件，第一计算参数，和所述第三安全参数；

25 所述终端基于以下至少一项，对所述第二信息或所述第二信息中的部分内容进行安全处理：所述第一安全要件或所述第二安全要件，第一计算参数，和所述第三安全参数。

7. 根据权利要求 6 所述的方法，其中，所述安全保护包括机密性保护、加密、和完整性保护中的至少一项；所述安全处理包括解密、机密性处理、完整性处理、完整性校验中的至少一项。

30 8. 根据权利要求 1 至 7 中任一项所述的方法，其中，所述目标无线信令包括以下至少一项：

至少一个第一标识信息和至少一个第一目标信息；

至少一对第一标识信息与第一目标信息；

其中，第一目标信息与第一标识信息为一到一或多映射；

35 或者，第一标识信息与第一目标信息为一到零或一映射；

或者，N 个第一标识信息与所有第一目标信息存在对应关系，且 N 小于或等于所述目标无线信令中包含的第一标识信息的数量。

9. 根据权利要求 1 至 8 中任一项所述的方法，其中，所述终端为空闲态或非激活态，或在发送所述第一信息前为空闲态或非激活态，或在接收所述第二信息前为空闲态或非激活态。

40 10. 根据权利要求 1 至 9 中任一项所述的方法，其中，所述终端接收目标无线信令之前，所述方法还包括：

所述终端向网络侧发送第二算法信息，所述第二算法信息用于指示以下至少一项：所述终端支持的算法、所述终端使用的算法；

45 其中，所述算法包括安全要件派生算法、机密性算法、和完整性算法中至少一项。

11. 根据权利要求 1 至 10 任一项所述的方法，其中，所述第一标识信息指示终端，或

者由终端标识生成，或者指示一组终端。

12. 根据权利要求 1 至 11 任一项所述的方法，其中，所述目标无线信令包括广播信令、寻呼信令、无线短消息、和系统消息中的任一项；

或者，所述目标无线信令通过寻呼信道 PCH、多播信道 MCH、广播信道 BCH 和下行共享信道 DL-SCH 中的至少一项发送；

或者，所述目标无线信令通过物理下行控制信道 PDCCH、物理下行共享信道 PDSCH、物理广播信道 PBCH 和物理多播信道 PMCH 中的至少一项发送。

13. 一种交互方法，其中，包括：

接入网节点发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

其中，所述加密信息和完整性保护信息基于第一安全要件生成，所述第一安全要件包括秘钥和密流中的至少一项。

14. 根据权利要求 13 所述的方法，其中，所述接入网节点发送目标无线信令之前，所述方法还包括：

所述接入网节点从核心网节点接收第三信息或目标数据；

其中，所述第三信息包括第二标识信息和第二目标信息；

所述第二目标信息包括以下至少一项：

所述第一安全要件或第三安全要件，所述第三安全要件包括秘钥和密流中的至少一项；

第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第二标识信息用于指示终端，或由终端标识生成，或指示一组终端，或与所述第一标识信息相关；所述第一算法信息包括以下至少一项：

安全要件派生算法、机密性算法、和完整性算法。

15. 根据权利要求 14 所述的方法，其中，所述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

至少一对第二标识信息与第二目标信息；

其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

或者，所述第二标识信息与所述第二目标信息为一到零或一映射；

或者，K 个第二标识信息与所有第二目标信息存在对应关系，且 K 小于或等于所述第三信息中包含的第二标识信息的数量。

16. 根据权利要求 13 至 15 中任一项所述的方法，其中，所述第一目标信息还包括以下至少一项：

第一安全辅助信息，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项。

17. 根据权利要求 13 至 16 中任一项所述的方法，其中，所述方法包括：

所述接入网节点执行以下至少一项：

基于第二派生信息和安全要件派生算法中的至少一项生成所述第一安全要件；

还基于机密性算法生成所述加密信息；

还基于完整性算法生成所述完整性保护信息；

还基于第一计算参数生成所述加密信息与所述完整性保护信息中的至少一项；

第三操作；

其中，所述第一计算参数包括以下至少一项：

终端接入网上下文中的信息；

所述第一标识信息；

第一安全辅助信息中的至少部分内容；

第二安全辅助信息中的至少部分内容；
其中，所述第二派生信息包括以下至少一项：

接入网相关密钥；

接入层面 AS 层相关密钥；

终端上下文中的密钥；

第三安全要件；

终端接入网上下文中的信息；

所述第一标识信息；

第一安全辅助信息中的至少部分内容；

第二安全辅助信息中的至少部分内容；

所述第三操作包括以下至少一项：

从终端接收第一信息；

从终端接收携带第三安全参数的第一信息；

向终端发送第二信息；

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件，所述第二安全要件包括密钥和密流中的至少一项，所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、AS 层相关密钥、终端上下文中的密钥、和所述第三安全参数。

18. 根据权利要求 17 所述的方法，其中，所述方法包括以下至少一项：

所述接入网节点基于以下至少一项，对所述第一信息或所述第一信息中的部分内容进行安全处理：所述第一安全要件或所述第二安全要件，所述第一计算参数，和所述第三安全参数；

所述接入网节点基于以下至少一项，对所述第二信息或所述第二信息中的部分内容进行安全保护：所述第一安全要件或所述第二安全要件，所述第一计算参数，和所述第三安全参数。

19. 根据权利要求 18 所述的方法，其中，所述安全保护包括机密性保护、加密、和完整性保护中的至少一项；所述安全处理包括解密、机密性处理、完整性处理、完整性校验中的至少一项。

