

(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 1 月 16 日 (16.01.2025)



(10) 国际公布号
WO 2025/010609 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

北京市海淀区西二旗中路 33 号院 6 号楼 8 层 018 号, Beijing 100085 (CN)。

(21) 国际申请号: PCT/CN2023/106667

(22) 国际申请日: 2023 年 7 月 10 日 (10.07.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 北京小米移动软件有限公司 (**BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.**) [CN/CN]; 中国北京市海淀区西二旗中路 33 号院 6 号楼 8 层 018 号, Beijing 100085 (CN)。

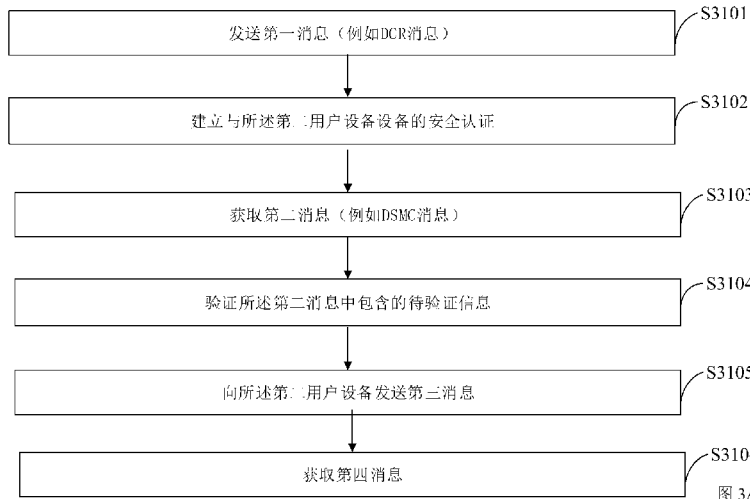
(72) 发明人: 陆伟 (**LU, Wei**); 中国北京市海淀区西二旗中路 33 号院 6 号楼 8 层 018 号, Beijing 100085 (CN)。 商正仪 (**SHANG, Zhengyi**); 中国北

(74) 代理人: 北京法胜知识产权代理有限公司 (**FASHENG INTELLECTUAL PROPERTY COMPANY, LTD.**); 中国北京市海淀区悦秀路 99 号 1 单元 4 层 401, Beijing 100085 (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 PROCESSING METHOD AND USER EQUIPMENT

(54) 发明名称: 通信处理方法、用户设备



S3101 Send a first message (e.g., a DCR message)
S3102 Establish security authentication with a second user equipment
S3103 Acquire a second message (e.g., a DSMC message)
S3104 Verify information to be verified, which is included in the second message
S3105 Send a third message to the second user equipment
S3106 Acquire a fourth message

(57) **Abstract:** The present disclosure relates to a communication processing method. The method comprises: sending a first message to a second user equipment, wherein the first message comprises unprotected content information; receiving a second message sent by the second user equipment, wherein the second message comprises information to be verified, which comprises at least part of the unprotected content information; verifying the information to be verified; sending a third message to the second user equipment, wherein the third message is used for indicating a verification result of the information to be verified; and receiving a fourth message

[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))。

sent by the second user equipment. In this way, a first user equipment can verify information returned by a second user equipment, so as to verify the integrity of unprotected content information received by the second user equipment, such that information in a received first message is prevented from being tampered with, and thus a secure connection can be established between user equipments.

(57) 摘要: 本公开涉及通信处理方法, 包括: 向第二用户设备发送第一消息, 其中, 第一消息包括未受保护内容信息; 接收第二用户设备发送的第二消息, 其中, 第二消息包括待验证信息, 待验证信息包括未受保护内容信息的至少一部分; 验证待验证信息; 向第二用户设备发送第三消息, 其中, 第三消息用于指示待验证信息的验证结果; 接收第二用户设备发送的第四消息。由此, 第一用户设备可以对第二用户设备返回的信息进行验证, 从而可以验证第二用户设备接收到的未受保护内容信息的完整性, 避免接收到的第一消息中的信息被篡改, 进而用户设备之间可以建立安全连接。

通信处理方法、用户设备

技术领域

本公开涉及通信技术领域，尤其涉及通信处理方法、用户设备。

背景技术

- 5 在通信系统中，具有车联网（Vehicle-to-everything, V2X）能力的终端在进行测距/侧行链路（sidelink, SL）定位终端的发现和选择的过程中，往往会发送包含 V2X 服务信息的请求消息，以与目标终端建立通信连接。

发明内容

- 10 本公开的方法可以用于解决“请求消息中的信息被攻击者篡改，而导致后续过程（例如测距/SL 定位控制）失败或导致意外结果”这一技术问题。

本公开实施例提出了一种通信处理方法、用户设备。

根据本公开实施例的第一方面，提出了一种通信处理方法，由第一用户设备执行，包括：

向第二用户设备发送第一消息，其中，所述第一消息包括未受保护内容信息；

- 15 接收所述第二用户设备发送的第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

验证所述待验证信息；

向所述第二用户设备发送第三消息，其中，第三消息用于指示所述待验证信息的验证结果；

接收所述第二用户设备发送的第四消息。

根据本公开实施例的第二方面，提出了一种通信处理方法，由第二用户设备执行，包括：

- 20 接收第一用户设备发送的第一消息，其中，所述第一消息包括未受保护内容信息；

向所述第一用户设备发送第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

接收所述第一用户设备发送的第三消息，其中，所述第三消息指示所述待验证信息的验证结果；

根据所述第三消息向所述第一用户设备发送第四消息。

- 25 根据本公开实施例的第三方面，提出了一种第一用户设备，包括：

收发模块，用于向第二用户设备发送第一消息，其中，所述第一消息包括未受保护内容信息；

所述收发模块，还用于接收所述第二用户设备发送的第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

处理模块，用于验证所述待验证信息；

- 30 所述收发模块，用于向所述第二用户设备发送第三消息，其中，第三消息用于指示所述待验证信息的验证结果；

所述收发模块，还用于接收所述第二用户设备发送的第四消息。

根据本公开实施例的第四方面，提出了一种第二用户设备，包括：

收发模块，用于接收第一用户设备发送的第一消息，其中，所述第一消息包括未受保护内容信息；

- 35 所述收发模块，还用于向所述第一用户设备发送第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

所述收发模块，还用于接收所述第一用户设备发送的第三消息，其中，所述第三消息指示所述待验证信息的验证结果；

- 40 所述收发模块，还用于根据所述第三消息向所述第一用户设备发送第四消息。

根据本公开实施例的第五方面，提出了一种通信设备，包括：

一个或多个处理器；

其中，所述处理器用于调用指令以使得所述通信设备执行第一方面、第二方面中任一方面所述的方法。

根据本公开实施例的第六方面，提出了一种通信系统，包括：

- 45 第一用户设备，用于实现第一方面中所述的通信处理方法；

第二用户设备，用于实现第二方面中所述的通信处理方法。

根据本公开实施例的第七方面，提出了一种存储介质，所述存储介质存储有指令，当所述指令在通信

设备上运行时，使得所述通信设备执行如第一方面、第二方面中任一方面所述的通信处理方法。

本公开实施例中，接收到第一消息的第二用户设备，可以将第一消息中包含的未受保护内容信息中的一部分返回给第一用户设备，由第一用户设备对返回的信息进行验证，从而可以验证第二用户设备接收到的未受保护内容信息的完整性，避免第二用户设备接收到的第一消息中的信息被篡改，进而用户设备之间可以建立安全连接。

附图说明

本公开上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 是根据本公开实施例示出的通信系统的架构示意图；

图 2 是根据本公开实施例示出的通信处理方法的交互示意图；

图 3A-3B 是根据本公开实施例示出的通信处理方法的流程示意图；

图 4A-4B 是根据本公开实施例示出的通信处理方法的流程示意图；

图 5 是根据本公开实施例示出的通信处理方法的交互示意图；

图 6A 是本公开实施例提出的第一用户设备的结构示意图；

图 6B 是本公开实施例提出的第二用户设备的结构示意图；

图 7A 是本公开实施例提出的通信设备的结构示意图；

图 7B 是本公开实施例提出的芯片的结构示意图。

具体实施方式

本公开实施例提出了通信处理方法、用户设备。

第一方面，本公开实施例提出了一种信息的处理方法，所述方法由第一用户设备执行，包括：

向第二用户设备发送第一消息，其中，所述第一消息包括未受保护内容信息；

接收所述第二用户设备发送的第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

验证所述待验证信息；

在接收所述第二消息之后，验证所述待验证信息，向所述第二用户设备发送第三消息，其中，第三消息用于指示所述待验证信息的验证结果；

接收所述第二用户设备发送的第四消息。

在上述实施例中，接收到第一消息的第二用户设备，可以将第一消息中包含的未受保护内容信息中的一部分返回给第一用户设备，由第一用户设备对返回的信息进行验证，从而可以验证第二用户设备接收到的未受保护内容信息的完整性，避免接收到的第一消息中的信息被篡改，进而用户设备之间可以建立安全连接。

结合第一方面的一些实施例，在一些实施例中，所述第一消息为直接通信请求 DCR 消息。

在上述实施例中，在 DCR 消息中携带未受保护内容信息，可以减少通信资源的开销。

结合第一方面的一些实施例，在一些实施例中，所述未受保护内容信息包括所述第一消息的第一信息和第二信息，所述第二信息为安全保护相关的信息。

在上述实施例中，将未受保护的内容信息划分为可用于验证的第一信息，和与安全保护相关的第二信息，从而可以在第二消息中携带可用于验证的第一信息的一部分，进行可以节省传输待验证信息的信令开销，提高验证效率。

结合第一方面的一些实施例，在一些实施例中，所述第二消息为 DSMC 消息。

在上述实施例中，将未受保护的内容信息划分为可用于验证的第一信息，和与安全保护相关的第二信息，从而可以在第二消息中携带可用于验证的第一信息的一部分，进行可以节省传输待验证信息的信令开销，提高验证效率。

结合第一方面的一些实施例，在一些实施例中，所述验证所述待验证信息，包括：

根据所述第一信息对所述待验证信息进行验证。

在上述实施例中，由于待验证信息包括所述第一信息的至少一部分，因此，直接基于第一信息对所述待验证信息进行验证，可以提高验证效率。

结合第一方面的一些实施例，在一些实施例中，所述验证结果为验证通过，所述第三消息为直接安全模式完成消息；或者，所述验证结果为验证未通过，所述第三消息为直接安全模式拒绝消息。

在上述实施例中，根据所述待验证信息的验证结果，确定第三消息，从而可以准确地通知第二用户设备待验证信息的验证结果。

5 结合第一方面的一些实施例，在一些实施例中，所述第四消息为直接通信接受消息时，直接通信连接建立成功；或者，所述第四消息为直接通信拒绝消息时，直接通信连接建立失败。

在上述实施例中，通过直接通信接受消息及直接通信拒绝消息指示直接通信连接建立结果，可以减少通信资源的开销。

结合第一方面的一些实施例，在一些实施例中，所述第一信息包括以下至少一项：

10 测距与侧行链路定位协议 RSPP 元数据；

目标用户信息；

源用户信息；

组标识 ID；

业务信息。

15 结合第一方面的一些实施例，在一些实施例中，所述第二信息包括所述第一用户设备的 PC5 安全策略信息、第一用户设备安全能力的至少一项。

第二方面，本公开实施例提出了一种通信处理方法，所述方法由第二用户设备执行，该方法包括：

接收第一用户设备发送的第一消息，其中，所述第一消息包括未受保护内容信息；

20 向所述第一用户设备发送第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

接收所述第一用户设备发送的第三消息，其中，所述第三消息指示所述待验证信息的验证结果；

根据所述第三消息向所述第一用户设备发送第四消息。

25 上述实施例中，接收到第一消息的第二用户设备，可以将第一消息中包含的未受保护内容信息中的一部分返回给第一用户设备，由第一用户设备对返回的信息进行验证，从而可以验证第二用户设备接收到的未受保护内容信息的完整性，避免接收到的第一消息中的信息被篡改，进而用户设备之间可以建立安全连接。

