

(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 19 日 (19.06.2025)



(10) 国际公布号
WO 2025/124347 A1

(51) 国际专利分类号:
H04W 12/04 (2021.01) H04W 12/03 (2021.01)

(21) 国际申请号: PCT/CN2024/137854

(22) 国际申请日: 2024 年 12 月 9 日 (09.12.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311731505.0 2023年12月14日 (14.12.2023) CN

(71) 申请人: 展讯通信(上海)有限公司
(**SPREADTRUM COMMUNICATIONS (SHANGHAI) CO., LTD.**) [CN/CN]; 中国上海市浦东新区中国
(上海) 自由贸易试验区祖冲之路 2288 弄
展讯中心1号楼 201203 (CN)。

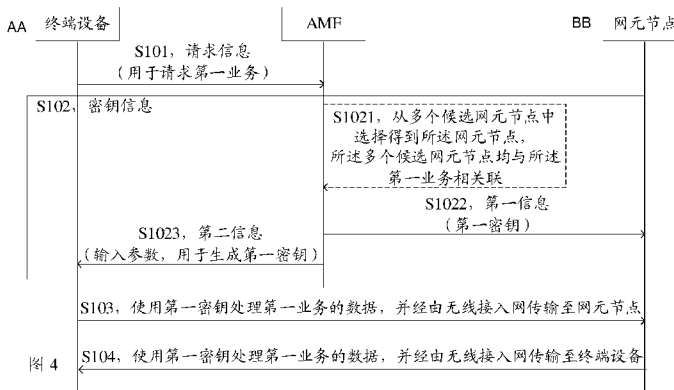
(72) 发明人: 刘星 (**LIU, Xing**); 中国上海市浦东新区
中国(上海) 自由贸易试验区祖冲之路 2288
弄展讯中心1号楼 201203 (CN)。

(74) 代理人: 北京同立钧成知识产权代理有限公司(**LEADER PATENT & TRADEMARK FIRM**);
中国北京市海淀区西直门北大街 32 号枫
蓝国际A座8F-6 100082 (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,

(54) **Title:** COMMUNICATION METHOD AND APPARATUS, AND COMPUTER READABLE STORAGE MEDIUM

(54) 发明名称: 通信方法及装置、计算机可读存储介质



S101 REQUEST INFORMATION (USED FOR REQUESTING A FIRST SERVICE)
S102 KEY INFORMATION
S103 USE A FIRST KEY TO PROCESS DATA OF THE FIRST SERVICE, AND TRANSMIT THE PROCESSED
DATA TO A NETWORK ELEMENT NODE VIA A WIRELESS ACCESS NETWORK
S104 USE THE FIRST KEY TO PROCESS THE DATA OF THE FIRST SERVICE, AND TRANSMIT THE
PROCESSED DATA TO A TERMINAL DEVICE VIA THE WIRELESS ACCESS NETWORK
S1021 PERFORM SELECTION FROM A PLURALITY OF CANDIDATE NETWORK ELEMENT NODES TO
OBTAIN THE NETWORK ELEMENT NODE, THE PLURALITY OF CANDIDATE NETWORK ELEMENT
NODES BEING ALL ASSOCIATED WITH THE FIRST SERVICE
S1022 FIRST INFORMATION (THE FIRST KEY)
S1023 SECOND INFORMATION (AN INPUT PARAMETER, USED FOR GENERATING THE FIRST KEY)
AA TERMINAL DEVICE
BB NETWORK ELEMENT NODE

(57) **Abstract:** A communication method and apparatus, and a computer readable storage medium, relating to the technical field of communications. The method comprises: receiving request information, the request information being used for requesting a first service; and sending key information, the key information being used for indicating a first key, and the first key being used for encrypting data of the first service transmitted between a network element node and a terminal device. By means of the solution of the present disclosure, a proper encryption mechanism can be provided for a service-based RAN architecture, and data between a core network element and a terminal device can still be guaranteed to be securely transmitted without passing through an AMF.

[见续页]

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, 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, 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: 一种通信方法及装置、计算机可读存储介质, 涉及通信技术领域, 该方法包括: 接收请求信息, 该请求信息用于请求第一业务; 发送密钥信息, 该密钥信息用于指示第一密钥, 该第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。通过本公开方案能够为服务化RAN架构提供合适的加密机制, 在核心网网元和终端设备之间的数据传输不经过AMF的情况下仍能保证安全性。

通信方法及装置、计算机可读存储介质

本申请要求于 2023 年 12 月 14 日提交中国专利局、申请号为 202311731505.0、申请名称为“通信方法及装置、计算机可读存储介质”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，具体地涉及一种通信方法及装置、计算机可读存储介质。

背景技术

当前，终端设备和核心网的网元之间的交互需要通过访问和移动性管理功能（Access and Mobility Management Function，AMF）转发，安全性由 AMF 的加密机制来保护。

未来有极大可能引入服务化无线接入网（Radio access network，RAN），核心网网元和 AMF 之间的嵌套关系会被突破，终端设备可以和核心网网元直接交互而无需经过 AMF 中转。此时，AMF 无法再实现加密功能，终端设备和核心网网元之间的业务安全性无法得到保障。

发明内容

本申请可以解决的技术问题是如何确保服务化 RAN 架构下的业务安全性。

为解决上述技术问题，本申请实施例提供一种通信方法，包括：接收请求信息，所述请求信息用于请求第一业务；发送密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。

可选的，所述发送密钥信息包括：向所述网元节点发送第一信息，所述第一信息包括所述第一密钥。

可选的，在向网元节点发送第一信息之前，所述方法还包括：从多个候选网元节点中选择得到所述网元节点，所述多个候选网元节点均与所述第一业务相关联。

可选的，所述发送密钥信息包括：向所述终端设备发送第二信息，所述第二信息包括输入参数，所述输入参数用于生成所述第一密钥。

可选的，所述输入参数包括：所述网元节点的标识和/或所述网元节点的地址。

可选的，所述请求信息接收自服务器或者所述终端设备。

可选的，所述网元节点选自：定位管理功能节点以及感知功能节点。

为解决上述技术问题，本申请实施例还提供一种通信方法，包括：接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述网元节点。

