(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
2023 年 4 月 6 日 (06.04.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/050373 A1

(51) 国际专利分类号:
H04W 12/06 (2021.01) *H04W 12/04* (2021.01)

(21) 国际申请号: PCT/CN2021/122352

(22) 国际申请日: 2021 年 9 月 30 日 (30.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

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

(72) 发明人: 王勇 (WANG, Yong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李明超 (LI, Mingchao); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 何青春 (HE, Qingchun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** COMMUNICATION METHOD, APPARATUS AND SYSTEM

(54) **发明名称**: 一种通信方法、装置及系统

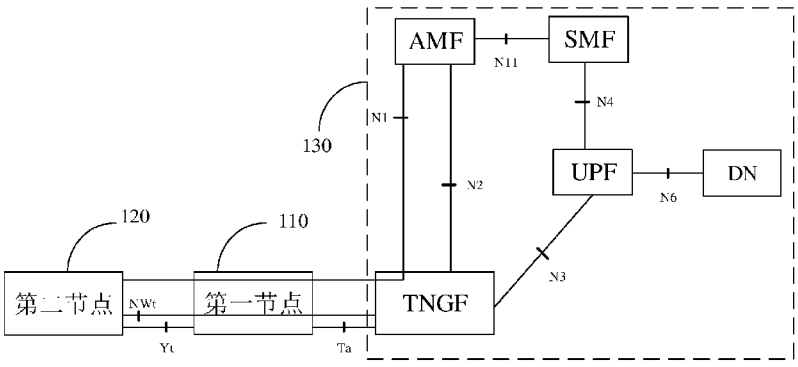

图 2

110 First node
120 Second node

(57) **Abstract:** A communication method, apparatus and system, which relate to the technical field of communications. The method comprises: a first node/a second node acquiring first information; and establishing a first communication connection according to the first information and the second node, wherein the first communication connection is used for transmitting data of a first service, the first communication connection corresponds to first communication technology, the first node is a node that accesses a network corresponding to second communication technology, and the first service is a service of the first communication technology or a service of the second communication technology. The solution is conducive to satisfying a security requirement of heterogeneous communication technology in a converged communication scenario.

(57) **摘要**: 一种通信方法、装置及系统，涉及通信技术领域。该方法包括：第一节点/第二节点获取第一信息；根据所述第一信息与第二节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点，所述第一业务为所述第一通信技术的业务或者所述第二通信技术的业务。通过该方案，有助于满足异构式通信技术在融合通信场景中的安全需求。

WO 2023/050373 A1

[见续页]

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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种通信方法、装置及系统

技术领域

本申请实施例涉及通信技术领域，特别涉及一种通信方法、装置及系统。

背景技术

随着信息化飞速发展，移动终端（例如手机、平板电脑、或其他可携带式智能终端等）已成为个人不可缺少的重要智能工具。进入移动互联网时代后，这些移动终端和传统的计算机（例如台式工作站、服务器等）相比，使用更加便利，同时也更加容易威胁与损害个人的信息，因此通信技术的安全性至关重要。

随着智能汽车、智能终端、智能家居和智能制造等新兴产业的快速发展，创新需求和应用不断涌现，在一些场景中，提出基于不同通信技术进行融合通信的设计，而如何保障异构式通信技术在融合通信场景中的安全需求仍为亟需解决的重要问题。

发明内容

本申请实施例提供了一种通信方法、装置及系统，有助于满足异构式通信技术在融合通信场景中的安全需求。

第一方面，本申请实施例提供一种通信方法，该方法可应用于第一节点，该第一节点可以支持第一通信技术和第二通信技术。该方法可以包括：获取第一信息；根据所述第一信息与第二节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点。示例地，所述第一业务可以为所述第一通信技术的业务或者所述第二通信技术的业务。