结合第二方面的一些实施例，在一些实施例中，所述第一消息为直接通信请求 DCR 消息。

在上述实施例中，在 DCR 消息中携带未受保护内容信息，可以减少通信资源的开销。

30 结合第二方面的一些实施例，在一些实施例中，所述未受保护内容信息包括第一信息和第二信息，所述第二信息为安全保护相关的信息。

在上述实施例中，将未受保护的内容信息划分为可用于验证的第一信息，和与安全保护相关的第二信息，从而可以在第二消息中携带可用于验证的第一信息的一部分，进行可以节省传输待验证信息的信令开销，提高验证效率。

结合第二方面的一些实施例，在一些实施例中，所述第二消息为直接安全模式命令 DSMC 消息。

35 在上述实施例中，在 DSMC 消息中携带待验证信息，可以减少通信资源的开销。

结合第二方面的一些实施例，在一些实施例中，所述验证结果为验证通过，所述第三消息为直接安全模式完成消息。或者，所述验证结果为验证未通过，所述第三消息为直接安全模式拒绝消息。

在上述实施例中，可以通过直接安全模式完成消息及直接安全模式拒绝消息指示不同的验证结果，从而第二用户设备可以通过不同的消息，准确地确定验证结果，而且可以减少通信资源的开销。

40 结合第二方面的一些实施例，在一些实施例中，所述第三消息为直接安全模式完成消息时，所述第四消息为直接通信接受消息。或者，所述第三消息为直接安全模式拒绝消息，所述第四消息为直接通信拒绝消息。

在上述实施例中，可以根据第三消息向所述第一用户设备发送第四消息，从而使发送的第四消息可以与验证结果相匹配，进而两个用户设备可以准确地建立通信连接。

45 结合第二方面的一些实施例，在一些实施例中，所述第一信息包括以下至少一项：

测距与侧行链路定位协议 RSPP 元数据；

目标用户信息；
源用户信息；
组标识 ID；
业务信息。

5 结合第二方面的一些实施例，在一些实施例中，所述第二信息包括所述第一用户设备的 PC5 安全策略信息、第一用户设备安全能力中的至少一项。

第三方面，本公开实施例提出了第一用户设备，上述第一用户设备包括收发模块、处理模块中的至少一者；其中，

收发模块，用于向第二用户设备发送第一消息，其中，所述第一消息包括未受保护内容信息；

10 所述收发模块，还用于接收所述第二用户设备发送的第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

处理模块，用于验证所述待验证信息；

所述收发模块，用于向所述第二用户设备发送第三消息，其中，第三消息用于指示所述待验证信息的验证结果；

15 所述收发模块，还用于接收所述第二用户设备发送的第四消息。

结合第三方面的一些实施例，在一些实施例中，所述第一消息为直接通信请求 DCR 消息。

结合第三方面的一些实施例，在一些实施例中，所述未受保护内容信息包括所述第一消息的第一信息和第二信息，所述第二信息为安全保护相关的信息。

结合第三方面的一些实施例，在一些实施例中，所述第二消息为 DSMC 消息。

20 结合第三方面的一些实施例，在一些实施例中，所述处理模块，用于：

根据所述第一信息对所述待验证信息进行验证。

结合第三方面的一些实施例，在一些实施例中，所述验证结果为验证通过，所述第三消息为直接安全模式完成消息；或者，所述验证结果为验证未通过，所述第三消息为直接安全模式拒绝消息。

结合第三方面的一些实施例，在一些实施例中，所述第四消息为直接通信接受消息时，直接通信连接建立成功；或者，所述第四消息为直接通信拒绝消息时，直接通信连接建立失败。

25 结合第三方面的一些实施例，在一些实施例中，所述第一信息包括以下至少一项：

测距与侧行链路定位协议 RSPP 元数据；

目标用户信息；

源用户信息；

30 组标识 ID；

业务信息。

结合第三方面的一些实施例，在一些实施例中，所述第二信息包括所述第一用户设备的 PC5 安全策略信息、第一用户设备安全能力的至少一项。

35 第四方面，本公开实施例提出了第二用户设备，上述第二用户设备包括收发模块、处理模块中的至少一者；其中，

收发模块，用于接收第一用户设备发送的第一消息，其中，所述第一消息包括未受保护内容信息；

所述收发模块，还用于向所述第一用户设备发送第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；

40 所述收发模块，还用于接收所述第一用户设备发送的第三消息，其中，所述第三消息指示所述待验证信息的验证结果；

所述收发模块，还用于根据所述第三消息向所述第一用户设备发送第四消息。

结合第四方面的一些实施例，在一些实施例中，所述第一消息为直接通信请求 DCR 消息。

结合第四方面的一些实施例，在一些实施例中，所述未受保护内容信息包括第一信息和第二信息，
45 所述第二信息为安全保护相关的信息。

结合第四方面的一些实施例，在一些实施例中，所述第二消息为直接安全模式命令 DSMC 消息。

结合第四方面的一些实施例，在一些实施例中，所述验证结果为验证通过，所述第三消息为直接安

全模式完成消息；或者，所述验证结果为验证未通过，所述第三消息为直接安全模式拒绝消息。

结合第四方面的一些实施例，在一些实施例中，所述第三消息为直接安全模式完成消息，所述第四消息为直接通信接受消息；或者，所述第三消息为直接安全模式拒绝消息，所述第四消息为直接通信拒绝消息。

5 结合第四方面的一些实施例，在一些实施例中，所述第一信息包括以下至少一项：

测距与侧行链路定位协议 RSPP 元数据；

目标用户信息；

源用户信息；

组标识 ID；

10 业务信息。

结合第四方面的一些实施例，在一些实施例中，所述第二信息包括所述第一用户设备的 PC5 安全策略信息、第一用户设备安全能力的至少一项。

第五方面，本公开实施例提出了通信设备，上述通信设备包括：一个或多个处理器；其中，上述通信设备用于执行第一方面和第一方面的可选实现方式。

15 第六方面，本公开实施例提出了通信设备，上述通信设备包括：一个或多个处理器；其中，上述通信设备用于执行第二方面和第二方面的可选实现方式。

第七方面，本公开实施例提出了通信系统，上述通信系统包括：

第一用户设备，用于实现如第一方面和第一方面的可选实现方式所描述的方法；

第二用户设备，用于实现如第二方面和第二方面的可选实现方式所描述的方法。

20 第八方面，本公开实施例提出了存储介质，上述存储介质存储有指令，当上述指令在通信设备上运行时，使得上述通信设备执行如第一方面和第一方面的可选实现方式所描述的方法、或执行如第二方面和第二方面的可选实现方式所描述的方法。

第九方面，本公开实施例提出了程序产品，上述程序产品被通信设备执行时，使得上述通信设备执行如第一方面和第一方面的可选实现方式所描述的方法、或执行如第二方面和第二方面的可选实现方式所描述的方法。

25 第十方面，本公开实施例提出了计算机程序，当其在计算机上运行时，使得计算机执行如第一方面和第一方面的可选实现方式所描述的方法、或执行如第二方面和第二方面的可选实现方式所描述的方法。

30 第十一方面，本公开实施例提供了一种芯片或芯片系统。该芯片或芯片系统包括处理电路，被配置为执行第一方面和第一方面的可选实现方式所描述的方法、或执行如第二方面和第二方面的可选实现方式所描述的方法。

可以理解地，上述用户设备、通信系统、存储介质、程序产品、计算机程序、芯片或芯片系统均用于执行本公开实施例所提出的方法。因此，其所能达到的有益效果可以参考对应方法中的有益效果，此处不再赘述。

35 本公开实施例提出了通信处理方法、用户设备。在一些实施例中，通信处理方法与信息处理方法、通信方法等术语可以相互替换，信息传输装置与信息处理装置、通信装置等术语可以相互替换，信息处理系统、通信系统等术语可以相互替换。

本公开实施例并非穷举，仅为部分实施例的示意，不作为对本公开保护范围的具体限制。在不矛盾的情况下，某一实施例中的每个步骤均可以作为独立实施例来实施，且各步骤之间可以任意组合，例如，在某一实施例中去掉部分步骤后的方案也可以作为独立实施例来实施，且在某一实施例中各步骤的顺序可以任意交换，另外，某一实施例中的可选实现方式可以任意组合；此外，各实施例之间可以任意组合，例如，不同实施例的部分或全部步骤可以任意组合，某一实施例可以与其他实施例的可选实现方式任意组合。

40 在各本公开实施例中，如果没有特殊说明以及逻辑冲突，各实施例之间的术语和/或描述具有一致性，且可以互相引用，不同实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。

本公开实施例中所使用的术语只是为了描述特定实施例的目的，而并非作为对本公开的限制。

在本公开实施例中，除非另有说明，以单数形式表示的元素，如“一个”、“一种”、“该”、“上述”、“所述”、“前述”、“这一”等，可以表示“一个且只有一个”，也可以表示“一个或多个”、“至少一个”等。例如，在翻译中使用如英语中的“a”、“an”、“the”等冠词（article）的情况下，冠词之后的名词可以理解为单数表

达形式，也可以理解为复数表达形式。

在本公开实施例中，“多个”是指两个或两个以上。

在一些实施例中，“至少一者（至少一项、至少一个）（at least one of）”、“一个或多个（one or more）”、“多个（a plurality of）”、“多个（multiple）”等术语可以相互替换。

5 在一些实施例中，“A、B 中的至少一者”、“A 和/或 B”、“在一情况下 A，在另一情况下 B”、“响应于一情况 A，响应于另一情况 B”等记载方式，根据情况可以包括以下技术方案：在一些实施例中 A（与 B 无关地执行 A）；在一些实施例中 B（与 A 无关地执行 B）；在一些实施例中从 A 和 B 中选择执行（A 和 B 被选择性执行）；在一些实施例中 A 和 B（A 和 B 都被执行）。当有 A、B、C 等更多分支时也类似上述。

10 在一些实施例中，“A 或 B”等记载方式，根据情况可以包括以下技术方案：在一些实施例中 A（与 B 无关地执行 A）；在一些实施例中 B（与 A 无关地执行 B）；在一些实施例中从 A 和 B 中选择执行（A 和 B 被选择性执行）。当有 A、B、C 等更多分支时也类似上述。

本公开实施例中的“第一”、“第二”等前缀词，仅仅为了区分不同的描述对象，不对描述对象的位置、顺序、优先级、数量或内容等构成限制，对描述对象的陈述参见权利要求或实施例中上下文的描述，不应
15 因为使用前缀词而构成多余的限制。例如，描述对象为“字段”，则“第一字段”和“第二字段”中“字段”之前的序数词并不限制“字段”之间的位置或顺序，“第一”和“第二”并不限制其修饰的“字段”是否在同一个消息中，也不限制“第一字段”和“第二字段”的先后顺序。再如，描述对象为“等级”，则“第一等级”和“第二等级”中“等级”之前的序数词并不限制“等级”之间的优先级。再如，描述对象的数量并不受序数词的限制，可以是一个或者多个，以“第一装置”为例，其中“装置”的数量可以是一个或者多个。此外，不同前缀词修饰
20 的对象可以相同或不同，例如，描述对象为“装置”，则“第一装置”和“第二装置”可以是相同的装置或者不同的装置，其类型可以相同或不同；再如，描述对象为“信息”，则“第一信息”和“第二信息”可以是相同的信息或者不同的信息，其内容可以相同或不同。

在一些实施例中，“包括 A”、“包含 A”、“用于指示 A”、“携带 A”，可以解释为直接携带 A，也可以解释为间接指示 A。

25 在一些实施例中，“响应于……”、“响应于确定……”、“在……的情况下”、“在……时”、“当……时”、“若……”、“如果……”等术语可以相互替换。

在一些实施例中，装置等可以解释为实体的、也可以解释为虚拟的，其名称不限于实施例中所记载的名称，“装置”、“设备（equipment）”、“设备（device）”、“电路”、“网元”、“节点”、“功能”、“单元”、“部件（section）”、“系统”、“网络”、“芯片”、“芯片系统”、“实体”、“主体”等术语可以相互替换。