20. 根据权利要求 17 至 19 中任一项所述的方法，其中，所述终端为空闲态或非激活态，或在发送所述第一信息前为空闲态或非激活态，或在接收所述第二信息前为空闲态或非激活态。

21. 根据权利要求 13 至 20 中任一项所述的方法，其中，所述目标无线信令包括以下至少一项：

至少一个第一标识信息和至少一个第一目标信息；

至少一对第一标识信息与第一目标信息；

其中，第一目标信息与第一标识信息为一到一或多映射；

或者，第一标识信息与第一目标信息为一到零或一映射；

或者，N 个第一标识信息与所有第一目标信息存在对应关系，且 N 小于或等于所述目标无线信令包含的第一标识信息的数量。

22. 根据权利要求 13 至 21 任一项所述的方法，其中，所述第一标识信息指示终端，或者由终端标识生成，或者指示一组终端。

23. 根据权利要求 13 至 22 任一项所述的方法，其中，所述目标无线信令为广播信令、寻呼信令、无线短消息、系统消息中的任一项；

或者，所述目标无线信令通过寻呼信道 PCH、多播信道 MCH、广播信道 BCH 和下行共享信道 DL-SCH 中的至少一项发送；

或者，所述目标无线信令通过物理下行控制信道 PDCCH、物理下行共享信道 PDSCH、

物理广播信道 PBCH 和物理多播信道 PMCH 中的至少一项发送。

24. 一种交互方法, 其中, 包括:

核心网节点向接入网节点发送第三信息或目标数据, 所述第三信息包括第二标识信息和第二目标信息;

5 其中, 所述第二目标信息包括以下至少一项:

第一安全要件或第三安全要件;

第一算法信息;

第二安全参数;

第二安全辅助信息, 所述第二安全辅助信息包括终端核心网上下文中的信息;

10 其中, 所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项; 所述第一安全要件包括秘钥和密流中的至少一项, 所述第三安全要件包括秘钥和密流中的至少一项, 所述第二标识信息指示终端, 或由终端标识生成, 或指示一组终端。

25. 根据权利要求 24 所述的方法, 其中, 所述方法还包括:

15 所述核心网节点基于第三派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件或所述第三安全要件;

其中, 所述第三派生信息包括以下至少一项: 核心网相关密钥、NAS 层相关密钥、终端上下文中的密钥、所述第一算法信息、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

26. 根据权利要求 24 或 25 所述的方法, 其中, 所述第三信息包括以下至少一项:

20 至少一个第二标识信息和至少一个第二目标信息;

至少一对第二标识信息与第二目标信息;

其中, 所述第二目标信息与所述第二标识信息为一到一或多映射;

或者, 所述第二标识信息与所述第二目标信息为一到零或一映射;

25 或者, K 个第二标识信息与所有第二目标信息存在对应关系, 且 K 小于或等于第二标识信息的数量。

27. 根据权利要求 24 至 26 中任一项所述的方法, 其中, 所述方法还包括:

所述核心网节点从所述终端接收第二算法信息, 所述第二算法信息用于指示以下至少一项: 所述终端支持的算法、所述终端使用的算法;

其中, 所述第一算法信息基于所述第二算法信息生成。

30 28. 一种交互方法, 其中, 包括:

接入网节点发送目标无线信令, 所述目标无线信令包括第一标识信息以及第一目标信息, 所述第一目标信息包括加密信息与完整性保护信息中的至少一项, 其中, 所述加密信息和完整性保护信息基于第一安全要件生成;

终端接收所述目标无线信令;

35 在所述终端与所述第一标识信息相关的情况下, 所述终端执行以下至少一项:

基于第一安全要件执行第一操作;

第二操作;

其中, 所述第一操作包括以下至少一项:

解密所述加密信息;

40 对所述加密信息进行机密性处理;

对所述第一目标信息进行机密性处理;

校验或验证所述完整性保护信息;

对所述第一目标信息进行安全处理;

对所述第一目标信息进行完整性校验或完整性处理;

45 基于所述完整性保护信息, 对以下至少一项进行完整性校验或完整性处理: 所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果;

其中, 所述第二操作包括以下至少一项:

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件;

向接入网节点发送第一信息;

向接入网节点发送携带第三安全参数的第一信息;

5 从接入网节点接收第二信息;

其中, 所述第一安全要件基于第一派生信息生成, 所述第一安全要件包括秘钥和密流中的至少一项; 所述第一派生信息包括以下至少一项: 核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信息、和终端接入网上下文中的信息; 所述第四派生信息
10 包括以下至少一项: 核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、终端上下文中的密钥、终端核心网上下文中的信息、第一标识信息、终端接入网上下文中的信息、和所述第三安全参数; 所述第二安全要件包括密钥和密流中的至少一项。

29. 根据权利要求 28 所述的方法, 其中, 所述方法还包括:

15 核心网节点向接入网节点发送第三信息或目标数据, 所述第三信息包括第二标识信息和第二目标信息;

所述接入网节点基于所述第二目标信息获知或生成所述第一安全要件, 并基于所述第三信息发送所述目标无线信令;