可选的，所述接收密钥信息包括：接收第二信息，所述第二信息包括输入参数，所述输入参数用于生成所述第一密钥。

可选的，所述输入参数包括：所述网元节点的标识和/或所述网元节点的网络互连协议地址。

5 可选的，所述方法还包括：发送请求信息，所述请求信息用于请求第一业务。

为解决上述技术问题，本申请实施例还提供一种通信方法，包括：接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述终端设备。

10 可选的，所述接收密钥信息包括：接收第一信息，所述第一信息包括所述第一密钥。

可选的，所述网元节点选自：定位管理功能节点以及感知功能节点。

为解决上述技术问题，本申请实施例还提供一种通信装置，包括：接收模块，用于接收请求信息，所述请求信息用于请求第一业务；发送模块，用于发送密钥信息，
15 所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。

为解决上述技术问题，本申请实施例还提供一种通信装置，包括：接收模块，用于接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；传输模块，用于使用所述第一密钥处理所述
20 所述第一业务的数据，并经由无线接入网传输至所述网元节点。

为解决上述技术问题，本申请实施例还提供一种通信装置，包括：接收模块，用于接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；传输模块，用于使用所述第一密钥处理所述
25 所述第一业务的数据，并经由无线接入网传输至所述终端设备。

为解决上述技术问题，本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质为非易失性存储介质或非瞬态存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时执行上述方法的步骤。

为解决上述技术问题，本申请实施例还提供一种通信装置，包括存储器和处理器，所述存储器上存储有可在所述处理器上运行的计算机程序，所述处理器运行所述计算机程序时执行上述方法的步骤。
30

与现有技术相比，本申请实施例的技术方案具有以下有益效果：

在 AMF 侧，本申请实施例提供一种通信方法，包括：接收请求信息，所述请求信息用于请求第一业务；发送密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。

35 相较于现有技术中 AMF 作为中转节点在为终端设备和核心网网元转发消息/数据时完成加密，本实施方案涉及的第一业务为服务化 RAN 架构下进行的业务，由于此时 AMF 不起到数据中转功能，因而通过将密钥信息发送给通信的双方（例如，终端设备和网元节点），确保通信各方能够正确加解密传输的数据。由此，为服务化 RAN 架构提供合适的加密机制，在核心网网元和终端设备之间的数据传输不经过 AMF 的情况

下仍能保证安全性。

在终端设备侧，本申请实施例还提供一种通信方法，包括：接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述网元节点。

相较于现有技术中终端设备只需收发由 AMF 解加密的数据，本实施方案通过将 AMF 侧配置的第一密钥指示给终端设备，使得终端设备在通过 RAN 和网元节点通信期间，能够正确加解密传输的数据。由此，为服务化 RAN 架构提供合适的加密机制，在核心网网元和终端设备之间的数据传输不经过 AMF 的情况下仍能保证安全性。

在核心网侧，本申请实施例还提供一种通信方法，包括：接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述终端设备。

相较于现有技术中网元节点只需收发由 AMF 解加密的数据，本实施方案通过将 AMF 侧配置的第一密钥指示给网元节点，使得网元节点在通过 RAN 和终端设备通信期间，能够正确加解密传输的数据。由此，为服务化 RAN 架构提供合适的加密机制，在核心网网元和终端设备之间的数据传输不经过 AMF 的情况下仍能保证安全性。

附图说明

图 1 是本申请第一种服务化 RAN 的架构示意图；
图 2 是本申请第二种服务化 RAN 的架构示意图；
图 3 是本申请第三种服务化 RAN 的架构示意图；
图 4 是本申请实施例一种通信方法的信令交互图；
图 5 是本申请实施例一种通信装置的结构示意图；
图 6 是本申请实施例另一种通信装置的结构示意图；
图 7 是本申请实施例又一种通信装置的结构示意图。

具体实施方式

如背景技术所言，在服务化 RAN 架构下，现有通过 AMF 实现的加密功能不再适用，终端设备和核心网网元之间的业务安全性无法得到保障。

具体而言，现有终端设备和核心网的网元之间的交互，通过 AMF 转发。以定位业务举例，定位管理服务器（也称，位置管理功能 Location management function, LMF）和终端设备之间没有直接接口。出于业务安全性考虑，定位业务的数据（例如，包括定位请求和定位报告）需要被加密，由于终端设备和 LMF 之间的交互必然经过 AMF，因此可以通过 AMF 加密。

考虑到 6G 会引入服务化架构，其中一种选项是 RAN 直接接入核心网，不再通过 AMF 转发。因而，需要为服务化 RAN 的架构设计新的加密机制。

为解决上述技术问题，本申请实施例提供一种通信方法，包括：接收请求信息，所述请求信息用于请求第一业务；发送密钥信息，所述密钥信息用于指示第一密钥，

所述第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。

本实施方案涉及的第一业务为服务化 RAN 架构下进行的业务，由于此时 AMF 不
起到数据中转功能，因而通过将密钥信息发送给通信的双方（例如，终端设备和网元
节点），确保通信各方能够正确加解密传输的数据。由此，为服务化 RAN 架构提供合
5 适的加密机制，在核心网网元和终端设备之间的数据传输不经过 AMF 的情况下仍能
保证安全性。

本申请实施例中服务化 RAN 架构可以如图 1 至图 3 中的任一种所示。

图 1 示例性的展示 N2 接口全服务化下的网络架构，可以实现接入网网络功能
（RAN Network Function，RAN NF）和核心网网络功能（Core Network NF，CN NF）
10 之间的直接服务调用。具体而言，终端设备（图中以 UE 标识）可以通过 AMF 接入总
线（即访问核心网）。进一步，终端设备还可以通过 RAN 直接访问核心网，从而突破
现有 AMF 唯一转发的机制。RAN 包括控制面 RAN（图中以 RAN-C 标识）以及用户
面 RAN（图中以 RAN-U 标识）。进一步，图 1 所示架构中，核心网侧的应用功能
（Application Function，AF）、网络存储功能（Network Repository Function，NRF）、
15 策略控制功能（Policy Control Function，PCF）以及统一数据管理功能（Unified Data
Management，UDM）也直接接入总线。进一步，用户面功能（User Plane Function，简
称 UPF）以及数据网络（Data Network，DN）可以通过会话管理功能（Session Management
Function，简称 SMF）接入总线。