30 在一些实施例中，“接入网设备（access network device, AN device）”、“无线接入网设备（radio access network device, RAN device）”、“基站（base station, BS）”、“无线基站（radio base station）”、“固定台（fixed station）”、“节点（node）”、“接入点（access point）”、“发送点（transmission point, TP）”、“接收点（reception point, RP）”、“发送接收点（transmission / reception point, TRP）”、“面板（panel）”、“天线面板（antenna panel）”、“天线阵列（antenna array）”、“小区（cell）”、“宏小区（macro cell）”、“小型
35 小区（small cell）”、“毫微微小区（femto cell）”、“微微小区（pico cell）”、“扇区（sector）”、“小区组（cell group）”、“载波（carrier）”、“分量载波（component carrier）”、“带宽部分（bandwidth part, BWP）”等术语可以相互替换。

在一些实施例中，“终端（terminal）”、“终端设备（terminal device）”、“用户设备（user equipment, UE）”、“用户终端（user terminal）”、“移动台（mobile station, MS）”、“移动终端（mobile terminal, MT）”、
40 订户站（subscriber station）、移动单元（mobile unit）、订户单元（subscriber unit）、无线单元（wireless unit）、远程单元（remote unit）、移动设备（mobile device）、无线设备（wireless device）、无线通信设备（wireless communication device）、远程设备（remote device）、移动订户站（mobile subscriber station）、接入终端（access terminal）、移动终端（mobile terminal）、无线终端（wireless terminal）、远程终端（remote terminal）、手持设备（handset）、用户代理（user agent）、移动客户端（mobile client）、客户端（client）等术语可
45 以相互替换。

在一些实施例中，接入网设备、核心网设备、或网络设备可以被替换为终端。例如，针对将接入网设

备、核心网设备、或网络设备以及终端间的通信置换为多个终端间的通信（例如，也可以被称为设备对设备（device-to-device, D2D）、车联网（vehicle-to-everything, V2X）等）的结构，也可以应用本公开的各实施例。在该情况下，也可以设为终端具有接入网设备所具有的全部或部分功能的结构。此外，“上行”、“下行”等语言也可以被替换为与终端间通信对应的语言（例如，“侧行（side）”）。例如，上行信道、下行信道等可以被替换为侧行信道，上行链路、下行链路等可以被替换为侧行链路。

在一些实施例中，终端可以被替换为接入网设备、核心网设备、或网络设备。在该情况下，也可以设为接入网设备、核心网设备、或网络设备具有终端所具有的全部或部分功能的结构。

在一些实施例中，获取数据、信息等可以遵照所在地国家的法律法规。

在一些实施例中，可以在得到用户同意后获取数据、信息等。

图 1 是根据本公开实施例示出的通信系统的架构示意图。如图 1 所示，通信系统 100 可以包括第一用户设备（terminal）101、第二用户设备 102。第一用户设备 101 与第二用户设备 102 之间可以建立有通信连接。第一用户设备 101 与第二用户设备 102 之间可以进行 SL 通信。

在一些实施例中，通信系统 100 还可以包括网络设备，网络设备可以包括接入网设备和核心网设备（core network device）的至少一者。

在一些实施例中，第一用户设备 101 或第二用户设备 102 例如包括手机（mobile phone）、可穿戴设备、物联网设备、具备通信功能的汽车、智能汽车、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、增强现实（augmented reality, AR）终端设备、工业控制（industrial control）中的无线终端设备、无人驾驶（self-driving）中的无线终端设备、远程手术（remote medical surgery）中的无线终端设备、智能电网（smart grid）中的无线终端设备、运输安全（transportation safety）中的无线终端设备、智慧城市（smart city）中的无线终端设备、智慧家庭（smart home）中的无线终端设备中的至少一者，但不限于此。

在一些实施例中，接入网设备例如是将终端接入到无线网络的节点或设备，接入网设备可以包括 5G 通信系统中的演进节点 B（evolved NodeB, eNB）、下一代演进节点 B（next generation eNB, ng-eNB）、下一代节点 B（next generation NodeB, gNB）、节点 B（node B, NB）、家庭节点 B（home node B, HNB）、家庭演进节点 B（home evolved nodeB, HeNB）、无线回传设备、无线网络控制器（radio network controller, RNC）、基站控制器（base station controller, BSC）、基站收发台（base transceiver station, BTS）、基带单元（base band unit, BBU）、移动交换中心、6G 通信系统中的基站、开放型基站（Open RAN）、云基站（Cloud RAN）、其他通信系统中的基站、WiFi 系统中的接入节点中的至少一者，但不限于此。

在一些实施例中，本公开的技术方案可适用于 Open RAN 架构，此时，本公开实施例所涉及的接入网设备间或者接入网设备内的接口可变为 Open RAN 的内部接口，这些内部接口之间的流程和信息交互可以通过软件或者程序实现。

在一些实施例中，接入网设备可以由集中单元（central unit, CU）与分布式单元（distributed unit, DU）组成的，其中，CU 也可以称为控制单元（control unit），采用 CU-DU 的结构可以将接入网设备的协议层拆分开，部分协议层的功能放在 CU 集中控制，剩下部分或全部协议层的功能分布在 DU 中，由 CU 集中控制 DU，但不限于此。

在一些实施例中，核心网设备可以是一个设备，包括一个或多个网元，也可以是多个设备或设备群，分别包括一个或多个网元中的全部或部分。网元可以是虚拟的，也可以是实体的。核心网例如包括演进分组核心（Evolved Packet Core, EPC）、5G 核心网络（5G Core Network, 5GCN）、下一代核心（Next Generation Core, NGC）中的至少一者。

可以理解的是，本公开实施例描述的通信系统是为了更加清楚的说明本公开实施例的技术方案，并不构成对于本公开实施例提出的技术方案的限定，本领域普通技术人员可知，随着系统架构的演变和新业务场景的出现，本公开实施例提出的技术方案对于类似的技术问题同样适用。

下述本公开实施例可以应用于图 1 所示的通信系统 100、或部分主体，但不限于此。图 1 所示的各主体是例示，通信系统可以包括图 1 中的全部或部分主体，也可以包括图 1 以外的其他主体，各主体数量和形态为任意，各主体之间的连接关系是例示，各主体之间可以不连接也可以连接，其连接可以是任意方式，可以是直接连接也可以是间接连接，可以有有线连接也可以是无连接。

本公开各实施例可以应用于长期演进 (Long Term Evolution, LTE)、LTE-Advanced (LTE-A)、LTE-Beyond (LTE-B)、SUPER 3G、IMT-Advanced、第四代移动通信系统 (4th generation mobile communication system, 4G)、)、第五代移动通信系统 (5th generation mobile communication system, 5G)、5G 新空口 (new radio, NR)、未来无线接入 (Future Radio Access, FRA)、新无线接入技术 (New-Radio Access Technology, RAT)、新无线 (New Radio, NR)、新无线接入 (New radio access, NX)、未来一代无线接入 (Future generation radio access, FX)、Global System for Mobile communications (GSM (注册商标))、CDMA2000、超移动宽带 (Ultra Mobile Broadband, UMB)、IEEE 802.11 (Wi-Fi (注册商标))、IEEE 802.16 (WiMAX (注册商标))、IEEE 802.20、超宽带 (Ultra-WideBand, UWB)、蓝牙 (Bluetooth (注册商标))、陆上公用移动通信网 (Public Land Mobile Network, PLMN) 网络、设备到设备 (Device-to-Device, D2D) 系统、机器到机器 (Machine to Machine, M2M) 系统、物联网 (Internet of Things, IoT) 系统、车联网 (Vehicle-to-Everything, V2X)、利用其他通信方法的系统、基于它们而扩展的下一代系统等。此外, 也可以将多个系统组合 (例如, LTE 或者 LTE-A 与 5G 的组合等) 应用。

本公开实施例中, 具有 V2X 能力的 UE 的测距/SL 定位 UE 发现和选择的过程, 或发送直接通信请求 (Direct Communication Request, DCR) 消息, DCR 消息中包含指示 “测距/侧链定位” 的 V2X 服务信息, 源用户信息 (例如, 源 UE 的应用层 ID、源 UE 的服务公共陆地移动网 (Public Land Mobile Network, PLMN))、目标用户信息 (如, 目标 UE 的应用层层 ID)、测距与侧行链路定位协议 (ranging and sidelink positioning protocol, RSPP) 元数据信息、应用层组 ID 等。所有这些对于测距/SL 定位通信的成功至关重要。如果任何信息 (例如源用户信息、目标用户信息、包括 UE 角色的 RSPP 元数据) 被攻击者篡改, 则后续过程 (例如测距/SL 定位控制) 将失败或导致意外后果。

相关技术中, 对于用于具有 V2X 能力的 UE 的 DCR 消息的安全保护, 由 UE 的网络层构建的 DCR 消息在网络层不受 UE 的保护, 即 DCR 消息完整性在网络层没有受到 UE 的保护, 使得接收到 DCR 消息的 V2X UE 无法验证接收到的 DCR 消息中的信息是否被篡改。

目前没有现有的方法来验证测距/SL 定位服务的 DCR 消息中包含的任何特定信息 (例如, RSPP 元数据、组 ID 等) 的完整性。因此, 需要研究 V2X UE 接收 DCR 消息以验证 DCR 消息中包含的特定信息的完整性的方法。

图 2 是根据本公开实施例示出的通信处理方法的交互示意图。如图 2 所示, 本公开实施例涉及通信处理方法, 用于通信系统 100, 上述方法包括:

步骤 S2101, 第一用户设备向第二用户设备发送第一消息。

在一些实施例中, 所述第一消息之中包括未受保护内容信息。

在一些实施例中, 第一消息可以为直接通信请求 DCR 消息。也可以为其他可以携带未保护内容信息的消息, 本公开对此不做限定。

在一些实施例中, 未受保护内容信息为待对其进行保护的信息。

在一些实施例中, 对未受保护内容信息的名称不做限定, 比如, 特定信息, 指定信息等等。

在一些实施例中, 所述未受保护内容信息可以包括第一信息和第二信息, 所述第二信息为与安全保护相关的信息。

在一些实施例中, 第一信息包括以下至少一项:

测距与侧行链路定位协议 RSPP 元数据;

目标用户信息;

源用户信息;

组标识 ID;

业务信息。

在一些实施例中, RSPP 元数据可以为用于短距离直接通信接口 (PC5) 上的 RSPP 控制操作的数据。

在一些实施例中, 目标用户信息可以为目标 UE 的应用层层 ID 等。本公开对此不做限定。

在一些实施例中, 源用户信息可以为源 UE 的应用层 ID、源 UE 的服务 PLMN 等。本公开对此不做限定。

在一些实施例中,组标识(Identity document, ID)可以为应用层组 ID。

在一些实施例中,业务信息可以为第一用户设备想要实现的业务的具体信息,比如,业务可以为测距/SL 定位相关的业务。

5 在一些实施例中,第二信息可以包括第一用户设备的 PC5 安全策略信息、第一用户设备安全能力信息中的至少一项。

在一些实施例中,第一用户设备的 PC5 安全策略信息可以为用于保护第一用户设备的 PC5 的安全相关的信息。

在一些实施例中,第一用户设备安全能力信息可以为第一用户设备安全能力相关的信息。比如,其支持的安全算法等。

10 在一些实施例中,第一消息中还可以包括认证信息。认证信息可以包括第一用户设备与第二用户设备之间的认证和安全建立所需的信息。

在一些实施例中,认证信息可以包括密钥、随机数和密钥建立信息 key_Est_info 中的至少一项。

15 在一些实施例中,密钥是在加密和解密过程中使用的一组参数或代码,用于对信息进行加密和解密。密钥通常是一个长字符串或数(比如 128 位或 256 位),由随机数生成器生成。或者是由第一用户设备和第二用户设备协商后分配的一组唯一的数字或代码。

在一些实施例中,随机数可以为由随机数生成器生成的一组看似随机的数字或字符,其生成过程不受人为的干扰或控制,且每次生成的结果都是不同的。随机数可以用来产生加密密钥或确保通信中的一次性密码的安全性。

20 在一些实施例中,密钥建立信息 key_Est_info 可以为用于指示创建终端之间认证和安全建立所需的密钥的相关信息。

25 在一些实施例中,“特定(certain)”、“预定(preseted)”、“预设”、“设定”、“指示(indicated)”“某一”、“任意”、“任一”、“第一”等术语可以相互替换,“特定 A”、“预定 A”、“预设 A”、“设定 A”、“指示 A”、“某一 A”、“任意 A”、“任一 A”“第一 A”可以解释为在协议等中预先规定的 A,也可以解释为通过设定、配置、或指示等得到的 A,也可以解释为特定 A、某一 A、任意 A、任一 A 或第一 A 等,但不限于此。