其中, 所述第二目标信息包括以下至少一项: 所述第一安全要件或第三安全要件、第一算法信息、第二安全参数、和第二安全辅助信息; 所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少一项;

其中, 所述第二安全辅助信息包括终端核心网上下文中的信息, 所述第三安全要件包括秘钥和密流中的至少一项, 所述第二标识信息指示终端, 或由终端标识生成, 或指示一组终端, 或与所述第一标识信息相关。

25 30. 根据权利要求 29 所述的方法, 其中, 所述接入网节点基于所述第二目标信息生成所述第一安全要件包括:

所述接入网节点基于第二派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件;

其中, 所述第二派生信息包括以下至少一项: 接入网相关密钥、AS 层相关密钥、终端上下文中的密钥、所述第一安全辅助信息中的至少部分内容、所述第二安全辅助信息中的至少部分内容、第一标识信息、和终端接入网上下文中的信息。

31. 根据权利要求 29 所述的方法, 其中, 所述方法还包括:

所述核心网节点基于第三派生信息和所述安全要件派生算法中的至少一项生成所述第一安全要件或所述第三安全要件;

35 其中, 所述第三派生信息包括以下至少一项: 核心网相关密钥、NAS 层相关密钥、终端上下文中的密钥、所述第二安全参数、和所述第二安全辅助信息中的至少部分内容。

32. 根据权利要求 28 至 31 中任一项所述的方法, 其中, 所述目标无线信令包括第一安全辅助信息;

和/或, 所述第一派生信息包括第一安全辅助信息中的至少部分内容;

40 其中, 所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项。

33. 一种交互装置, 应用于终端, 其中, 包括:

第一接收模块, 用于接收目标无线信令, 所述目标无线信令包括第一标识信息以及第一目标信息, 所述第一目标信息包括加密信息与完整性保护信息中的至少一项;

45 第一执行模块, 用于执行以下至少一项:

基于第一安全要件执行第一操作;

第二操作；

其中，所述第一操作包括以下至少一项：

解密所述加密信息；

对所述加密信息进行机密性处理；

5 对所述第一目标信息进行机密性处理；

校验或验证所述完整性保护信息；

对所述第一目标信息进行安全处理；

对所述第一目标信息进行完整性校验或完整性处理；

10 基于所述完整性保护信息，对以下至少一项进行完整性校验或完整性处理：所述第一目标信息、所述第一目标信息中的部分内容、和所述解密的结果；

其中，所述第二操作包括以下至少一项：

基于第四派生信息和所述第一安全要件中的至少一项生成第二安全要件；

向接入网节点发送第一信息；

从接入网节点接收第二信息；

15 其中，所述第一安全要件基于第一派生信息生成，所述第一安全要件包括密钥和密流中的至少一项；所述第一派生信息和所述第四派生信息包括以下至少一项：核心网相关密钥、非接入层面 NAS 层相关密钥、接入网相关密钥、接入层面 AS 层相关密钥、和终端上下文中的密钥；所述第二安全要件包括密钥和密流中的至少一项。