通过上述方法，第一节点可基于与第一业务关联的第一信息，来建立第一节点与第二节点之间的第一通信连接，进而使得第一节点和第二节点之间进行业务数据传输时，可以使用与所述第一业务对应的通信连接传输该第一业务对应的数据，不同的通信连接可以对应不同的业务数据传输，以满足融合通信场景下的安全需求，并保障相应业务数据的安全性。示例地，该第一通信技术可为短距离通信技术，第二通信技术可为第五代移动通信技术（the 5th generation mobile communication technology，5G）。

需要说明的是，本申请实施例仅是以基于第一通信技术和第一通信技术的融合场景为例进行说明，本申请实施例还可以应用于其它融合通信场景中，第一业务也可以包括对应其它通信技术的业务，本申请实施例对此不做限定。

结合第一方面，在一种可能的实现方式中，所述第一信息可以包括用于与所述第二节点通信认证的第一密钥，所述获取第一信息，可以包括：根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。

通过上述方法，可由第一节点触发第一节点与第二节点之间的连接建立过程，该第一节点可以根据当前所处的通信场景和/或业务需求获取第一密钥，以便根据所获取的第一密钥，在第一节点和第二节点之间建立相应的第一通信连接，来传输对应于第一业务的数据。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。

结合第一方面，在一种可能的实现方式中，所述第一信息可以包括用于与所述第二节点通信认证的第一密钥，所述方法还包括：接收来自所述第二节点的第一消息，所述第一消息承载密钥类型指示信息或业务类型指示信息；所述获取第一信息，包括：根据所述密钥类型指示信息或所述业务类型指示信息，获取所述第一密钥。

通过上述方法，可由第二节点触发第一节点与第二节点之间的连接建立过程，第一节点可以根据来自第二节点的密钥类型指示信息或业务类型指示信息，来获取与第一业务关联的第一密钥，以便基于所获取的第一密钥，在第一节点和第二节点之间建立相应的第一通信连接，来传输对应于第一业务的数据。

结合第一方面，在一种可能的实现方式中，所述根据所述第一信息与第二节点建立第一通信连接，包括：向所述第二节点发送与所述第一密钥关联的第二消息，所述第二消息用于所述第一节点的身份认证；接收响应于所述第二消息的第三消息，所述第三消息用于所述第二节点的身份认证；在所述第二节点的身份认证成功的情况下，向所述第二节点发送第四消息，所述第四消息用于与所述第二节点建立所述第一通信连接。

需要说明的是，本申请实施例中，该第三消息可以对应一个消息，例如该消息可用于所述第二节点的身份认证，以及隐式地指示所述第一节点身份认证成功；或者，又例如该消息既可用于显示地指示所述第一节点身份认证成功、又可用于所述第二节点的身份认证；或者，该第三消息可以对应至少两个消息，例如指示所述第一节点身份认证成功的消息，和用于所述第二节点的身份认证的消息，本申请实施例对该第三消息的具体实现方式不做限定。相似地，第四消息也可以对应一个消息，例如该消息用于与所述第二节点建立所述第一通信连接，以及隐式地指示所述第二节点身份认证成功；或者，又例如该消息既可以用于与所述第二节点建立所述第一通信连接，又可用于显示地指示所述第二节点身份认证成功；或者，该第四消息可以对应至少两个消息，例如用于与所述第二节点建立所述第一通信连接的消息，和用于指示所述第二节点身份认证成功的消息，本申请实施例对该第四消息的具体实现方式不做限定。

通过上述方法，第一节点可以基于所获取的第一密钥，来与第二节点之间相互进行身份认证（或者说身份鉴权），并在相互认证成功后，在双方之间建立安全的第一通信连接。

结合第一方面，在一种可能的实现方式中，所述第一密钥为用于所述第一通信技术的业务的密钥，或者，为用于所述第二通信技术的业务的密钥。

结合第一方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；和/或，在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

通过上述方法，第一节点可以获得至少一个密钥，该第一节点可以根据第一业务在至少一个密钥中进行选择，以便建立与所述第一业务对应的第一通信连接，以保障第一业务的业务数据的安全性。