在一些实施例中,“发送”、“发射”、“上报”、“下发”、“传输”、“双向传输”、“发送和/或接收”等术语可以相互替换。

30 在一些实施例中,“获取”、“获得”、“得到”、“接收”、“传输”、“双向传输”、“发送和/或接收”可以相互替换,其可以解释为从其他主体接收,从协议中获取,从高层获取,自身处理得到、自主实现等多种含义。

在一些实施例中,信息等的名称不限于实施例中所记载的名称,“信息(information)”、“消息(message)”、“信号(signal)”、“信令(signaling)”、“报告(report)”、“配置(configuration)”、“指示(indication)”、“指令(instruction)”、“命令(command)”、“参数(parameter)”等术语可以相互替换。

35 **步骤 S2102**,第二用户设备根据第一消息中的认证信息建立与第一用户设备的安全认证。

在一些实施例中,第二用户设备可以对第一消息进行解析,以获取第一消息中包含的认证信息,进而基于认证信息,与第一用户设备的建立安全认证。

在一些实施例中,第二用户设备可以使用在 Key_Est_Info 中交换的信息来发起与第一用户设备之间的直接认证和密钥建立过程,以用于 UE 之间的相互认证。

40 **步骤 S2103**,第二用户设备向第一用户设备发送第二消息。

其中,第二消息包括待验证信息,待验证信息包括第一消息中未受保护内容信息的至少一部分。

在一些实施例中,第二消息可以为直接安全模式命令(Direct Security Mode Command,DSMC)消息。

在一些实施例中,DSMC 消息可以为第二用户设备向第一用户设备发送的,用于请求与第一用户设备建立通信连接的消息。

45 在一些实施例中,第二消息可以为直接安全模式命令 DSMC 消息,也可以为其他消息。本公开对此不做限定。

在一些实施例中,待验证信息可以为待第一用户设备对其安全性进行验证的信息。

在一些实施例中，待验证信息可以包括第一信息的至少一部分。比如，待验证信息可以包括测距与侧行链路定位协议 RSPP 元数据、目标用户信息、源用户信息、组 ID、业务信息中的一项或多项。

在一些实施例中，在获取了认证信息之后，还可以根据认证信息生成第一用户设备和第二用户设备之间的中间密钥，进而使用随机数和中间密钥生成安全上下文，以通过安全上下文对第二消息进行完整性保护。

在一些实施例中，可以通过密钥派生函数（Key Derivation Function, KDF），根据认证信息中的随机数派生中间密钥。

在一些实施例中，第二消息还包括第二用户设备所使用的加密算法和密钥推导信息。

在一些实施例中，加密算法可以为对称密钥加密算法，比如数据加密标准（Data Encryption Standard, DES）算法、高级加密标准（Advanced Encryption Standard, AES）算法等。也可以为非对称密钥加密算法，比如数字签名算法（Digital Signature Algorithm, DSA）等。本公开对此不做限定。

在一些实施例中，密钥推导信息可以包括第一用户设备用于密钥推导的随机数等。

步骤 S2104，第一用户设备验证第二消息中的待验证信息。

在一些实施例中，第一用户设备可以使用第一消息中包含的未受保护内容信息对待验证信息进行验证。

在一些实施例中，可以将未受保护内容信息与待验证信息进行匹配，若未受保护内容信息中包含与待验证信息相匹配的信息，则待验证信息验证通过。若待验证信息中的任一信息与未受保护内容信息中的信息不匹配，则待验证信息未通过验证。

在一些实施例中，第一用户设备也可以使用第一信息对待验证信息进行验证。

在一些实施例中，可以将第一信息与待验证信息进行匹配，若第一信息中包含与待验证信息相匹配的信息，则待验证信息验证通过。若待验证信息中的任一信息与第一信息中的信息不匹配，则待验证信息为未通过验证。

在一些实施例中，第一用户设备在接收到第二消息之后，可以先对第二消息的完整性进行验证，在第二消息的完整性通过验证的情况下，再对待验证信息进行验证。

在一些实施例中，可以使用随机数和中间密钥生成安全上下文，并通过安全上下文对第二消息进行完整性验证。

在一些实施例中，第二消息中还可以包括加密算法和密钥推导信息。从而第一用户设备还可以根据加密算法和密钥推导信息从第二消息之中解析获得待验证信息。

步骤 S2105，第一用户设备向第二用户设备发送第三消息。

在一些实施例中，第三消息指示待验证信息的验证结果。

在一些实施例中，第一用户设备可以根据待验证信息的验证结果，向第二用户设备发送第三消息。

在一些实施例中，若验证结果为验证通过，则第三消息用于指示验证结果为验证通过。若验证结果为未验证通过，则第三消息用于指示验证结果为验证未通过。

在一些实施例中，验证结果为验证通过，第三消息为直接安全模式完成消息。即在验证通过的情况下，第一用户设备可以向第二用户设备发送直接安全模式完成消息。

在一些实施例中，验证结果为验证未通过，第三消息为直接安全模式拒绝消息。即在验证未通过的情况下，第一用户设备可以向第二用户设备发送直接安全模式拒绝消息。

在一些实施例中，第一用户设备可以通过生成的中间密钥及第二消息中包含的密钥推导信息，生成安全上下文，基于安全上下文对第三消息进行安全性保护。

步骤 S2106，第二用户设备根据第三消息向第一用户设备发送第四消息。

在一些实施例中，第三消息为直接安全模式完成消息时，第四消息为直接通信接受消息。即第二用户设备在接收到直接安全模式完成消息时，向第一用户设备发送直接通信接受消息。

在一些实施例中，第三消息为直接安全模式拒绝消息时，第四消息为直接通信拒绝消息。即第二用户设备在接收到直接安全模式拒绝消息时，向第一用户设备发送直接通信拒绝消息。

在一些实施例中，根据第三消息指示的验证结果，向第一用户设备发送第四消息。

在一些实施例中，若第三消息指示的验证结果为通过验证，确定第四消息为直接通信接受消息，即向一用户设备发送直接通信接受消息。

在一些实施例中，若第三消息指示的验证结果为未通过验证，确定第四消息为直接通信拒绝消息，即在第三消息指示的验证结果为未通过验证时，第二用户设备向第一用户设备发送直接通信拒绝消息。

在一些实施例中，第四消息为直接通信接受消息时，直接通信连接建立成功。即第二用户设备可以向第一用户设备发送直接通信接受消息，以告诉第一用户设备成功建立通信连接。

在一些实施例中，第四消息为直接通信拒绝消息时，直接通信连接建立失败。即第二用户设备可以向第一用户设备发送直接通信拒绝消息，以告诉第一用户设备拒绝建立通信连接。

在一些实施例中，第二用户设备在接收到第一用户设备发送的直接安全模式完成消息的情况下，第二用户设备可以确定接收到并返回给第一用户设备的待验证信息是第一消息中的真实信息，没有被篡改。且第一用户设备和第二用户设备之间的安全性连接已经建立。可选地，第二用户设备可以向第一用户设备发送受安全保护的直接通信接受消息。

本公开实施例所涉及的通信方法可以包括步骤 S2101~步骤 S2106 中的至少一者。例如，步骤 S2103 可以作为独立实施例来实施，步骤 S2104 可以作为独立实施例来实施，步骤 S2103+S2104 可以作为独立实施例来实施，步骤 S2101+S2102+S2103+S2104+S2105 可以作为独立实施例来实施，但不限于此。

在一些实施例中，步骤 S2101、S2102、S2103、S2104、S2106 是可选的，在不同实施例中可以对这些步骤中的一个或多个步骤进行省略或替代。

在一些实施例中，步骤 S2101、S2103、S2104、S2105、S2106 是可选的，在不同实施例中可以对这些步骤中的一个或多个步骤进行省略或替代。

在本实施方式或实施例中，在不矛盾的情况下，各步骤可以独立、任意组合或交换顺序，可选方式或可选例可以任意组合，且可以与其他实施方式或其他实施例的任意步骤之间进行任意组合。

图 3A 是根据本公开实施例示出的通信处理方法的流程示意图。如图 3A 所示，本公开实施例涉及通信处理方法，用于第一用户设备 101，上述方法包括：

步骤 S3101，发送第一消息。

步骤 S3101 的可选实现方式可以参见图 2 的步骤 S2101、及图 2、图 3A 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，第一用户设备 101 可以向第二用户设备 102 发送第一消息。但不限于此，也可以向其他用户设备发送的第一信息，比如，广播第一消息。

在一些实施例中，第一消息包括未受保护内容信息。

步骤 S3102，建立与第二用户设备的安全认证。

步骤 S3102 的可选实现方式可以参见图 2 的步骤 S2102、及图 2 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，第二用户设备 102 可以为接收到第一用户设备 102 发送第一消息的用户设备。

步骤 S3103，获取第二消息。

步骤 S3103 的可选实现方式可以参见图 2 的步骤 S2103、及图 2 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，第二消息包括待验证信息，待验证信息包括第一消息中未受保护内容信息的至少一部分。

在一些实施例中，第一用户设备 101 接收第二用户设备 102 发送的第二消息。但不限于此，也可以接收由其他用户设备发送的第二消息。

步骤 S3104，验证第二消息中包含的待验证信息。

步骤 S3104 的可选实现方式可以参见图 2 的步骤 S2104、及图 2 所涉及的实施例中其他关联部分，此处不再赘述。

步骤 S3105，向第二用户设备发送第三消息。

步骤 S3105 的可选实现方式可以参见图 2 的步骤 S2105、及图 2 所涉及的实施例中其他关联部分，此处不再赘述。

步骤 S3106，获取第四消息。

步骤 S3106 的可选实现方式可以参见图 2 的步骤 S2106、及图 2 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，第一用户设备 101 接收第二用户设备 102 发送的第二消息。但不限于此，也可以接收由其他用户设备发送的第二消息。

本公开实施例所涉及的方法可以包括步骤 S3101~步骤 S3106 中的至少一者。例如，步骤 S3101+S3103+S3104 可以作为独立实施例来实施，步骤 S3103+S3104 可以作为独立实施例来实施，步骤 S3103+S3104+S3105 可以作为独立实施例来实施，步骤 S3101+S3103+S3104+S3105 可以作为独立实施例来实施，但不限于此。

在一些实施例中，步骤 S3102、S3103、S3104、S3105、S3105 是可选的，在不同实施例中可以对这些步骤中的一个或多个步骤进行省略或替代。

在本实施方式或实施例中，在不矛盾的情况下，各步骤可以独立、任意组合或交换顺序，可选方式或可选例可以任意组合，且可以与其他实施方式或其他实施例的任意步骤之间进行任意组合。

图 3B 是根据本公开实施例示出的通信处理方法的流程图。如图 3B 所示，本公开实施例涉及通信处理方法，用于第一用户设备 101，上述方法包括：

步骤 S3201，向第二用户设备发送第一消息。

其中，第一消息包括未受保护内容信息。

在一些实施例中，第一消息为直接通信请求 DCR 消息。

在一些实施例中，未受保护内容信息包括第一消息的第一信息和第二信息，第二信息为与安全保护相关的信息。

在一些实施例中，第一信息包括以下至少一项：

测距与侧行链路定位协议 RSPP 元数据；

目标用户信息；

源用户信息；

组标识 ID；

业务信息。

在一些实施例中，第二信息包括第一用户设备的 PC5 安全策略信息、第一用户设备安全能力的至少一项。

步骤 S3202，接收第二用户设备发送的第二消息。

其中，第二消息包括待验证信息，待验证信息包括第一消息中未受保护内容信息的至少一部分。

在一些实施例中，第二消息为 DSMC 消息。

步骤 S3203，验证待验证信息。

在一些实施例中，验证待验证信息，包括：

根据第一信息对待验证信息进行验证。

步骤 S3204，向第二用户设备发送第三消息。

其中，第三消息用于指示待验证信息的验证结果。

在一些实施例中，验证结果为验证通过，第三消息为直接安全模式完成消息。验证结果为验证未通过，第三消息为直接安全模式拒绝消息。

步骤 S3205，接收第二用户设备发送的第四消息。

在一些实施例中，接收第二用户设备发送的第四消息，其中，第四消息指示直接通信连接建立结果。

在一些实施例中，第四消息为直接通信接受消息时，直接通信连接建立成功。第四消息为直接通信拒绝消息时，直接通信连接建立失败。

关于步骤 S3201-S3205 的详细介绍可以参考上述实施例描述。

本公开实施例所涉及的通信处理方法可以包括步骤 S3201~步骤 S3205 中的至少一者。例如,步骤 S3201 可以作为独立实施例来实施,步骤 S3202 可以作为独立实施例来实施,步骤 S3203 可以作为独立实施例来实施,步骤 S3202+步骤 S3203+步骤 S3204 可以作为独立实施例来实施,但不限于此。