20 34. 根据权利要求 33 所述的交互装置，其中，所述第一目标信息还包括第一安全辅助信息；

其中，所述第一安全辅助信息包括第一算法信息、第一安全参数、和第二安全参数中的至少一项；

所述第一算法信息包括以下至少一项：

安全要件派生算法，所述第一安全要件还基于所述安全要件派生算法生成；

25 机密性算法和完整性算法中至少一项，所述第一操作还基于所述机密性算法和完整性算法中至少一项执行。

35. 根据权利要求 33 或 34 所述的交互装置，其中，所述第一派生信息还包括以下至少一项：

第一安全辅助信息中的至少部分内容；

30 终端核心网上下文中的信息；

终端接入网上下文中的信息；

所述第一标识信息。

36. 根据权利要求 33 至 35 任一项所述的交互装置，其中，所述基于第一安全要件执行第一操作，包括：

35 所述第一执行模块基于所述第一安全要件以及第一计算参数执行所述第一操作，所述第一计算参数包括以下至少一项：

终端核心网上下文中的信息；

终端接入网上下文中的信息；

所述第一标识信息；

40 第一安全辅助信息中的至少部分内容。

37. 一种交互装置，应用于接入网节点，其中，包括：

第一发送模块，用于发送目标无线信令，所述目标无线信令包括第一标识信息以及第一目标信息，所述第一目标信息包括加密信息与完整性保护信息中的至少一项；

45 其中，所述加密信息和完整性保护信息基于第一安全要件生成，所述第一安全要件包括秘钥和密流中的至少一项。

38. 根据权利要求 37 所述的交互装置，其中，所述交互装置还包括：

第二接收模块，用于在所述第一发送模块发送目标无线信令之前，从核心网节点接收第三信息或目标数据；

其中，所述第三信息包括第二标识信息和第二目标信息；

所述第二目标信息包括以下至少一项：

5 所述第一安全要件或第三安全要件，所述第三安全要件包括秘钥和密流中的至少一项；

第一算法信息；

第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

10 其中，所述第二标识信息用于指示终端，或由终端标识生成，或指示一组终端，或与
所述第一标识信息相关；所述第一算法信息包括以下至少一项：

安全要件派生算法、机密性算法、和完整性算法。

39. 根据权利要求 38 所述的交互装置，其中，所述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

至少一对第二标识信息与第二目标信息；

15 其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

或者，所述第二标识信息与所述第二目标信息为一到零或一映射；

或者，K 个第二标识信息与所有第二目标信息存在对应关系，且 K 小于或等于所述第三信息中包含的第二标识信息的数量。

40. 一种交互装置，应用于核心网节点，其中，包括：

20 第二发送模块，用于向接入网节点发送第三信息或目标数据，所述第三信息包括第二
标识信息和第二目标信息；

其中，所述第二目标信息包括以下至少一项：

第一安全要件或第三安全要件；

第一算法信息；

25 第二安全参数；

第二安全辅助信息，所述第二安全辅助信息包括终端核心网上下文中的信息；

其中，所述第一算法信息包安全要件派生算法、机密性算法、和完整性算法中的至少
一项；所述第一安全要件包括秘钥和密流中的至少一项，所述第三安全要件包括秘钥和密
流中的至少一项，所述第二标识信息指示终端。

30 41. 根据权利要求 40 所述的交互装置，其中，所述交互装置还包括：

第三执行模块，用于基于第三派生信息和所述安全要件派生算法中的至少一项生成所
述第一安全要件或所述第三安全要件；

35 其中，所述第三派生信息包括以下至少一项：核心网相关密钥、NAS 层相关密钥、终
端上下文中的密钥、所述第一算法信息、所述第二安全参数、和所述第二安全辅助信息中的
至少部分内容。

42. 根据权利要求 40 或 41 所述的交互装置，其中，所述第三信息包括以下至少一项：

至少一个第二标识信息和至少一个第二目标信息；

至少一对第二标识信息与第二目标信息；

其中，所述第二目标信息与所述第二标识信息为一到一或多映射；

40 或者，所述第二标识信息与所述第二目标信息为一到零或一映射；

或者，K 个第二标识信息与所有第二目标信息存在对应关系，且 K 小于或等于第二标
识信息的数量。

43. 根据权利要求 40 至 42 中任一项所述的交互装置，其中，所述交互装置还包括：

45 第三接收模块，用于从所述终端接收第二算法信息，所述第二算法信息用于指示以下
至少一项：所述终端支持的算法、所述终端使用的算法；

其中，所述第一算法信息基于所述第二算法信息生成。

44. 一种终端，其中，包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如权利要求 1 至 12 任一项所述的交互方法的步骤。

5 45. 一种网络侧设备，其中，包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如权利要求 13 至 32 任一项所述的交互方法的步骤。

46. 一种交互系统，其中，包括：网络侧设备和终端，其中，

所述网络侧设备被配置用于执行如权利要求 13 至 32 任一项所述的交互方法的步骤，所述终端被配置用于执行如权利要求 1 至 12 任一项所述的交互方法的步骤。

10 47. 一种可读存储介质，其中，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如权利要求 1 至 32 任一项所述的交互方法的步骤。