结合第一方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的密钥包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥，所述非可信密钥为未经过所述网络鉴权的密钥，所述可信密钥的优先级高于所述非可信密钥的优先级。

通过上述方法，第一节点所获得的至少一个密钥可以具有相应的优先级和/或使用原则，使得第一节点可以根据第一业务、所述优先级和/或所述使用原则，在所述至少一个密钥中

选择与该第一业务密切相关的密钥作为所述第一密钥。

需要说明的是，本申请实施例中，密钥和业务是对应的，在第一业务为第一通信技术的业务的情况下，不使用用于第二通信技术的业务的密钥；在第一业务为第二通信技术的业务的情况下，不使用用于第一通信技术的业务的密钥，并且在存在可信密钥的情况下，不使用非可信密钥。

结合第一方面，在一种可能的实现方式中，在建立所述第一通信连接之前，所述方法还包括：接收来自所述网络的用于所述第二通信技术的业务的密钥。

通过上述方法，在基于第一通信技术和第二通信技术的融合通信场景下，第二通信技术的网络可以向第一节点下发用于第二通信技术的业务的密钥，第一节点接收该密钥，以便在所述融合通信场景下，基于该密钥在所述第一节点和第二节点之间建立第一通信连接。应理解，本申请实施例中，用于第二通信技术的业务的密钥可以是默认值也可以是动态变化的数值，本申请实施例对此不做限定。并且，若该密钥为经过所述网络鉴权成功的密钥，该密钥为可信密钥，若该密钥为未经过所述网络鉴权的密钥，该密钥为可信密钥。

结合第一方面，在一种可能的实现方式中，所述第一信息包括用于与所述第二节点通信的第一安全上下文，所述获取第一信息，包括：接收来自所述第二节点的第五消息，所述第五消息承载与所述第一安全上下文关联的标识；所述获取第一信息，包括：根据所述标识，获取所述第一安全上下文。

通过上述方法，第二节点中可以存在多套安全上下文，第二节点例如可以根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，在所述多套安全上下文中选择第一安全上下文，并向第一节点发送所述第五消息，以指示所述第一安全上下文的标识。第一节点可以根据第二节点指示的与第一安全上下文关联的标识，获取对应于所述第一业务的第一安全上下文，从而基于所获取的第一安全上下文，在双方之间建立安全的第一通信连接。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。

结合第一方面，在一种可能的实现方式中，所述第一安全上下文为用于第一通信技术的业务的安全上下文，或者，为用于所述第二通信技术的业务的安全上下文。

结合第一方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；和/或，在所述第一业务为第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

结合第一方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的安全上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文，所述可信安全上下文的优先级高于所述非可信安全上下文的优先级。

通过上述方法，第一节点与第二节点之间可以具有至少一套安全上下文，且所述至少一套安全上下文可以具有相应的优先级和/或使用原则，使得第一节点可以根据第一业务、所述优先级和/或使用原则，在所述至少一套安全上下文中选择与该第一业务密切相关的安全上下文作为所述第一安全上下文。

需要说明的是，本申请实施例中，与密钥相似，安全上下文也是与业务对应的，在第一业务为第一通信技术的业务的情况下，不使用用于第二通信技术的业务的安全上下文；

在第一业务为第二通信技术的业务的情况下，不使用用于第一通信技术的业务的安全上下文，并且在存在可信安全上下文的情况下不使用非可信安全上下文。

结合第一方面，在一种可能的实现方式中，所述获取第一信息之前，所述方法还包括：向所述第二节点发送第六消息，所述第六消息承载用于指示所述第一节点支持所述第二通信技术的信息。需要说明的是，在本申请实施例中，第一节点支持所述第二通信技术，也可以理解为，第一节点支持所述第二通信技术的业务的传输，第一节点支持对应于所述第二通信技术的业务传输，或者，第一节点支持基于所述第二通信技术实现的业务传输。

通过上述方法，第一节点可以在第六消息中携带相关指示信息，来向第二节点告知自身支持的业务类型，以便第二节点根据与第一节点之间进行的业务来进行决策，以便在双方之间建立安全的第一通信连接、传输第一业务的数据。