图 2 示例性的展示针对传统 RAN 功能的服务化的网络架构，将功能（也称，RAN
能力）拆分为服务，并进一步实现 RAN 和 CN 相关功能服务与流程的融合设计，以更
20 好满足高内聚、松耦合的设计原则，精简网络设计。具体而言，终端设备（图中以 UE
标识）可以通过 AMF 接入总线。进一步，终端设备还可以通过无线电单元（Radio Unit，
RU）访问 RAN，并经由 RAN 直接访问核心网，其中，RU 负责处理数字前端（DFE）
和部分物理（PHY）层功能。进一步，RAN 拆分为 RAN 控制面服务（基于控制面服
25 务（Control Plane Service，CPS）实现）和 RAN 用户面服务（基于用户面服务（User
Plane Service，UPS）实现）。进一步，设置核心网用户面服务（基于 UPS 实现），与
RAN 相通信并直接接入总线。进一步，其他诸如 AF、NRF、PCF 和 UDM 之类的核心
网网元直接接入总线。进一步，SMF 也可直接接入总线。进一步，DN 通过核心网用
户面服务接入总线。

图 3 示例性的展示针对新增 DOICT 能力的服务化的网络架构，该架构将人工智能
（Artificial Intelligence，简称 AI）、计算、数据等功能定义为服务。其中，DOICT 通
过通信技术（Communication Technology，CT）技术来简化现场网组网；通过运营技术
（Operational Technology，OT）技术，与工业协议深度协同实现高可靠性；通过数据
30 技术（Data technology，DT）技术实现智能化，闭环保障低时延体验；通过信息技术
（Information Technology，IT）技术使能更多工业应用，降低建设成本，实现灵活组网。
具体而言，终端设备通过 RU 访问 RAN，并经由 RAN 直接访问核心网。进一步，RAN
拆分为 RAN 控制面服务（基于网络物理系统（Cyber Physical System，CPS）实现）、
RAN 用户面服务（基于用户面物理系统（User Physical System，UPS）实现），以及
多维能力服务化（包括 AI 服务、计算服务和数据服务）。进一步，AMF 接入总线并

与终端设备解耦。进一步，其他诸如网络开放功能（Network Exposure Function, NEF）、AF、NRF、PCF 和 UDM 之类的核心网网元直接接入总线。进一步，SMF 也可直接接入总线。进一步，DN 通过 UPF 接入总线，UPF 与 RAN 相通信。

本申请实施例中，网元节点可以是执行第一业务相关功能的核心网网元。第一业务可以是基于服务化 RAN 架构实现的业务。例如，第一业务可以为定位业务，相应的网元节点可以为定位管理功能（LMF）节点（简称 SMF）。又如，第一业务可以为通感（也称感知，sensing）业务，相应的网元节点可以为感知功能（Sensing Function, SF）节点（简称 SF）。

本申请实施例中，AMF 虽然不再在终端设备和网元节点之间转发数据，但还是起到管理功能。

为使本申请的上述目的、特征和有益效果能够更为明显易懂，下面结合附图对本申请的具体实施例做详细的说明。

图 4 是本申请实施例一种通信方法的信令交互图。

本实施方案可以应用于服务化 RAN 架构下的通信场景，终端设备直接经由 RAN 和网元节点交互以传输第一业务的数据，无需经过 AMF 中转。

在具体实施中，下述步骤 S101~步骤 S102 所提供的通信方法中，由终端设备实现的步骤，可以由终端设备中的具有通信功能的芯片执行，也可以由终端设备中的基带芯片执行；由 AMF 实现的步骤，可以由 AMF 中的具有通信功能的芯片执行，也可以由 AMF 中的基带芯片执行；由网元节点实现的步骤，可以由网元节点中的具有通信功能的芯片执行，也可以由网元节点中的基带芯片执行。

具体地，参考图 4，本实施方案所述通信方法可以包括如下步骤：

步骤 S101，终端设备向 AMF 发送请求信息。相应的，AMF 接收请求信息。其中，请求信息用于请求第一业务。

例如，第一业务可以为定位业务，相应的，请求信息可以为定位请求信息。

在一些实施例中，可以由终端设备主动触发请求信息的发送。

在一些实施例中，可以由服务器触发终端设备向 AMF 发送请求信息。其中，服务器可以例如是外部服务器，用于实现第一业务。

在一些实施例中，可以由服务器直接向 AMF 发送请求信息。

在一些实施例中，请求的第一业务可以是上行业务，也可以是下行业务。

在一些实施例中，请求信息可以包括实现第一业务的相关信息，如终端设备的标识（用于唯一识别终端设备）、服务质量（Quality of Service, 简称 QoS）。

仍以终端设备请求定位业务为例，步骤 S101 中发送的定位请求信息可以包括终端设备的标识、定位的 QoS（如定位的精度要求、时延要求等）。

在一个具体实施中，继续参考图 4，响应于接收到请求信息，AMF 可以执行步骤 S102，分别向终端设备和网元节点发送密钥信息。相应的，网元节点和终端设备各自接收密钥信息。其中，密钥信息用于指示第一密钥，第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据。

在一些实施例中，对于网元节点和 AMF 之间的交互，步骤 S102 具体可以包括步骤 S1021 和步骤 S1022。

步骤 S1021 中，AMF 从多个候选网元节点中选择得到网元节点，多个候选网元节点均与第一业务相关联。

具体而言，核心网针对第一业务可以部署多个网元节点，这些网元节点作为候选网元节点。AMF 在接收到请求信息后，从多个候选网元节点中择一确定为与终端设备相通信的网元节点。