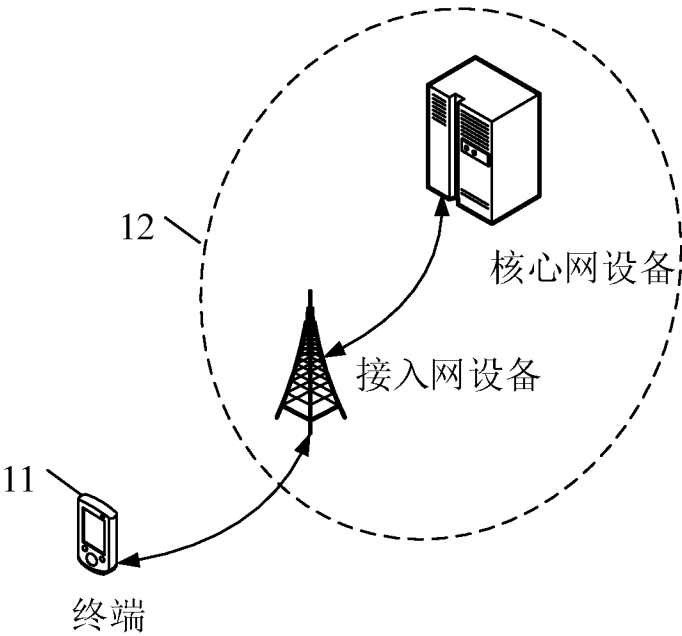


图 1

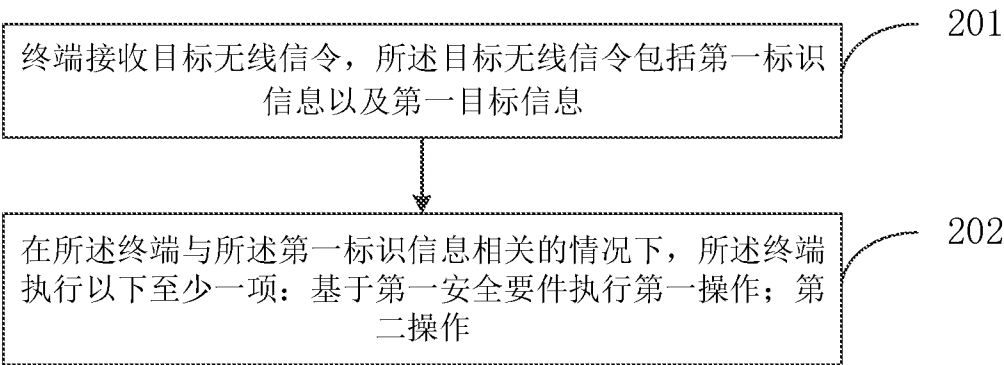


图 2

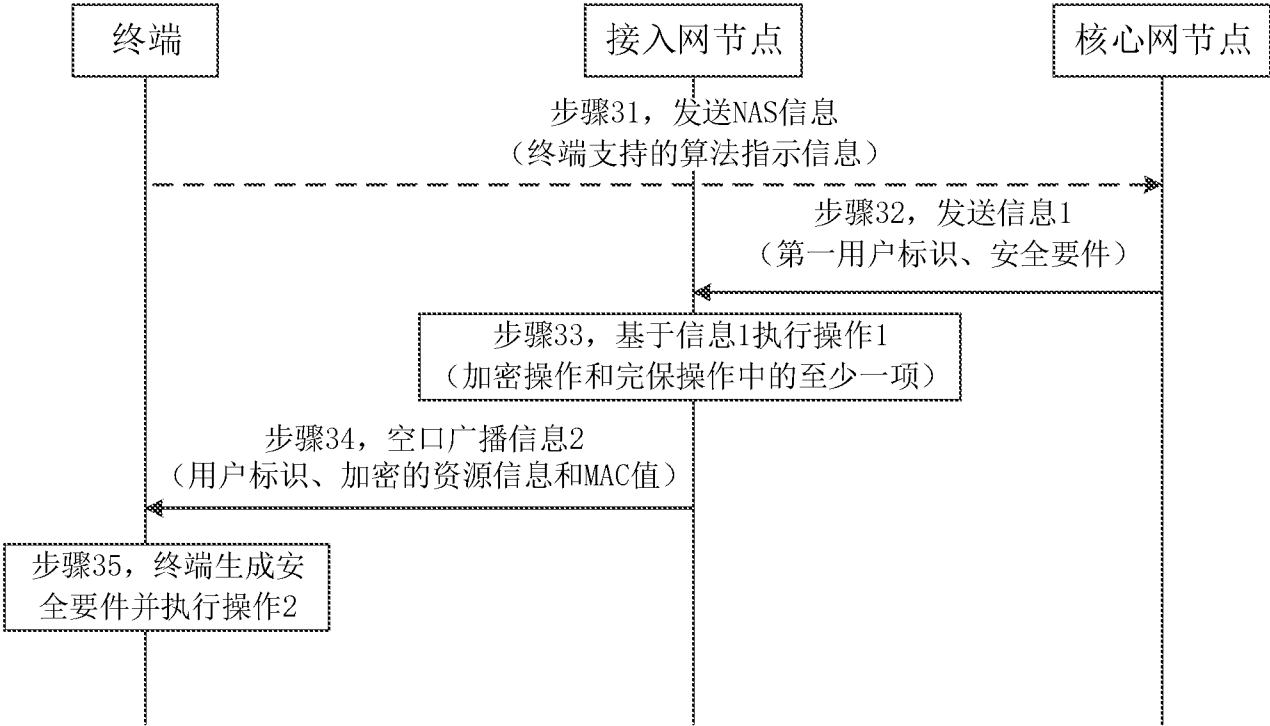


图 3

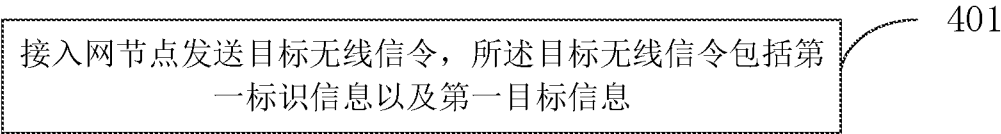


图 4

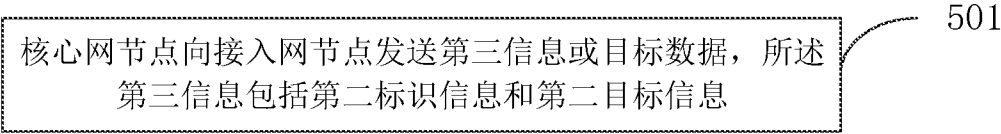


图 5

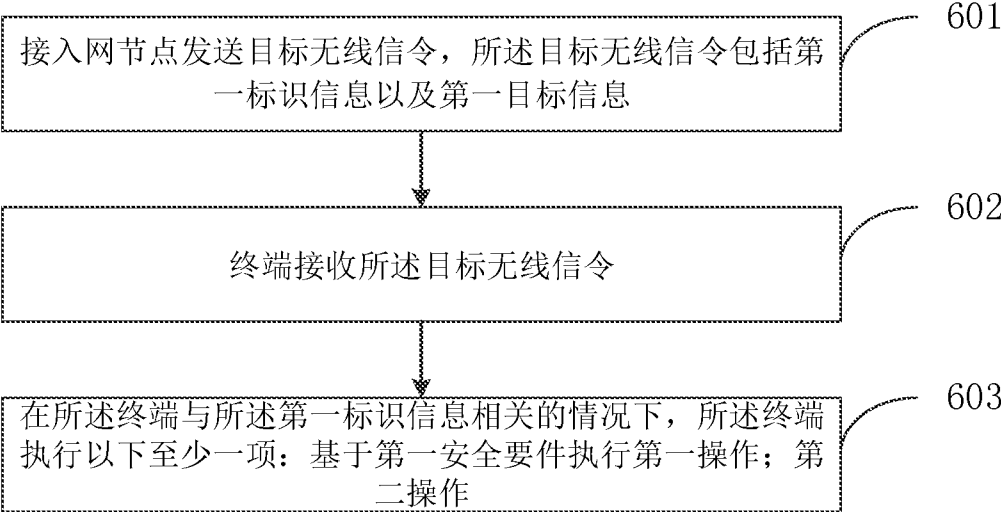


图 6

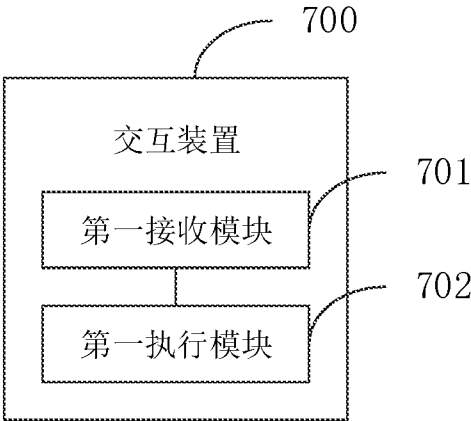


图 7

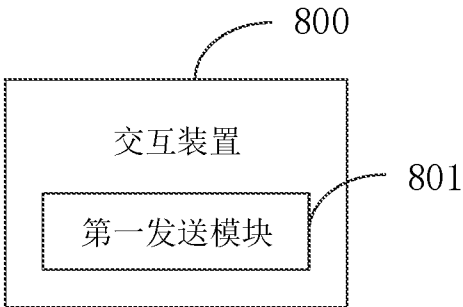


图 8

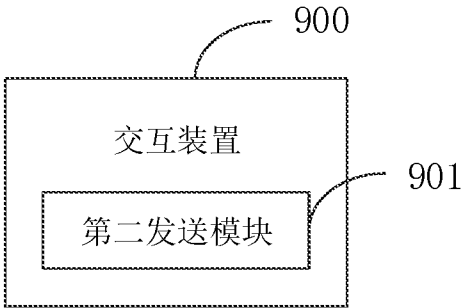


图 9

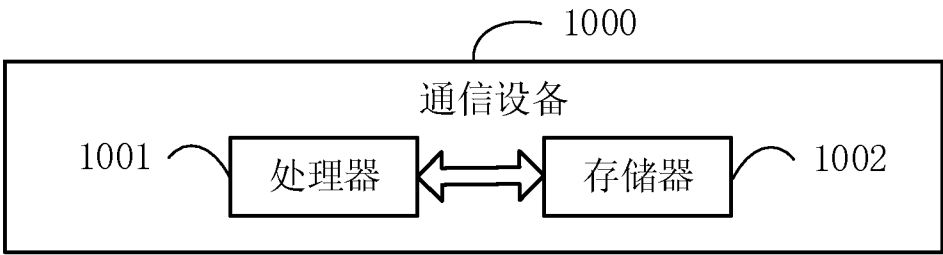


图 10

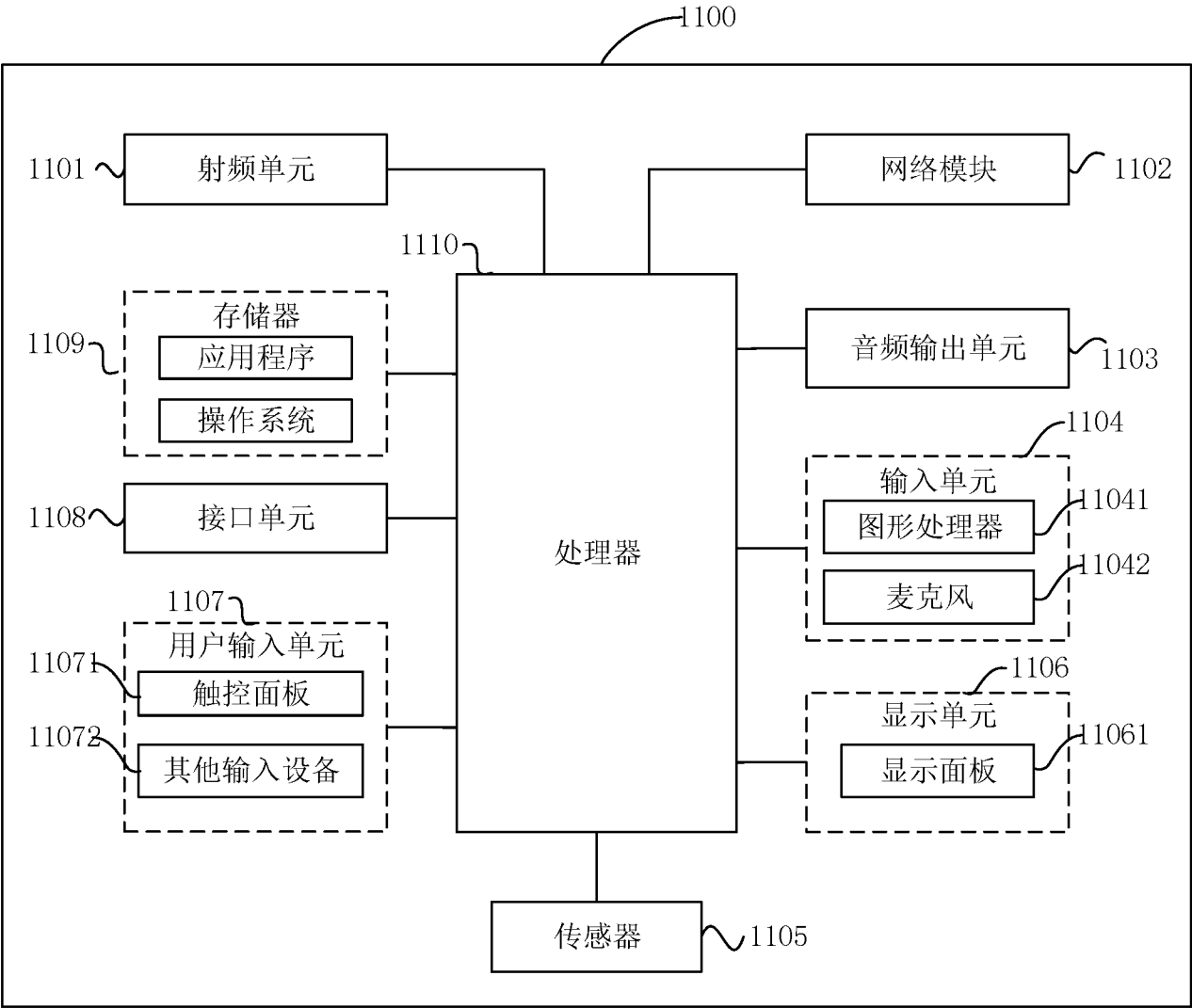


图 11

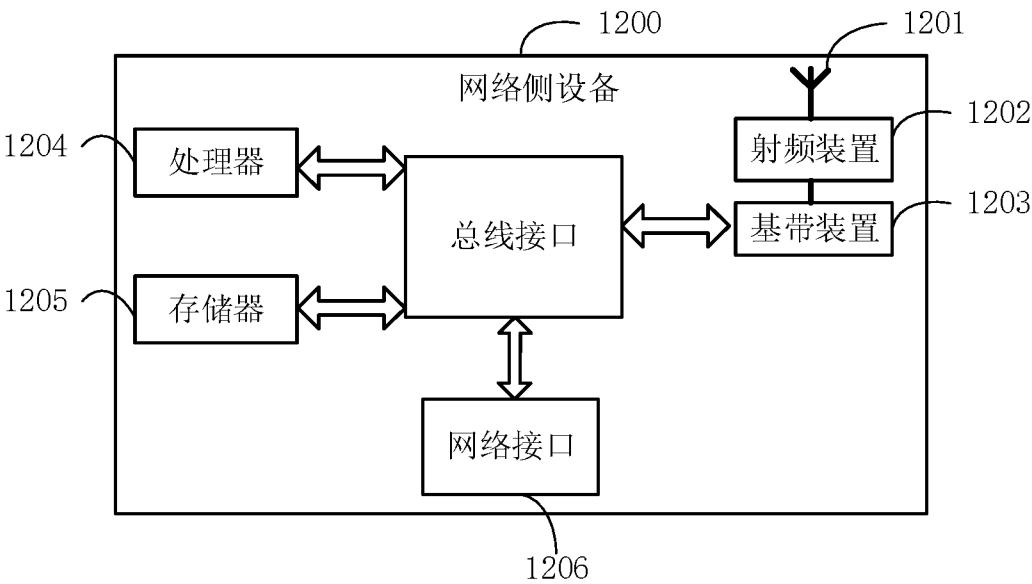


图 12

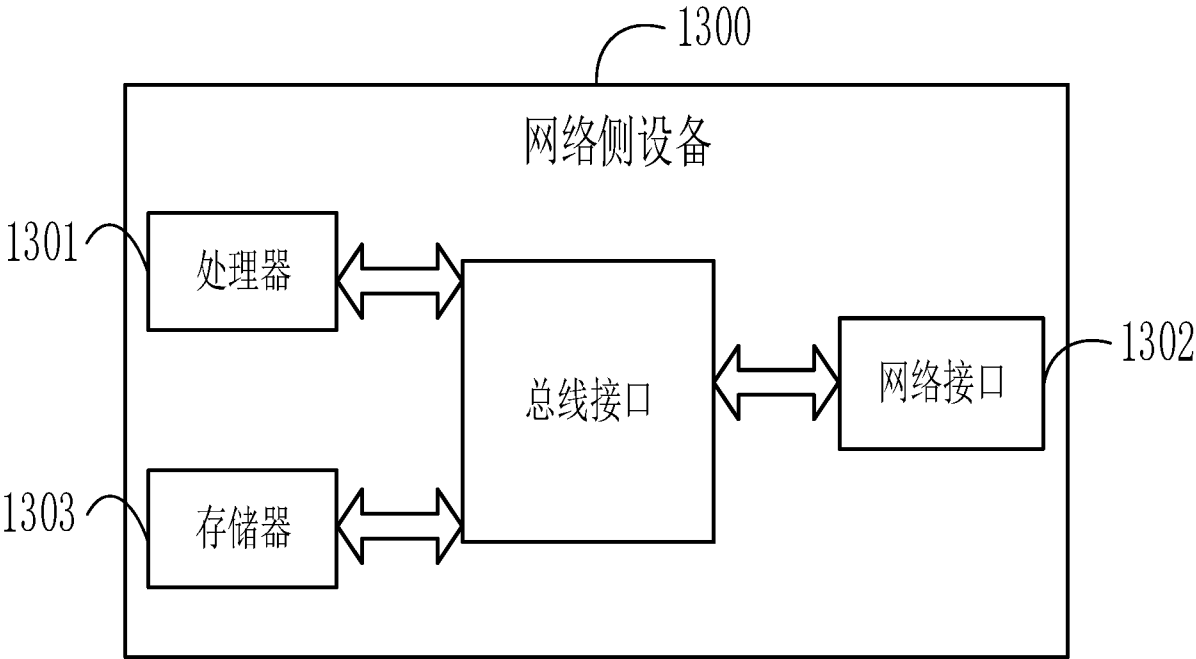


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/137563

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/037(2021.01)i; H04W12/03(2021.01)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)

IPC: H04W H04L

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)

CNXTX, ENTXTTC, ENTXT, DWPI: 小数据, 小包, 时延, 延时, 延迟, 标识, id, 名称, 相关, 关联, 相同, 一致, 对应, 匹配, 用户, 终端, 组, 密钥, 密流, 秘钥, 加密, 完整, SDT, delay, latency, id, TMSI, RNTI, name, same, relat+, correspond+, UE, terminal, MTC, KeyStream, Kausf, Kseaf, Kamf, Kasme, key, ciper