5 在一些实施例中,步骤 S3201、步骤 S3205 是可选的,在不同实施例中可以对这些步骤中的一个或多个步骤进行省略或替代。

在本实施方式或实施例中,在不矛盾的情况下,各步骤可以独立、任意组合或交换顺序,可选方式或可选例可以任意组合。

在本实施方式或实施例中,在不矛盾的情况下,可选方式或可选例可以任意组合。

10 图 4A 是根据本公开实施例示出的通信处理方法的流程示意图。如图 4A 所示,本公开实施例涉及通信处理方法,用于第二用户设备 102,上述方法包括:

步骤 S4101,获取第一消息。

步骤 S4101 的可选实现方式可以参见图 2 的步骤 S2101 的可选实现方式、及图 2 所涉及的实施例中其他关联部分,此处不再赘述。

15 在一些实施例中,第二用户设备 102 接收第一用户设备 101 发送的第一消息。但不限于此,也可以接收由其他用户设备发送的第一消息。

在一些实施例中,第一消息包括未受保护内容信息。

在一些实施例中,根据协议约定,获取未受保护的内容信息。

步骤 S4102,根据第一消息中的认证信息建立与第一用户设备的安全认证。

20 步骤 S4102 的可选实现方式可以参见图 2 的步骤 S2102 的可选实现方式、及图 2 所涉及的实施例中其他关联部分,此处不再赘述。

步骤 S4103,向第一用户设备发送第二消息。

步骤 S4103 的可选实现方式可以参见图 2 的步骤 S2103 的可选实现方式、及图 2 所涉及的实施例中其他关联部分,此处不再赘述。

25 **步骤 S4104**,获取第三消息。

在一些实施例中,第三消息指示待验证信息的验证结果。

步骤 S4104 的可选实现方式可以参见图 2 的步骤 S2105 的可选实现方式、及图 2 所涉及的实施例中其他关联部分,此处不再赘述。

30 在一些实施例中,第二用户设备 102 接收第一用户设备 101 发送的第三消息。但不限于此,也可以接收由其他用户设备发送的第三消息。

步骤 S4105,根据第三消息向第一用户设备发送第四消息。

步骤 4105 的可选实现方式可以参见图 2 的步骤 S2106、及图 2 所涉及的实施例中其他关联部分,此处不再赘述。

35 本公开实施例所涉及的方法可以包括步骤 S4101~步骤 S4105 中的至少一者。例如,步骤 S4101+S4102 可以作为独立实施例来实施,步骤 S4103+S4104 可以作为独立实施例来实施,步骤 S4103+S4104+S4105 可以作为独立实施例来实施,步骤 S4101+S4103+S4104+S4105 可以作为独立实施例来实施,但不限于此。

在一些实施例中,步骤 S4102、S4103、S4104、S4105 是可选的,在不同实施例中可以对这些步骤中的一个或多个步骤进行省略或替代。

40 在本实施方式或实施例中,在不矛盾的情况下,各步骤可以独立、任意组合或交换顺序,可选方式或可选例可以任意组合,且可以与其他实施方式或其他实施例的任意步骤之间进行任意组合。

图 4B 是根据本公开实施例示出的通信处理方法的流程示意图。如图 4B 所示,本公开实施例涉及通信处理方法,用于第二用户设备 102,上述方法包括:

45 **步骤 S4201**,接收第一用户设备发送的第一消息。

步骤 S4201 的可选实现方式可以参见图 2 的步骤 S2101、图 3A 的步骤 S4101 的可选实现方式、及图 2、图 3A 所涉及的实施例中其他关联部分,此处不再赘述。

在一些实施例中，第一消息包括未受保护内容信息。

在一些实施例中，第一消息为直接通信请求 DCR 消息。

在一些实施例中，未受保护内容信息包括第一消息的第一信息和第二信息，第二信息为安全保护相关的信息。

5 在一些实施例中，第一信息包括以下至少一项：

测距与侧行链路定位协议 RSPP 元数据；

目标用户信息；

源用户信息；

组标识 ID；

10 业务信息。

在一些实施例中，第二信息包括第一用户设备的 PC5 安全策略信息、第一用户设备安全能力中的至少一项。

步骤 S4202，向第一用户设备发送第二消息。

15 步骤 S4202 的可选实现方式可以参见图 2 的步骤 S2103、图 3A 的步骤 S4103 的可选实现方式、及图 2、图 3A 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，第二消息包括待验证信息，待验证信息包括未受保护内容信息的至少一部分。

在一些实施例中，第二消息为直接安全模式命令 DSMC 消息。

步骤 S4203，接收第一用户设备发送的第三消息。

20 步骤 S4203 的可选实现方式可以参见图 2 的步骤 S2105、图 3A 的步骤 S4104 的可选实现方式、及图 2、图 3A 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，第三消息指示待验证信息的验证结果。

在一些实施例中，验证结果为验证通过，第三消息为直接安全模式完成消息。验证结果为验证未通过，第三消息为直接安全模式拒绝消息。

步骤 S4204，根据第三消息向第一用户设备发送第四消息。

25 步骤 S4204 的可选实现方式可以参见图 2 的步骤 S2106、图 3A 的步骤 S4105 的可选实现方式、及图 2、图 3A 所涉及的实施例中其他关联部分，此处不再赘述。

在一些实施例中，根据第三消息指示的验证结果向第一用户设备发送第四消息。

在一些实施例中，第三消息为直接安全模式完成消息时，第四消息为直接通信接受消息。第三消息为直接安全模式拒绝消息时，第四消息为直接通信拒绝消息。

30 本公开实施例所涉及的通信处理方法可以包括步骤 S4201~步骤 S4204 中的至少一者。例如，步骤 S4201 可以作为独立实施例来实施，步骤 S4202 可以作为独立实施例来实施，步骤 S4203 可以作为独立实施例来实施，步骤 S4201+步骤 S4202+步骤 S4203 可以作为独立实施例来实施，但不限于此。

在一些实施例中，S4201 是可选的，在不同实施例中可以对这些步骤中的一个或多个步骤进行省略或替代。

35 在本实施方式或实施例中，在不矛盾的情况下，各步骤可以独立、任意组合或交换顺序，可选方式或可选例可以任意组合。

在本实施方式或实施例中，在不矛盾的情况下，可选方式或可选例可以任意组合。

40 图 5 是根据本公开实施例示出的通信处理方法的流程示意图。如图 5 所示，本公开实施例涉及通信处理方法，用于通信系统 100，通信系统 100 包括第一用户设备 101 和第二用户设备 102，上述方法包括：

步骤 S5101，第一用户设备发送第一消息。

其中，第一消息包括未受保护内容信息。

步骤 S5102，第二用户设备向第一用户设备发送第二消息。

其中，第二消息包括待验证信息，待验证信息包括第一消息中未受保护内容信息的至少一部分。

45 步骤 S5103，第一用户设备验证待验证信息。

步骤 S5104，向第二用户设备发送第三消息。

其中，第三消息用于指示待验证信息的验证结果。

步骤 S5105，第二用户设备向第一用户设备发送第四消息。

步骤 S5101-步骤 S5105 的可选实现方式可以参见上述实施例描述。

5 在一些实施例中，上述方法可以包括上述通信系统侧、第一用户设备侧、第二用户设备侧等的实施例的方法，此处不再赘述。

本公开实施例所涉及的处理方法可以包括步骤 S5101~步骤 S5105 中的至少一者。例如，步骤 S5102+S5103 可以作为独立实施例来实施，步骤 S5101+S5102+S5103+S5104 可以作为独立实施例来实施，但不限于此。

10 在本实施方式或实施例中，在不矛盾的情况下，各步骤可以独立、任意组合或交换顺序，可选方式或可选例可以任意组合，且可以与其他实施方式或其他实施例的任意步骤之间进行任意组合。

以下为对上述方法的示例性介绍。

15 步骤 1、第一用户设备向第二用户设备发送直接通信请求 DCR 消息。该消息包括需要包含在 DCR 消息中的所有信息，例如 RSPP 元数据（用于 PC5 上的 RSPP 控制操作）、目标用户信息、组 ID（用于 SLPP 信令群播）、第一用户设备的 PC5 信令安全策略等。该消息还包括终端之间的认证和安全建立所需的信息（例如密钥、随机数、key_Est_info）。

步骤 2、第二用户设备使用在 Key_Est_Info 中交换的信息来发起与第一用户设备的直接认证和密钥建立过程以用于 UE 之间的相互认证。

20 步骤 3、第二用户设备向第一用户设备发送直接安全模式命令 DSMC 消息，其中第二用户设备应返回接收到的 DCR 消息中包含的待第一用户设备验证的特定信息（如 RSPP 元数据、目标用户信息、组 ID）。使用第二用户设备从步骤 2 中生成的随机数和中间密钥导出的安全上下文来对 DSMC 消息进行完整性保护。可选地，所使用的加密算法和将由第一用户设备用于密钥推导的随机数也包括在 DSMC 消息中。

25 步骤 4、第一用户设备在接收到 DSMC 消息时，第一用户设备应首先检查 DSMC 消息上的完整性保护。如果 DSMC 消息的完整性得到验证，则 DSMC 检查返回的特定信息是否与其在 DCR 消息中发送的信息相匹配。如果返回的信息不匹配，则第二用户设备向第一用户设备发送指示失败原因的拒绝消息。只有当 DSMC 消息中的所有返回信息与 DCR 消息中的原始发送信息相匹配时，第二用户设备才向第一用户设备发送直接安全模式完成消息，可选的第一用户设备使用从步骤 2 中生成的中间密钥和从第二用户设备接收的随机数导出的安全上下文对直接安全模式完成消息进行完整性保护。

30 步骤 5、第二用户设备在接收到完整性保护的直接安全模式完成消息时，第二用户设备可以验证接收到并返回给第一用户设备的信息是 DCR 消息中的真实信息，而不会被篡改，并且第一用户设备和第二用户设备之间的安全性现在已经建立。第二用户设备应向第一用户设备发送受保护的直接通信接受消息。

35 在本公开实施例中，部分或全部步骤、其可选实现方式可以与其他实施例中的部分或全部步骤任意组合，也可以与其他实施例的可选实现方式任意组合。

本公开实施例还提出用于实现以上任一方法的装置，例如，提出一装置，上述装置包括用以实现以上任一方法中终端所执行的各步骤的单元或模块。再如，还提出另一装置，包括用以实现以上任一方法中网络设备（例如接入网设备、核心网功能节点、核心网设备等）所执行的各步骤的单元或模块。

40 应理解以上装置中各单元或模块的划分仅是一种逻辑功能的划分，在实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。此外，装置中的单元或模块可以以处理器调用软件的形式实现：例如装置包括处理器，处理器与存储器连接，存储器中存储有指令，处理器调用存储器中存储的指令，以实现以上任一方法或实现上述装置各单元或模块的功能，其中处理器例如为通用处理器，例如中央处理单元（Central Processing Unit, CPU）或微处理器，存储器为装置内的存储器或装置外的存储器。或者，装置中的单元或模块可以以硬件电路的形式实现，可以通过对硬件电路的设计实现部分或全部单元或模块的功能，上述硬件电路可以理解为一个或多个处理器；例如，在一种实现中，上述硬件电路为专用集成电路（application-specific integrated circuit, ASIC），通过对电路内元件逻辑关系的设计，实现以上部分或全部单元或模块的功能；再如，在另一种实现中，上述硬件电路为可以通过可编程逻辑器件（programmable logic device, PLD）实现，以现场可编程门阵列（Field Programmable Gate Array, FPGA）为例，其可以包括大量逻辑门电路，通过配置文件来配置逻辑门电路之间的连接关系，从而实现以上部分或全部单元或模块的功