仍以定位请求信息为例，AMF 可以从多个候选 LMF 中就近选择一个，确定为与终端设备相通信以实现定位业务的 LMF。

又例如，请求信息可以用于请求感知业务，AMF 可以从多个候选 SF 中择一确定为与终端设备相通信以实现感知业务的 SF。

进一步，在确定网元节点后，AMF 可以继续执行步骤 S1022，向网元节点发送第一信息。相应的，网元节点接收第一信息。其中，第一信息包括第一密钥。

由此，AMF 直接向网元节点提供生成好的第一密钥。

在一些实施例中，分配给不同候选网元节点的第一密钥可以互不重复。

在一个具体实施中，对于终端设备和 AMF 之间的交互，步骤 S102 具体可以包括步骤 S1023，AMF 向终端设备发送第二信息。相应的，终端设备接收第二信息。其中，第二信息包括输入（input）参数，所述输入参数用于生成所述第一密钥。

具体而言，输入参数中的一部分可以由网络预配置或协议预定义或由终端设备自行确定，剩余部分（例如，与网元节点相关的参数）可以由 AMF 指示给终端设备。

仍以第一业务为定位业务为例，LMF 的密钥（KLMF）的派生需要用到的输入参数可以包括：

- FC = 0x6E，用于区分不同的派生算法；
- P0 = 上/下行非接入层（Non-Access Stratum, NAS）计数（Uplink/Downlink NAS COUNT），为终端设备和 AMF 传递信令时的序列号；
- L0 = 上/下行 NAS 计数的长度（length of uplink/downlink NAS COUNT），例如 0x00 0x04；
- P1 = 网络功能标识（Network function distinguisher），用于区分不同的网络功能；
- L1 = 网络功能标识的长度（length of Network function distinguisher），例如 0x00 0x01。

在一些实施例中，第二信息中携带的输入参数可以包括 P1 参数。由于 P1 参数用于区分不同的网络功能，因而也可称为网元节点的标识（本示例中，可以理解为类型标识），以区分不同功能的网元节点。例如，LMF 对应的 P1 值为 0x01，SF 对应的 P1 值为 0x02。

在一个变化例中，P1 参数的内容可以为网元节点的身份标识（Identification, ID），用于唯一标识候选网元节点。例如，核心网侧包括多个候选 LMF，其中每一候选 LMF 分配有各自唯一的 ID。AMF 从多个候选 LMF 中选定一个后，将选定的 LMF 的 ID 通过第二信息指示给终端设备。

在一个变化例中，P1 参数的内容可以替换为网络功能地址（Network function address），相应的，L1 参数的内容可以替换为网络功能地址的长度（length of Network

function address)。

网元节点的地址可以例如是网络互连协议 (Internet Protocol, 简称 IP) 地址, 还可以例如是媒体访问控制 (Medium Access Control, MAC) 地址。

在另一个变化例中, 除了 P1 参数外, LMF 的密钥 (KLMF) 的派生需要用到的输入参数还可以包括 P2=网络功能地址, 以及 L2=网络功能地址的长度。进一步, 第二信息可以包括 P1 参数以及 P2 参数。

在一个具体实施中, AMF 通过在第二信息中指示第一业务关联的网元节点的标识 (包括类型标识和/或身份标识) 和/或地址, 供终端设备生成用于与该网元节点交互的第一密钥。

例如, 响应于接收到第二信息, 终端设备根据全球用户识别卡 (Universal Subscriber Identity Module, USIM) 里配置的 K 值和网络提供的动态参数, 计算 KAMF。进一步, 结合输入参数 (包括第二信息中携带的内容 (如 P1 和/或 P2) 以及终端设备自行确定的内容) 计算得到第一密钥。

在一些实施例中, 向终端设备发送第二信息 (对应步骤 S1023) 的动作, 可以在向网元节点发送第一信息 (对应步骤 S1021 和步骤 S1022) 的动作之前/之后/同时执行。

在一个具体实施中, 响应于分别接收到第一信息和第二信息, 网元节点和终端设备可以使用第一密钥经由 RAN 进行直接通信。

具体而言, 响应于接收到第二信息, 终端设备可以执行步骤 S103, 以使用第一密钥处理第一业务的数据, 并经由 RAN 传输至网元节点。

类似的, 响应于接收到第一信息, 网元节点可以执行步骤 S104, 以使用第一密钥处理第一业务的数据, 并经由 RAN 传输至终端设备。

在一个变化例中, 步骤 S101 可以被省略, AMF 可以在终端设备接入时即主动向其发送密钥信息。进一步, AMF 还可以向终端设备需要实现的第一业务对应的网元节点也主动发送密钥信息。

在一个变化例中, 步骤 S102 可以被省略。例如, 只有一个与第一业务相关联的网元节点, 则 AMF 可以直接执行步骤 S103, 以向该网元节点发送密钥信息。

由上, AMF 通过将密钥信息发送给通信的双方 (例如, 终端设备和网元节点), 确保通信各方能够正确加解密传输的数据。响应于接收到密钥信息 (例如, 第二信息), 终端设备在通过 RAN 和网元节点通信期间, 能够正确加解密传输的数据。响应于接收到密钥信息 (例如, 第一信息), 网元节点在通过 RAN 和终端设备通信期间, 能够正确加解密传输的数据。由此, 为服务化 RAN 架构提供合适的加密机制, 在核心网网元和终端设备之间的数据传输不经过 AMF 的情况下仍能保证安全性。

图 5 是本申请实施例一种通信装置 2 的结构示意图。本领域技术人员理解, 本实施例所述通信装置 2 可以用于实施上述图 1 至图 4 所述实施例中所述的方法技术方案。

具体而言, 本实施例所述通信装置 2 可以包括: 接收模块 21, 用于接收请求信息, 所述请求信息用于请求第一业务; 发送模块 22, 用于发送密钥信息, 所述密钥信息用于指示第一密钥, 所述第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。

关于所述通信装置 2 的工作原理、工作方式的更多内容, 可以参照上述图 1 至图

4 中的相关描述，这里不再赘述。

在具体实施中，上述的通信装置 2 可以对应于网络设备中具有通信功能的芯片，或者对应于具有数据处理功能的芯片，例如片上系统(System-On-a-Chip, 简称 SOC)、基带芯片等；或者对应于网络设备中包括具有通信功能芯片的芯片模组；或者对应于具有数据处理功能芯片的芯片模组，或者对应于网络设备。本示例中，网络设备可以例如是 AMF。