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 115696319 A (HUAWEI TECHNOLOGIES CO., LTD.) 03 February 2023 (2023-02-03) description, paragraphs 58-146 and 180-192, and figures 1 and 4	1-47
A	CN 108347726 A (ZTE CORP.) 31 July 2018 (2018-07-31) entire document	1-47
A	US 2021329452 A1 (NEC CORP.) 21 October 2021 (2021-10-21) entire document	1-47
A	US 2023073757 A1 (NOKIA TECHNOLOGIES OY) 09 March 2023 (2023-03-09) entire document	1-47
A	WO 2023143418 A1 (VIVO MOBILE COMMUNICATION CO., LTD.) 03 August 2023 (2023-08-03) entire document	1-47



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
“D” document cited by the applicant in the international application
“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

27 February 2025

Date of mailing of the international search report

05 March 2025

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2024/137563

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115696319	A	03 February 2023	WO	2023005929	A1	02 February 2023
				EP	4369762	A1	15 May 2024
				US	2024163674	A1	16 May 2024
CN	108347726	A	31 July 2018	WO	2018137617	A1	02 August 2018
US	2021329452	A1	21 October 2021	EP	3849228	A1	14 July 2021
				WO	2020050138	A1	12 March 2020
				JPWO	2020050138	A1	26 August 2021
				JP	7127689	B2	30 August 2022
US	2023073757	A1	09 March 2023	WO	2021156347	A1	12 August 2021
WO	2023143418	A1	03 August 2023	CN	116567625	A	08 August 2023

A. 主题的分类

H04W 12/037(2021.01)i; H04W12/03(2021.01)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)

IPC: H04W H04L

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))

CNTEXT, ENTXTC, ENTXT, DWPI: 小数据,小包,时延,延时,延迟,标识,id,名称,相关,关联,相同,一致,对应,匹配,用户,终端,组,密钥,密流,秘钥,加密,完整,SDT, delay, latency, id, TMSI, RNTI, name, same, relat+, correspond+, UE, terminal, MTC, KeyStream, Kausf, Kseaf, Kamf, Kasme, key, ciper

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
X	CN 115696319 A (华为技术有限公司) 2023年2月3日 (2023 - 02 - 03) 说明书第58-146、180-192段, 图1、4	1-47
A	CN 108347726 A (中兴通讯股份有限公司) 2018年7月31日 (2018 - 07 - 31) 全文	1-47