50

能。以上装置的所有单元或模块可以全部通过处理器调用软件的形式实现，或全部通过硬件电路的形式实现，或部分通过处理器调用软件的形式实现，剩余部分通过硬件电路的形式实现。

在本公开实施例中，处理器是具有信号处理能力的电路，在一种实现中，处理器可以是具有指令读取与运行能力的电路，例如中央处理单元（Central Processing Unit, CPU）、微处理器、图形处理器（graphics processing unit, GPU）（可以理解为微处理器）、或数字信号处理器（digital signal processor, DSP）等；在另一种实现中，处理器可以通过硬件电路的逻辑关系实现一定功能，上述硬件电路的逻辑关系是固定的或可以重构的，例如处理器为专用集成电路(application-specific integrated circuit, ASIC)或可编程逻辑器件(programmable logic device, PLD)实现的硬件电路,例如 FPGA。在可重构的硬件电路中，处理器加载配置文档，实现硬件电路配置的过程，可以理解为处理器加载指令，以实现以上部分或全部单元或模块的功能的过程。此外，还可以是针对人工智能设计的硬件电路,其可以理解为 ASIC,例如神经网络处理单元(Neural Network Processing Unit, NPU)、张量处理单元(Tensor Processing Unit, TPU)、深度学习处理单元(Deep learning Processing Unit, DPU)等。

图 6A 是本公开实施例提出的第一用户设备的结构示意图。如图 6A 所示，第一用户设备 6100 可以包括：收发模块 6101、处理模块 6102 等中的至少一者。在一些实施例中，收发模块，用于向第二用户设备发送第一消息，其中，第一消息包括未受保护内容信息；收发模块，还用于接收第二用户设备发送的第二消息，其中，第二消息包括待验证信息，待验证信息包括未受保护内容信息的至少一部分；处理模块，用于验证待验证信息；收发模块，用于向第二用户设备发送第三消息，其中，第三消息用于指示待验证信息的验证结果；收发模块，还用于接收第二用户设备发送的第四消息。可选地，上述处理模块用于执行以上任一方法中第一用户设备 101 执行的发送和/或接收等通信步骤（例如步骤 S2101，但不限于此）中的至少一者，此处不再赘述。可选地，上述处理模块用于执行以上任一方法中第一用户设备 101 执行的其他步骤（例如步骤 S2104，但不限于此）中的至少一者，此处不再赘述。

图 6B 是本公开实施例提出的第二用户设备的结构示意图。如图 6B 所示，第二用户设备 6200 可以包括：收发模块 6201、处理模块 6202 等中的至少一者。在一些实施例中，上述收发模块，用于接收第一用户设备发送的第一消息，其中，第一消息包括未受保护内容信息；收发模块，还用于向第一用户设备发送第二消息，其中，第二消息包括待验证信息，待验证信息包括未受保护内容信息的至少一部分；收发模块，还用于接收第一用户设备发送的第三消息，其中，第三消息指示待验证信息的验证结果；收发模块，还用于根据第三消息向第一用户设备发送第四消息。可选地，上述收发模块用于执行以上任一方法中第二用户设备 102 执行的发送和/或接收等通信步骤（例如步骤 S2103，但不限于此）中的至少一者，此处不再赘述。可选地，上述处理模块用于执行以上任一方法中第二用户设备 101 执行的其他步骤（例如步骤 S2102，但不限于此）中的至少一者，此处不再赘述。

在一些实施例中，收发模块可以包括发送模块和/或接收模块，发送模块和接收模块可以是分离的，也可以集成在一起。可选地，收发模块可以与收发器相互替换。

在一些实施例中，处理模块可以是一个模块，也可以包括多个子模块。可选地，上述多个子模块分别执行处理模块所需执行的全部或部分步骤。可选地，处理模块可以与处理器相互替换。

图 7A 是本公开实施例提出的通信设备 7100 的结构示意图。通信设备 7100 可以是网络设备（例如接入网设备、核心网设备等），也可以是终端（例如用户设备等），也可以是支持网络设备实现以上任一方法的芯片、芯片系统、或处理器等，还可以是支持终端实现以上任一方法的芯片、芯片系统、或处理器等。通信设备 7100 可用于实现上述方法实施例中描述的方法，具体可以参见上述方法实施例中的说明。

如图 7A 所示，通信设备 7100 包括一个或多个处理器 7101。处理器 7101 可以是通用处理器或者专用处理器等，例如可以是基带处理器或中央处理器。基带处理器可以用于对通信协议以及通信数据进行处理，中央处理器可以用于对通信装置（如，基站、基带芯片，终端设备、终端设备芯片，DU 或 CU 等）进行控制，执行程序，处理程序的数据。通信设备 7100 用于执行以上任一方法。

在一些实施例中，通信设备 7100 还包括用于存储指令的一个或多个存储器 7102。可选地，全部或部分存储器 7102 也可以处于通信设备 7100 之外。

在一些实施例中，通信设备 7100 还包括一个或多个收发器 7103。在通信设备 7100 包括一个或多个收发器 7103 时，收发器 7103 执行上述方法中的发送和/或接收等通信步骤（例如步骤 S2102，但不限于此）

中的至少一者，处理器 7101 执行其他步骤（例如步骤 S2101，但不限于此）中的至少一者。

在一些实施例中，收发器可以包括接收器和/或发送器，接收器和发送器可以是分离的，也可以集成在一起。可选地，收发器、收发单元、收发机、收发电路等术语可以相互替换，发送器、发送单元、发送机、发送电路等术语可以相互替换，接收器、接收单元、接收机、接收电路等术语可以相互替换。

5 在一些实施例中，通信设备 7100 可以包括一个或多个接口电路 7104。可选地，接口电路 7104 与存储器 7102 连接，接口电路 7104 可用于从存储器 7102 或其他装置接收信号，可用于向存储器 7102 或其他装置发送信号。例如，接口电路 7104 可读取存储器 7102 中存储的指令，并将该指令发送给处理器 7101。

10 以上实施例描述中的通信设备 7100 可以是网络设备或者终端，但本公开中描述的通信设备 7100 的范围并不限于此，通信设备 7100 的结构可以不受图 7A 的限制。通信设备可以是独立的设备或者可以是较大设备的一部分。例如所述通信设备可以是：（1）独立的集成电路 IC，或芯片，或，芯片系统或子系统；（2）具有一个或多个 IC 的集合，可选地，上述 IC 集合也可以包括用于存储数据，程序的存储部件；（3）ASIC，例如调制解调器（Modem）；（4）可嵌入在其他设备内的模块；（5）接收机、终端设备、智能终端设备、蜂窝电话、无线设备、手持机、移动单元、车载设备、网络设备、云设备、人工智能设备等等；（6）其他等等。

15 图 7B 是本公开实施例提出的芯片 7200 的结构示意图。对于通信设备 7200 可以是芯片或芯片系统的情况，可以参见图 7B 所示的芯片 7200 的结构示意图，但不限于此。

芯片 7200 包括一个或多个处理器 7201，芯片 8200 用于执行以上任一方法。

20 在一些实施例中，芯片 7200 还包括一个或多个接口电路 7202。可选地，接口电路 7202 与存储器 7203 连接，接口电路 7202 可以用于从存储器 7203 或其他装置接收信号，接口电路 7202 可用于向存储器 7203 或其他装置发送信号。例如，接口电路 7202 可读取存储器 7203 中存储的指令，并将该指令发送给处理器 7201。

在一些实施例中，接口电路 7202 执行上述方法中的发送和/或接收等通信步骤（例如步骤 S2102，但不限于此）中的至少一者，处理器 7201 执行其他步骤（例如步骤 S2101，但不限于此）中的至少一者。

在一些实施例中，接口电路、接口、收发管脚、收发器等术语可以相互替换。

25 在一些实施例中，芯片 7200 还包括用于存储指令的一个或多个存储器 7203。可选地，全部或部分存储器 7203 可以处于芯片 7200 之外。

30 本公开还提出存储介质，上述存储介质上存储有指令，当上述指令在通信设备 7100 上运行时，使得通信设备 7100 执行以上任一方法。可选地，上述存储介质是电子存储介质。可选地，上述存储介质是计算机可读存储介质，但不限于此，其也可以是其他装置可读的存储介质。可选地，上述存储介质可以是非暂时性（non-transitory）存储介质，但不限于此，其也可以是暂时性存储介质。

本公开还提出程序产品，上述程序产品被通信设备 7100 执行时，使得通信设备 7100 执行以上任一方法。可选地，上述程序产品是计算机程序产品。

本公开还提出计算机程序，当其在计算机上运行时，使得计算机执行以上任一方法。

权利要求书

- 1、一种通信处理方法，其特征在于，所述方法由第一用户设备执行，所述方法包括：
向第二用户设备发送第一消息，其中，所述第一消息包括未受保护内容信息；
接收所述第二用户设备发送的第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；
验证所述待验证信息；
向所述第二用户设备发送第三消息，其中，第三消息用于指示所述待验证信息的验证结果；
接收所述第二用户设备发送的第四消息。
- 2、如权利要求 1 所述的方法，其特征在于，所述第一消息为直接通信请求 DCR 消息。
- 3、如权利要求 1 或 2 所述的方法，其特征在于，所述未受保护内容信息包括第一信息和第二信息，所述第二信息为安全保护相关的信息。
- 4、如权利要求 1-3 任一所述的方法，其特征在于，所述第二消息为 DSMC 消息。
- 5、如权利要求 3 所述的方法，其特征在于，所述验证所述待验证信息，包括：
根据所述第一信息对所述待验证信息进行验证。
- 6、如权利要求 1-5 所述的方法，其特征在于，所述验证结果为验证通过，所述第三消息为直接安全模式完成消息；或者，所述验证结果为验证未通过，所述第三消息为直接安全模式拒绝消息。
- 7、如权利要求 6 所述的方法，其特征在于，所述第四消息为直接通信接受消息时，直接通信连接建立成功；或者，所述第四消息为直接通信拒绝消息时，直接通信连接建立失败。
- 8、如权利要求 3 所述的方法，其特征在于，所述第一信息包括以下至少一项：
测距与侧行链路定位协议 RSPP 元数据；
目标用户信息；
源用户信息；
组标识 ID；
业务信息。
- 9、如权利要求 3 所述的方法，其特征在于，所述第二信息包括所述第一用户设备的 PC5 安全策略信息、第一用户设备安全能力的至少一项。
- 10、一种通信处理方法，其特征在于，所述方法由第二用户设备执行，所述方法包括：
接收第一用户设备发送的第一消息，其中，所述第一消息包括未受保护内容信息；
向所述第一用户设备发送第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；
接收所述第一用户设备发送的第三消息，其中，所述第三消息指示所述待验证信息的验证结果；
根据所述第三消息向所述第一用户设备发送第四消息。
- 11、如权利要求 10 所述的方法，其特征在于，所述第一消息为直接通信请求 DCR 消息。
- 12、如权利要求 10 或 11 所述的方法，其特征在于，所述未受保护内容信息包括第一信息和第二信息，所述第二信息为安全保护相关的信息。

13、如权利要求 10-12 任一所述的方法，其特征在于，所述第二消息为直接安全模式命令 DSMC 消息。

5 14、如权利要求 10-13 任一所述的方法，其特征在于，
所述验证结果为验证通过，所述第三消息为直接安全模式完成消息；或者，
所述验证结果为验证未通过，所述第三消息为直接安全模式拒绝消息。

10 15、如权利要求 14 所述的方法，其特征在于，
所述第三消息为直接安全模式完成消息，所述第四消息为直接通信接受消息；或者，
所述第三消息为直接安全模式拒绝消息，所述第四消息为直接通信拒绝消息。

15 16、如权利要求 12 所述的方法，其特征在于，所述第一信息包括以下至少一项：
测距与侧行链路定位协议 RSPP 元数据；
目标用户信息；
源用户信息；
组标识 ID；
业务信息。