图 6 是本申请实施例另一种通信装置 3 的结构示意图。本领域技术人员理解，本实施例所述通信装置 3 可以用于实施上述图 1 至图 4 所述实施例中所述的方法技术方案。

具体地，参考图 6，本实施例所述通信装置 3 可以包括：接收模块 31，用于接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；传输模块 32，用于使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述网元节点。

关于所述通信装置 3 的工作原理、工作方式的更多内容，可以参照上述图 1 至图 4 中的相关描述，这里不再赘述。

在具体实施中，上述的通信装置 3 可以对应于终端设备中具有通信功能的芯片，或者对应于具有数据处理功能的芯片，例如片上系统(System-On-a-Chip, 简称 SOC)、基带芯片等；或者对应于终端设备中包括具有通信功能芯片的芯片模组；或者对应于具有数据处理功能芯片的芯片模组，或者对应于终端设备。

图 7 是本申请实施例又一种通信装置 4 的结构示意图。本领域技术人员理解，本实施例所述通信装置 4 可以用于实施上述图 1 至图 4 所述实施例中所述的方法技术方案。

具体地，参考图 7，本实施例所述通信装置 4 可以包括：接收模块 41，用于接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；传输模块 42，用于使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述终端设备。

关于所述通信装置 4 的工作原理、工作方式的更多内容，可以参照上述图 1 至图 4 中的相关描述，这里不再赘述。

在具体实施中，上述的通信装置 4 可以对应于网络设备中具有通信功能的芯片，或者对应于具有数据处理功能的芯片，例如片上系统(System-On-a-Chip, 简称 SOC)、基带芯片等；或者对应于网络设备中包括具有通信功能芯片的芯片模组；或者对应于具有数据处理功能芯片的芯片模组，或者对应于网络设备。本示例中，网络设备可以例如是核心网网元（也即，网元节点）。

在具体实施中，关于上述实施例中描述的各个装置、产品包含的各个模块/单元，其可以是软件模块/单元，也可以是硬件模块/单元，或者也可以部分是软件模块/单元，部分是硬件模块/单元。

例如，对于应用于或集成于芯片的各个装置、产品，其包含的各个模块/单元可以都采用电路等硬件的方式实现，或者，至少部分模块/单元可以采用软件程序的方式实现，该软件程序运行于芯片内部集成的处理器，剩余的（如果有）部分模块/单元可以

采用电路等硬件方式实现；对于应用于或集成于芯片模组的各个装置、产品，其包含的各个模块/单元可以都采用电路等硬件的方式实现，不同的模块/单元可以位于芯片模组的同一组件（例如芯片、电路模块等）或者不同组件中，或者，至少部分模块/单元可以采用软件程序的方式实现，该软件程序运行于芯片模组内部集成的处理器，剩余的（如果有）部分模块/单元可以采用电路等硬件方式实现；对于应用于或集成于终端的各个装置、产品，其包含的各个模块/单元可以都采用电路等硬件的方式实现，不同的模块/单元可以位于终端内同一组件（例如，芯片、电路模块等）或者不同组件中，或者，至少部分模块/单元可以采用软件程序的方式实现，该软件程序运行于终端内部集成的处理器，剩余的（如果有）部分模块/单元可以采用电路等硬件方式实现。

本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质为非易失性存储介质或非瞬态存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时执行上述任一实施例提供的通信方法的步骤。优选地，所述存储介质可以包括诸如非挥发性（non-volatile）存储器或者非瞬态（non-transitory）存储器等计算机可读存储介质。所述存储介质可以包括 ROM、RAM、磁盘或光盘等。

本申请实施例还提供了另一种通信装置，包括存储器和处理器，所述存储器上存储有可在所述处理器上运行的计算机程序，所述处理器运行所述计算机程序时执行上述图 4 对应实施例所提供的通信方法的步骤。通信装置可以集成于终端/网络设备，或者，通信装置可以例如是终端/网络设备。

本申请技术方案可适用于第五代（5th Generation, 5G）通信系统，还可适用于第四代（4th Generation, 4G）、第三代（3rd Generation, 3G）通信系统，还可适用于未来新的各种通信系统，例如第六代（6th Generation, 6G）、第七代（7th Generation, 7G）等，本申请实施例对此并不限定。

本申请技术方案也适用于不同的网络架构，包括但不限于中继网络架构、双链接架构、车辆到任何物体的通信（Vehicle-to-Everything, V2X）架构、设备到设备的通信（Device-to-Device, D2D）等架构。

本申请实施例中的设备包含网络设备和终端设备。

本申请实施例中的网络设备包括接入网的基站和基站控制器，还可以包含终端设备。

本申请实施例中的基站（base station, BS），也可称为基站设备，是一种部署在无线接入网（RAN）用以提供无线通信功能的装置。例如在 2G 网络中提供基站功能的设备包括基地无线收发站（Base Transceiver Station, BTS），3G 网络中提供基站功能的设备包括节点 B（NodeB），在 4G 网络中提供基站功能的设备包括演进的节点 B（evolved NodeB, eNB），在无线局域网络（Wireless Local Area Networks, WLAN）中，提供基站功能的设备为接入点（Access Point, AP），5G 新无线（New Radio, NR）中的提供基站功能的设备 gNB，以及继续演进的节点 B（ng-eNB），其中 gNB 和终端设备之间采用 NR 技术进行通信，ng-eNB 和终端设备之间采用演进的通用地面无线接入（Evolved Universal Terrestrial Radio Access, E-UTRA）技术进行通信，gNB 和 ng-eNB 均可连接到 5G 核心网。本申请实施例中的基站还包含在未来新的通信系统中提供基站功能的设备等。

本申请实施例中的基站控制器，也可以称为基站控制器设备，是一种管理基站的装置，例如 2G 网络中的基站控制器（Base Station Controller, BSC）、3G 网络中的无线网络控制器（Radio Network Controller, RNC）、还可指未来新的通信系统中控制管理基站的装置。