A	US 2021329452 A1 (NEC CORP.) 2021年10月21日 (2021 - 10 - 21) 全文	1-47
A	US 2023073757 A1 (NOKIA TECHNOLOGIES OY) 2023年3月9日 (2023 - 03 - 09) 全文	1-47
A	WO 2023143418 A1 (VIVO MOBILE COMMUNICATION CO., LTD.) 2023年8月3日 (2023 - 08 - 03) 全文	1-47

☐ 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

“D” 申请人在国际申请中引证的文件

“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

2025年2月27日

国际检索报告邮寄日期

2025年3月5日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

陈晓伟

电话号码 (+86) 010-53961673

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/137563

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	115696319	A	2023年2月3日	WO	2023005929	A1	2023年2月2日
				EP	4369762	A1	2024年5月15日
				US	2024163674	A1	2024年5月16日
CN	108347726	A	2018年7月31日	WO	2018137617	A1	2018年8月2日
US	2021329452	A1	2021年10月21日	EP	3849228	A1	2021年7月14日
				WO	2020050138	A1	2020年3月12日
				JPWO	2020050138	A1	2021年8月26日
				JP	7127689	B2	2022年8月30日
US	2023073757	A1	2023年3月9日	WO	2021156347	A1	2021年8月12日
WO	2023143418	A1	2023年8月3日	CN	116567625	A	2023年8月8日