20 17、如权利要求 12 所述的方法，其特征在于，所述第二信息包括所述第一用户设备的 PC5 安全策略信息、第一用户设备安全能力的至少一项。

25 18、一种第一用户设备，其特征在于，包括：
收发模块，用于向第二用户设备发送第一消息，其中，所述第一消息包括未受保护内容信息；
所述收发模块，还用于接收所述第二用户设备发送的第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；
处理模块，用于验证所述待验证信息；
所述收发模块，用于向所述第二用户设备发送第三消息，其中，第三消息用于指示所述待验证信息的验证结果；
30 所述收发模块，还用于接收所述第二用户设备发送的第四消息。

35 19、一种第二用户设备，其特征在于，包括：
收发模块，用于接收第一用户设备发送的第一消息，其中，所述第一消息包括未受保护内容信息；
所述收发模块，还用于向所述第一用户设备发送第二消息，其中，所述第二消息包括待验证信息，所述待验证信息包括所述未受保护内容信息的至少一部分；
所述收发模块，还用于接收所述第一用户设备发送的第三消息，其中，所述第三消息指示所述待验证信息的验证结果；
40 所述收发模块，还用于根据所述第三消息向所述第一用户设备发送第四消息。

45 20、一种通信设备，其特征在于，包括：
一个或多个处理器；
其中，所述处理器用于调用指令以使得所述通信设备执行权利要求 1-9、10-17 中任一项所述的方法。

21、一种通信系统，其特征在于，包括：
第一用户设备，用于实现权利要求 1-9 中任一项所述的通信处理方法；
第二用户设备，用于实现权利要求 10-17 中任一项所述的通信处理方法。

22、一种存储介质，所述存储介质存储有指令，其特征在于，当所述指令在通信设备上运行时，使得所述通信设备执行如权利要求 1-9、10-17 中任一项所述的通信处理方法。

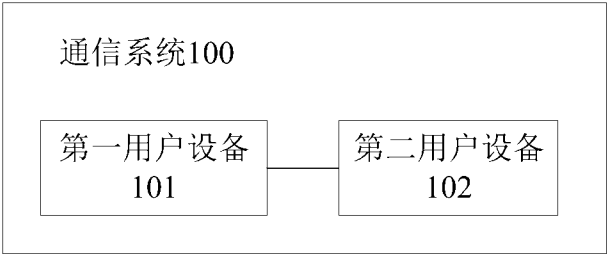


图 1

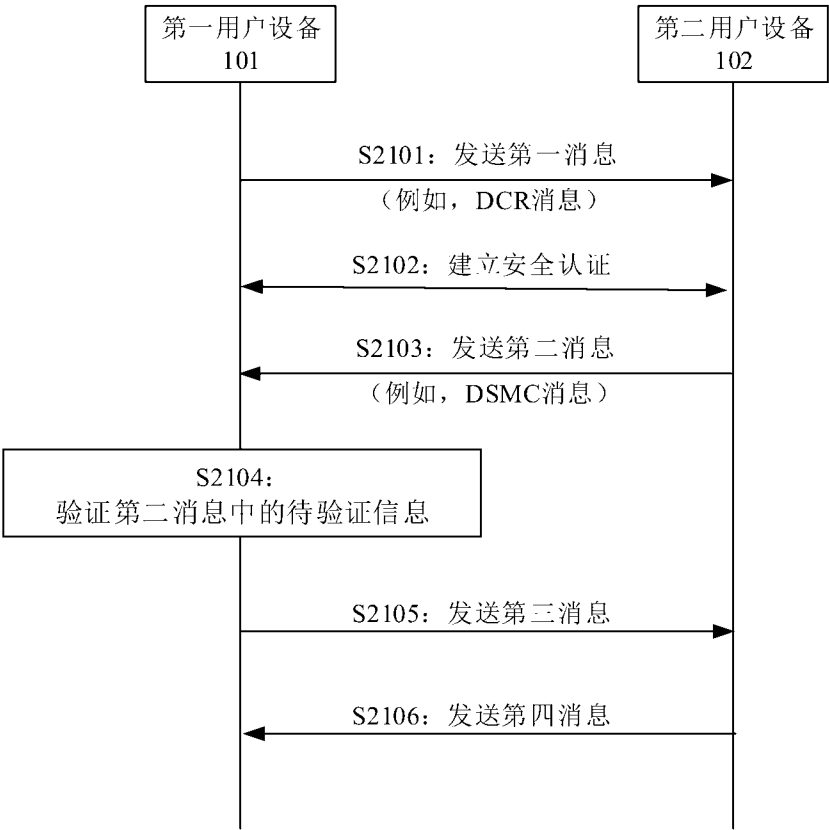
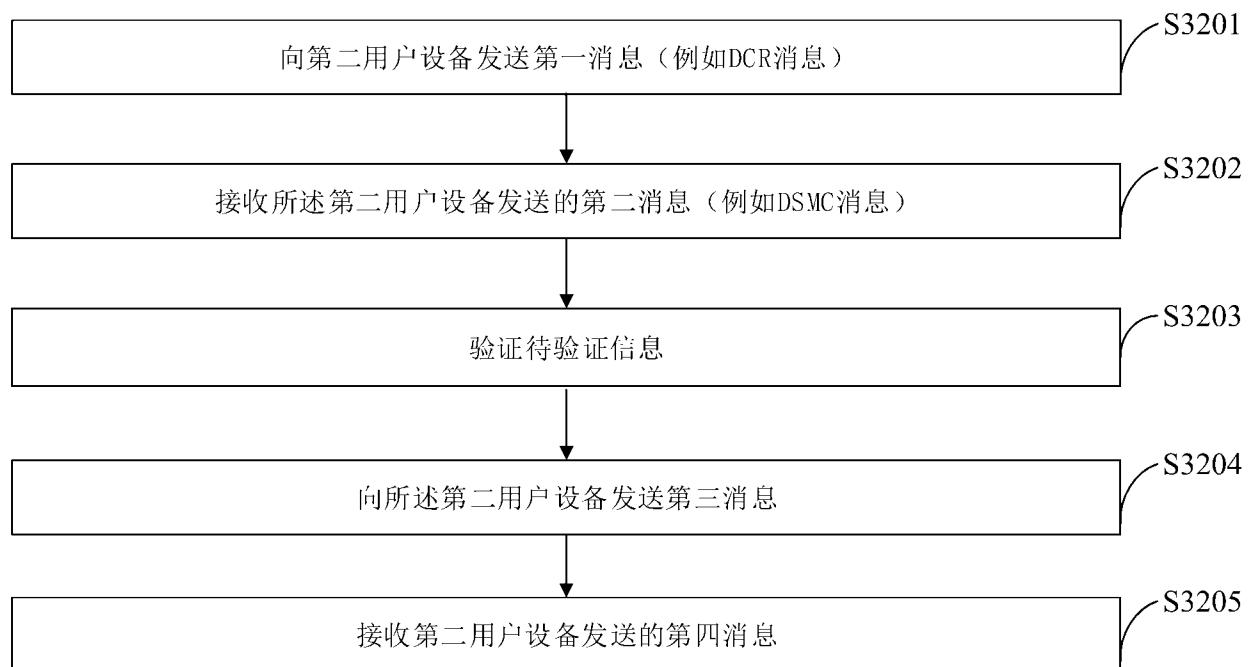
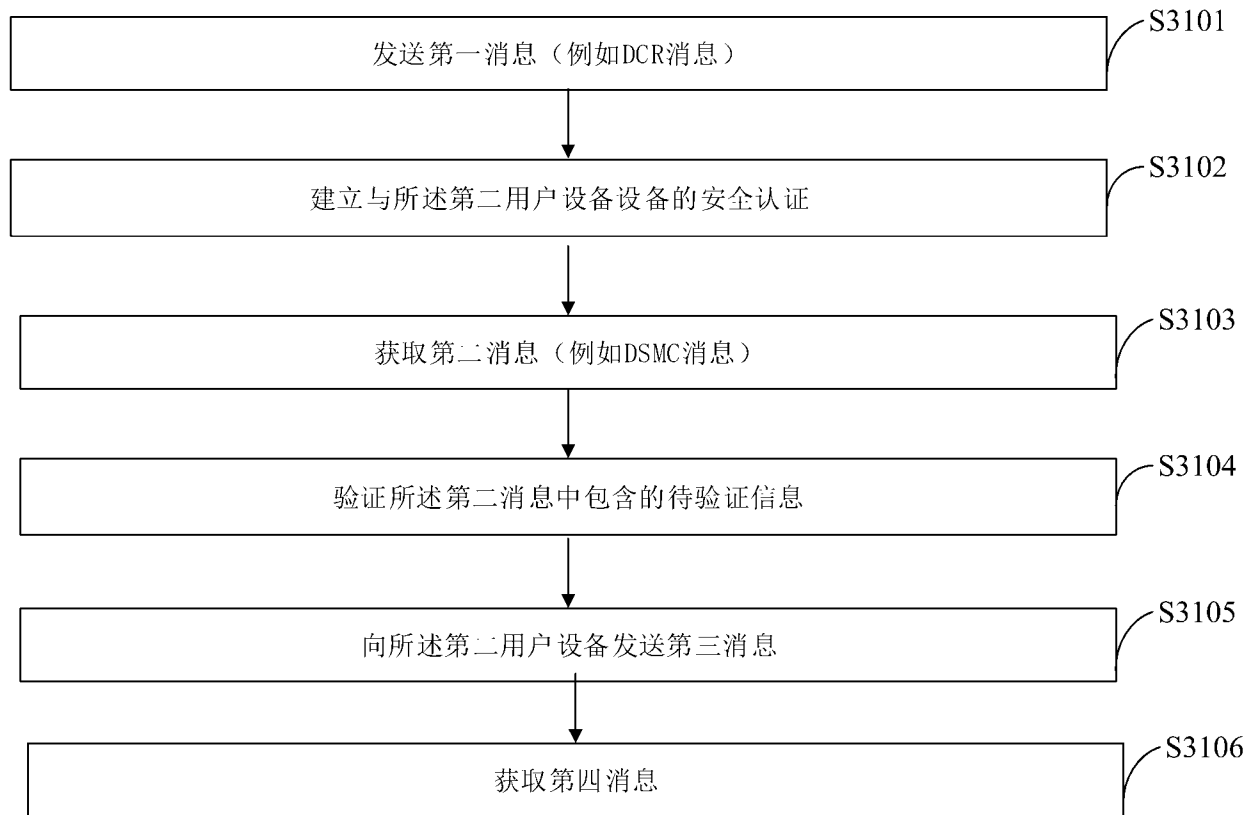