- 5 本申请实施例中的终端设备，也可以称为终端，可以指各种形式的用户设备（User Equipment, 简称 UE）、接入终端设备、用户单元、用户站、移动站、移动台（Mobile Station, MS）、远方站、远程终端设备、移动设备、用户终端设备、无线通信设备、用户代理或用户装置。终端设备还可以是蜂窝电话、无绳电话、会话启动协议（Session Initiation Protocol, 简称 SIP）电话、无线本地环路（Wireless Local Loop, WLL）站、
- 10 个人数字处理（Personal Digital Assistant, PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，未来 5G 网络中的终端设备或者未来演进的公用陆地移动通信网络（Public Land Mobile Network, PLMN）中的终端设备等，本申请实施例对此并不限定。

- 15 虽然本申请披露如上，但本申请并非限定于此。任何本领域技术人员，在不脱离本申请的精神和范围内，均可作各种更动与修改，因此本申请的保护范围应当以权利要求所限定的范围为准。

权 利 要 求 书

- 1.一种通信方法，其特征在于，包括：
接收请求信息，所述请求信息用于请求第一业务；
发送密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元
5 节点和终端设备之间传输的所述第一业务的数据。
- 2.根据权利要求 1 所述的方法，其特征在于，所述发送密钥信息包括：
向所述网元节点发送第一信息，所述第一信息包括所述第一密钥。
- 3.根据权利要求 2 所述的方法，其特征在于，在向网元节点发送第一信息之前，
还包括：
10 从多个候选网元节点中选择得到所述网元节点，所述多个候选网元节点均与所述
第一业务相关联。
- 4.根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述发送密钥信息包
括：
向所述终端设备发送第二信息，所述第二信息包括输入参数，所述输入参数用于
15 生成所述第一密钥。
- 5.根据权利要求 4 所述的方法，其特征在于，所述输入参数包括：所述网元节点
的标识和/或所述网元节点的地址。
- 6.根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述请求信息接收自
服务器或者所述终端设备。
- 7.根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述网元节点选自：
20 定位管理功能节点以及感知功能节点。
- 8.一种通信方法，其特征在于，包括：
接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元
节点和终端设备之间传输的第一业务的数据；
25 使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述网元
节点。
- 9.根据权利要求 8 所述的方法，其特征在于，所述接收密钥信息包括：
接收第二信息，所述第二信息包括输入参数，所述输入参数用于生成所述第一密
钥。
- 10.根据权利要求 9 所述的方法，其特征在于，所述输入参数包括：所述网元节点
30 的标识和/或所述网元节点的网络互连协议地址。
- 11.根据权利要求 8 至 10 中任一项所述的方法，其特征在于，还包括：
发送请求信息，所述请求信息用于请求第一业务。
- 12.一种通信方法，其特征在于，包括：
35 接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元
节点和终端设备之间传输的第一业务的数据；
使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述终端
设备。
- 13.根据权利要求 12 所述的方法，其特征在于，所述接收密钥信息包括：

接收第一信息，所述第一信息包括所述第一密钥。

14.根据权利要求 12 或 13 所述的方法，其特征在于，所述网元节点选自：定位管理功能节点以及感知功能节点。

15.一种通信装置，其特征在于，包括：

5 接收模块，用于接收请求信息，所述请求信息用于请求第一业务；

发送模块，用于发送密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的所述第一业务的数据。

16.一种通信装置，其特征在于，包括：

10 接收模块，用于接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；

传输模块，用于使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述网元节点。

17.一种通信装置，其特征在于，包括：

15 接收模块，用于接收密钥信息，所述密钥信息用于指示第一密钥，所述第一密钥用于加密在网元节点和终端设备之间传输的第一业务的数据；

传输模块，用于使用所述第一密钥处理所述第一业务的数据，并经由无线接入网传输至所述终端设备。

20 18.一种计算机可读存储介质，所述计算机可读存储介质为非易失性存储介质或非瞬态存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器运行时执行权利要求 1 至 14 中任一项所述方法的步骤。

19.一种通信装置，包括存储器和处理器，所述存储器上存储有可在所述处理器上运行的计算机程序，其特征在于，所述处理器运行所述计算机程序时执行权利要求 1 至 14 中任一项所述方法的步骤。

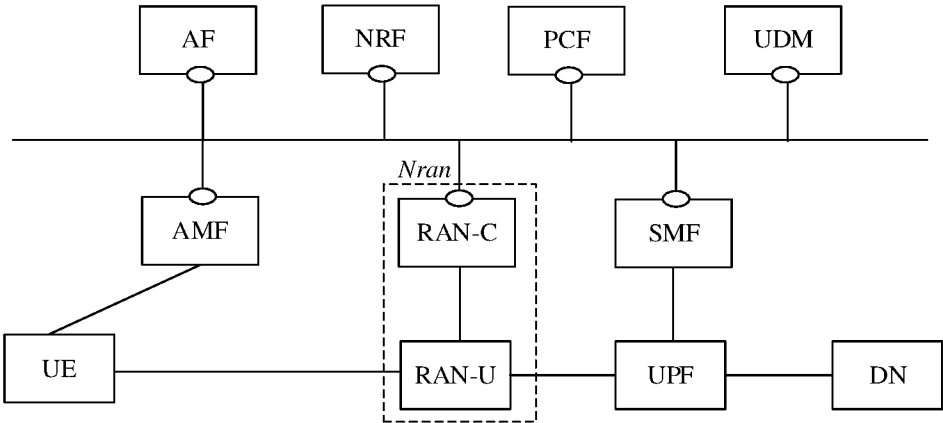


图 1

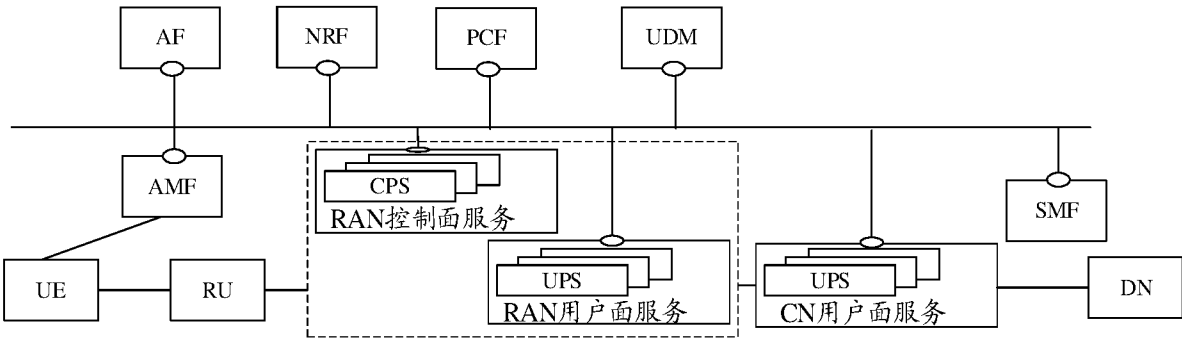


图 2

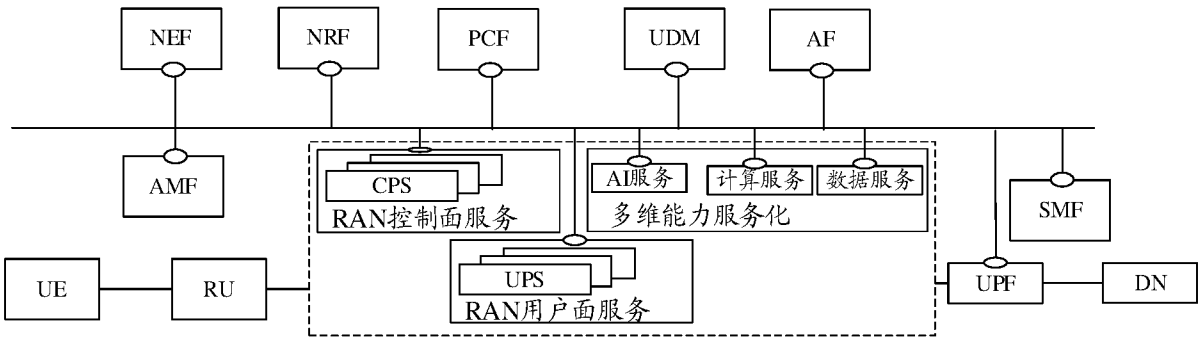


图 3

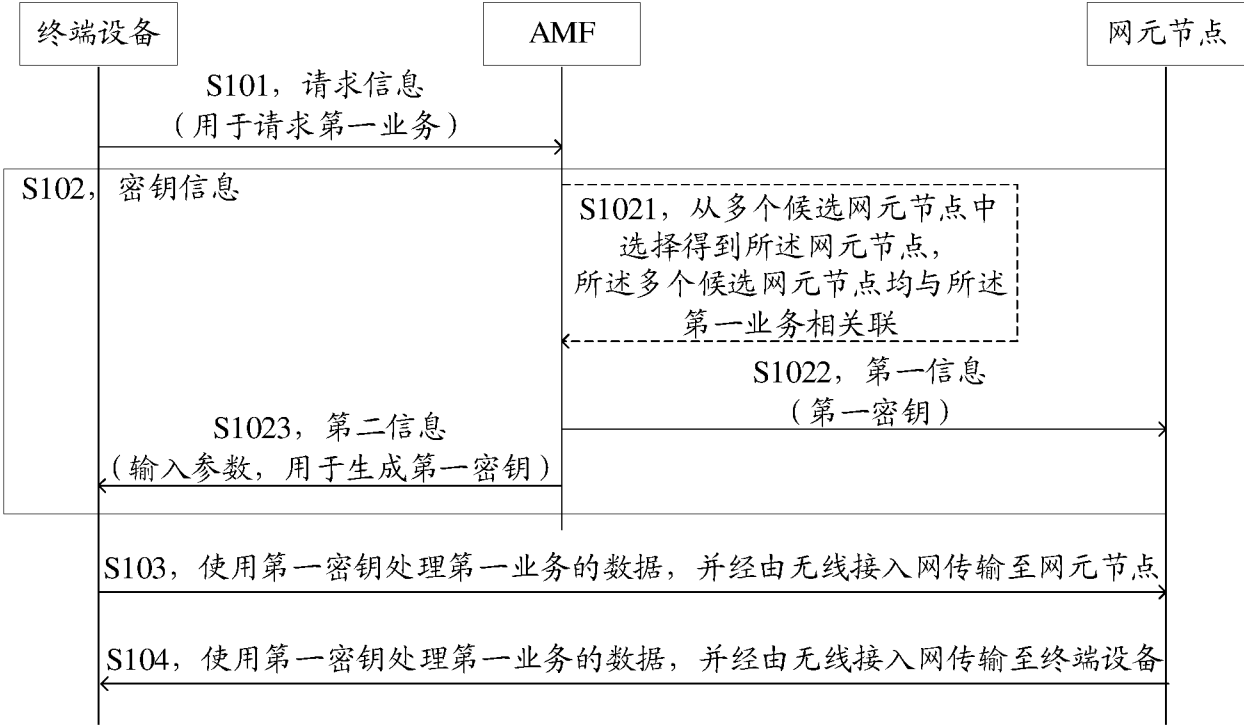


图 4

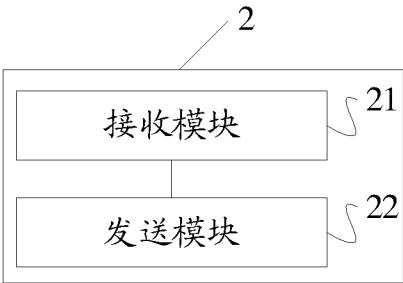


图 5

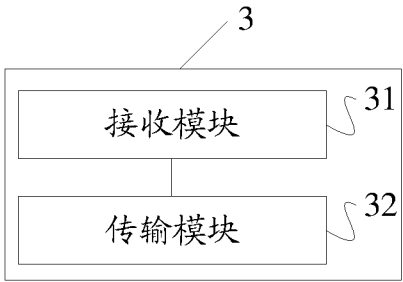


图 6

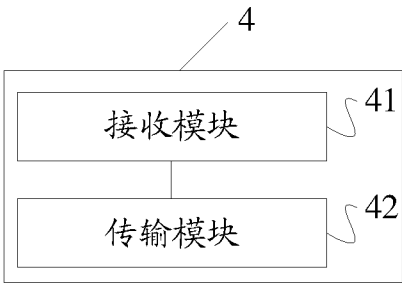


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/137854

A. CLASSIFICATION OF SUBJECT MATTER H04W 12/04(2021.01)i; H04W 12/03(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 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) CNABS, CNTXT, CNKI, VEN, WOTXT, USTXT, EPTXT, 3GPP: 服务化, 核心网, 功能, 密钥, 加密, 移动性管理功能, service-based, service based, architecture, SBA, core network, CN, network function, NF, security, key, AMF		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2023224915 A1 (INTEL CORP.) 23 November 2023 (2023-11-23) description, paragraphs [0003]-[0394]	1-19
X	US 2023018399 A1 (CISCO TECHNOLOGY INC.) 19 January 2023 (2023-01-19) description, paragraphs [0004]-[0098]	1-19
A	WO 2023229316 A1 (SAMSUNG ELECTRONICS CO., LTD.) 30 November 2023 (2023-11-30) entire document	1-19
A	CN 110830991 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 February 2020 (2020-02-21) entire document	1-19
A	CN 114867004 A (VIVO MOBILE COMMUNICATION CO., LTD.) 05 August 2022 (2022-08-05) entire document	1-19
☐ 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 19 February 2025		Date of mailing of the international search report 26 February 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/CN2024/137854

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2023224915	A1	23 November 2023	None			
US	2023018399	A1	19 January 2023	US	2023354017	A1	02 November 2023
				US	12041440	B2	16 July 2024
				WO	2023288082	A1	19 January 2023
				US	11706614	B2	18 July 2023
WO	2023229316	A1	30 November 2023	US	2023413059	A1	21 December 2023
CN	110830991	A	21 February 2020	WO	2020029938	A1	13 February 2020
				EP	3820181	A1	12 May 2021
				EP	3820181	A4	21 July 2021
				EP	3820181	B1	12 April 2023
				US	2021168594	A1	03 June 2021
				US	11778459	B2	03 October 2023
CN	114867004	A	05 August 2022	None			