图 2



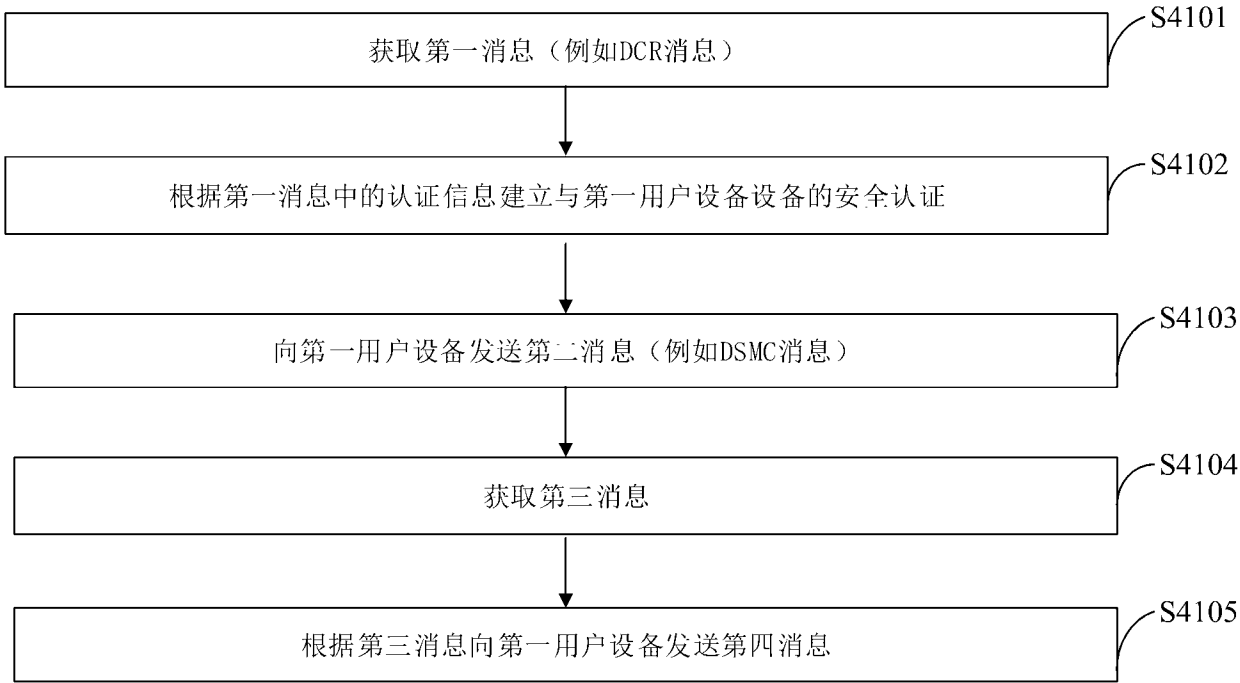


图 4A

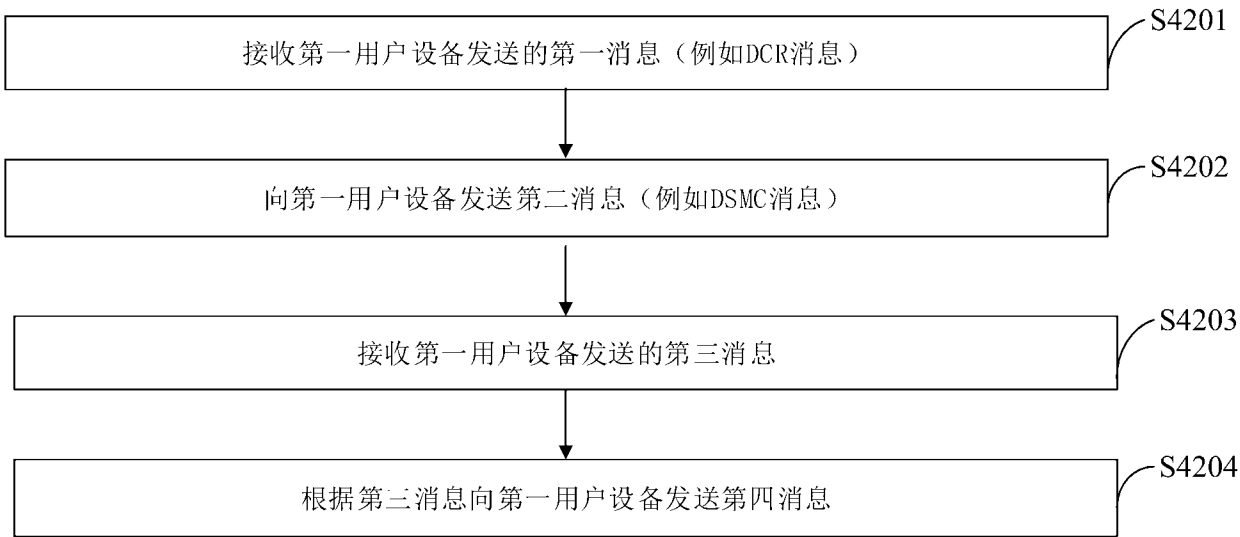


图 4B

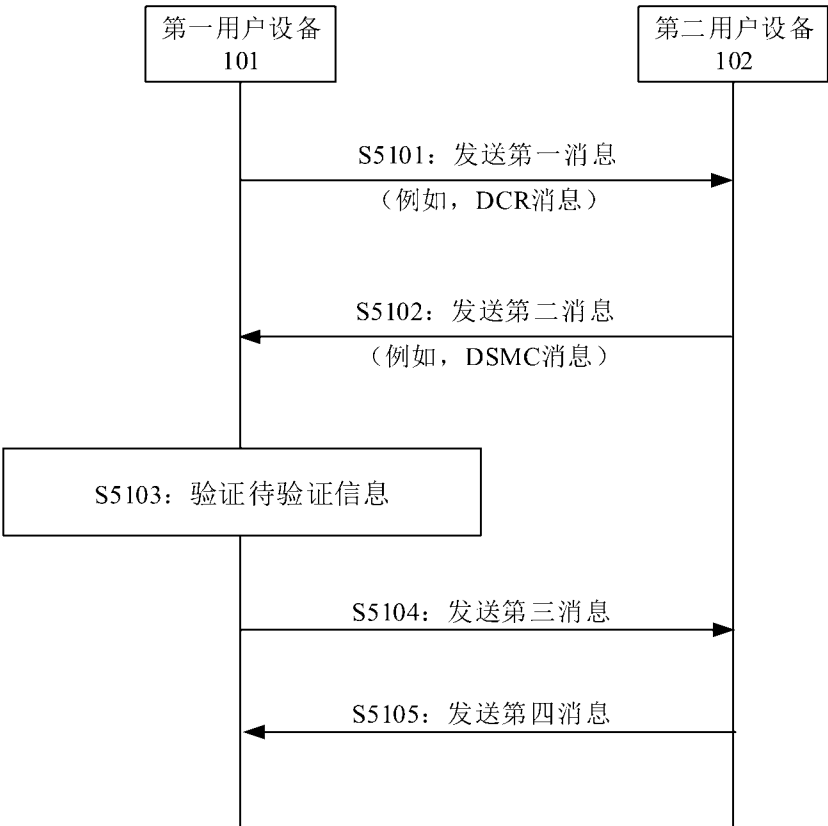


图 5

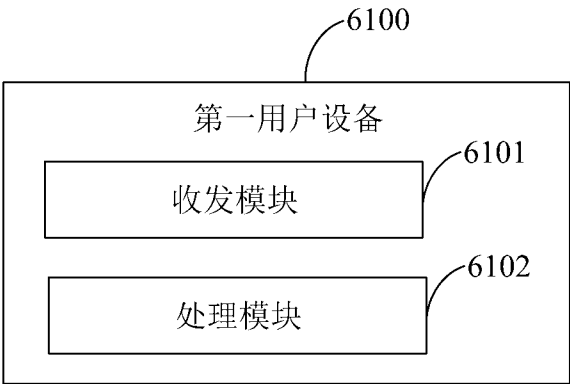


图 6A

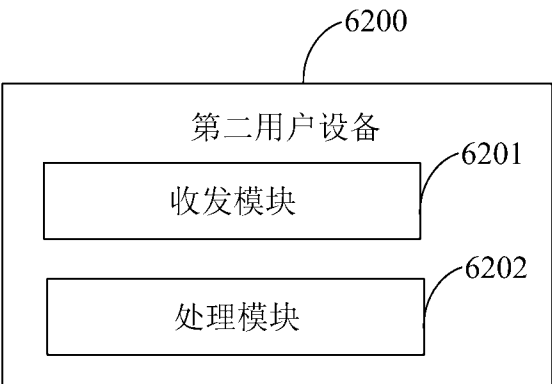


图 6B

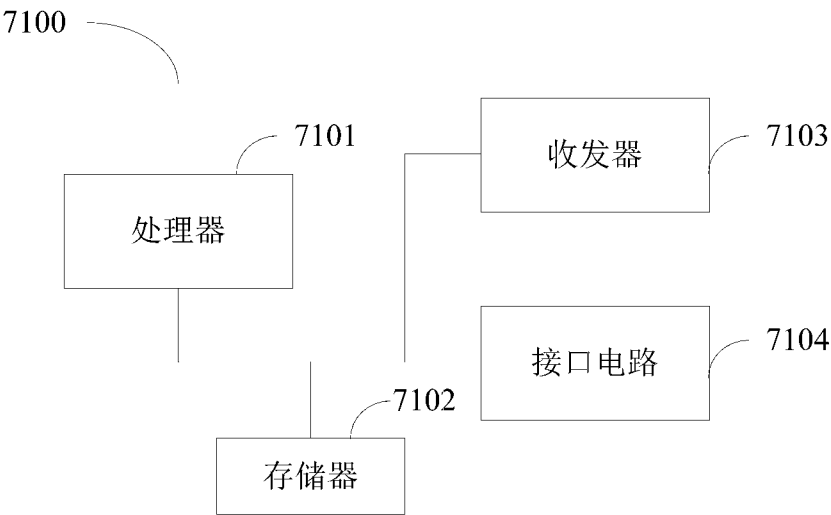


图 7A

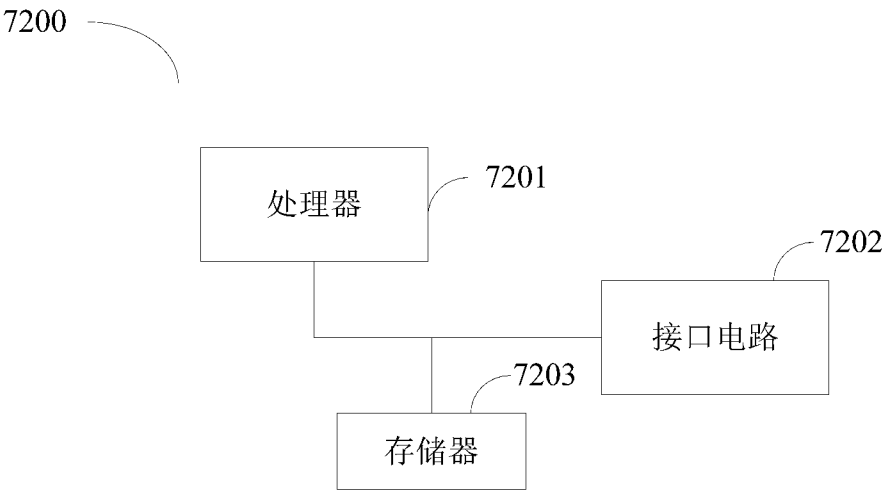


图 7B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/106667

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)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: 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)

3GPP, CNTXT, ENTXT, ENTXTC, VEN, WPABSC, CNKI: 保护, 认证, 验证, 完整性, 直接通信请求, 直连通信请求, 直接安全模式命令, 直连安全模式命令, protect, verify, authenticate, authorize, integrity, direct communication request, DCR, direct security mode command, DSMC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 113676898 A (HUAWEI TECHNOLOGIES CO., LTD.) 19 November 2021 (2021-11-19) claims 1-25, description, paragraphs [0247]-[0291], and figure 7	1-22
A	CN 115836539 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 March 2023 (2023-03-21) entire document	1-22
A	CN 116325845 A (HUAWEI TECHNOLOGIES CO., LTD.) 23 June 2023 (2023-06-23) entire document	1-22
A	US 2022360966 A1 (QUALCOMM INC.) 10 November 2022 (2022-11-10) entire document	1-22

☐ 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

05 March 2024

Date of mailing of the international search report

11 March 2024

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/CN2023/106667

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	113676898	A	19 November 2021	None	
CN	115836539	A	21 March 2023	None	
CN	116325845	A	23 June 2023	None	
US	2022360966	A1	10 November 2022	None	

A. 主题的分类

H04L 9/40(2022.01)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: 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))

3GPP,CNTEXT,ENTXT,ENTXTC,VEN,WPABSC,CNKL:保护,认证,验证,完整性,直接通信请求,直连通信请求,直接安全模式命令,直连安全模式命令, protect, verify, authenticate, authorize, integrity, direct communication request, DCR, direct security mode command, DSMC

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 113676898 A (华为技术有限公司) 2021年11月19日 (2021 - 11 - 19) 权利要求1-25, 说明书第[0247]-[0291]段, 图7	1-22
A	CN 115836539 A (华为技术有限公司) 2023年3月21日 (2023 - 03 - 21) 全文	1-22
A	CN 116325845 A (华为技术有限公司) 2023年6月23日 (2023 - 06 - 23) 全文	1-22
A	US 2022360966 A1 (QUALCOMM INC) 2022年11月10日 (2022 - 11 - 10) 全文	1-22

☐ 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

2024年3月5日

国际检索报告邮寄日期

2024年3月11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

李美丽

电话号码 (+86) 010-62089957

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/CN2023/106667

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	113676898	A	2021年11月19日	无	
CN	115836539	A	2023年3月21日	无	
CN	116325845	A	2023年6月23日	无	
US	2022360966	A1	2022年11月10日	无	