A. 主题的分类 H04W 12/04(2021.01)i; H04W 12/03(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 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)) CNABS;CNTXT;CNKI;VEN;WOTXT;USTXT;EPTXT;3GPP: 服务化, 核心网, 功能, 密钥, 加密, 移动性管理功能, service-based, service based, architecture, SBA, core network, CN, network function, NF, security, key, AMF																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>WO 2023224915 A1 (INTEL CORP) 2023年11月23日 (2023 - 11 - 23) 说明书第[0003]-[0394]段</td> <td>1-19</td> </tr> <tr> <td>X</td> <td>US 2023018399 A1 (CISCO TECH INC) 2023年1月19日 (2023 - 01 - 19) 说明书第[0004]-[0098]段</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>WO 2023229316 A1 (SAMSUNG ELECTRONICS CO LTD) 2023年11月30日 (2023 - 11 - 30) 全文</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>CN 110830991 A (华为技术有限公司) 2020年2月21日 (2020 - 02 - 21) 全文</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>CN 114867004 A (维沃移动通信有限公司) 2022年8月5日 (2022 - 08 - 05) 全文</td> <td>1-19</td> </tr> </tbody> </table> ☐ 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			类型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	WO 2023224915 A1 (INTEL CORP) 2023年11月23日 (2023 - 11 - 23) 说明书第[0003]-[0394]段	1-19	X	US 2023018399 A1 (CISCO TECH INC) 2023年1月19日 (2023 - 01 - 19) 说明书第[0004]-[0098]段	1-19	A	WO 2023229316 A1 (SAMSUNG ELECTRONICS CO LTD) 2023年11月30日 (2023 - 11 - 30) 全文	1-19	A	CN 110830991 A (华为技术有限公司) 2020年2月21日 (2020 - 02 - 21) 全文	1-19	A	CN 114867004 A (维沃移动通信有限公司) 2022年8月5日 (2022 - 08 - 05) 全文	1-19
类型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
X	WO 2023224915 A1 (INTEL CORP) 2023年11月23日 (2023 - 11 - 23) 说明书第[0003]-[0394]段	1-19																		
X	US 2023018399 A1 (CISCO TECH INC) 2023年1月19日 (2023 - 01 - 19) 说明书第[0004]-[0098]段	1-19																		
A	WO 2023229316 A1 (SAMSUNG ELECTRONICS CO LTD) 2023年11月30日 (2023 - 11 - 30) 全文	1-19																		
A	CN 110830991 A (华为技术有限公司) 2020年2月21日 (2020 - 02 - 21) 全文	1-19																		
A	CN 114867004 A (维沃移动通信有限公司) 2022年8月5日 (2022 - 08 - 05) 全文	1-19																		
国际检索实际完成的日期 2025年2月19日		国际检索报告邮寄日期 2025年2月26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 李晓 电话号码 (+86) 0512-88996167																		

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/137854

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)
WO	2023224915	A1	2023年11月23日	无	
US	2023018399	A1	2023年1月19日	US	2023354017 A1 2023年11月2日
				US	12041440 B2 2024年7月16日
				WO	2023288082 A1 2023年1月19日
				US	11706614 B2 2023年7月18日
WO	2023229316	A1	2023年11月30日	US	2023413059 A1 2023年12月21日
CN	110830991	A	2020年2月21日	WO	2020029938 A1 2020年2月13日
				EP	3820181 A1 2021年5月12日
				EP	3820181 A4 2021年7月21日
				EP	3820181 B1 2023年4月12日
				US	2021168594 A1 2021年6月3日
				US	11778459 B2 2023年10月3日
CN	114867004	A	2022年8月5日	无	