第二方面，本申请实施例提供了一种通信方法，应用于第二节点，该第二节点可支持第一通信技术，或者，该第二节点可支持第一通信技术和第二通信技术。所述方法可以包括：获取第一信息；根据所述第一信息与第一节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点。示例地，所述第一业务可以为所述第一通信技术的业务或者所述第二通信技术的业务。

结合第二方面，在一种可能的实现方式中，所述第一信息包括用于与所述第一节点通信认证的第一密钥，所述获取第一信息，包括：根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如5G技术。结合第二方面，在一种可能的实现方式中，所述方法还包括：向所述第一节点发送第一消息，所述第一消息承载与所述第一密钥相关联的信息。示例地，与所述第一密钥相关联的信息可以包括密钥类型指示信息或业务类型指示信息。在一种可选的实现方式中，与所述第一密钥相关联的信息也可以是所述第一密钥。

结合第二方面，在一种可能的实现方式中，所述根据第一信息与所述第一节点建立所述第一通信连接，包括：接收来自所述第一节点的第二消息，所述第二消息关联于所述第一密钥，所述第二消息用于所述第一节点的身份认证；在所述第一节点的身份认证成功的情况下，向所述第一节点发送第三消息，所述第三消息用于所述第二节点的身份认证；接收响应于所述第三消息的第四消息，所述第四消息用于与所述第二节点建立所述第一通信连接。

需要说明的是，本申请实施例中，该第三消息可以对应一个消息，例如该消息可用于所述第二节点的身份认证，以及隐式地指示所述第一节点身份认证成功；或者，又例如该消息既可用于显示地指示所述第一节点身份认证成功、又可用于所述第二节点的身份认证；或者，该第三消息可以对应至少两个消息，例如指示所述第一节点身份认证成功的消息，和用于所述第二节点的身份认证的消息，本申请实施例对该第三消息的具体实现方式不做限定。相似地，第四消息也可以对应一个消息，例如该消息用于与所述第二节点建立所述第一通信连接，以及隐式地指示所述第二节点身份认证成功；或者，又例如该消息既可以用于与所述第二节点建立所述第一通信连接，又可用于显示地指示所述第二节点身份认证成功；或者，该第四消息可以对应至少两个消息，例如用于与所述第二节点建立所述第一通信连接的消息，和用于指示所述第二节点身份认证成功的消息，本申请实施例对该第四

消息的具体实现方式不做限定。

结合第二方面，在一种可能的实现方式中，所述第一密钥为用于所述第一通信技术的业务的密钥，或者，为用于所述第二通信技术的业务的密钥。

结合第二方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；和/或，在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

结合第二方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的密钥包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥，所述非可信密钥为未经过所述网络鉴权的密钥，所述可信密钥的优先级高于所述非可信密钥的优先级。

结合第二方面，在一种可能的实现方式中，在建立所述第一通信连接之前，所述方法还包括：接收来自所述网络的用于所述第二通信技术的业务的密钥。

结合第二方面，在一种可能的实现方式中，所述第一信息包括第一安全上下文，所述第一安全上下文用于所述第二节点与所述第一节点建立所述第一通信连接，所述获取第一信息，包括：根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一安全上下文。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如5G技术。

结合第二方面，在一种可能的实现方式中，所述第一安全上下文为用于第一通信技术的业务的安全上下文，或者，为用于所述第二通信技术的业务的安全上下文。

结合第二方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；和/或，在所述第一业务为第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

结合第二方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的安全上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文，所述可信安全上下文的优先级高于所述非可信安全上下文的优先级。结合第二方面，在一种可能的实现方式中，所述方法还包括：向所述第一节点发送第五消息，所述第五消息承载与所述第一安全上下文关联的标识。

结合第二方面，在一种可能的实现方式中，所述方法还包括：接收来自所述第一节点的第六消息，所述第六消息承载用于指示所述第一节点支持对应于所述第二通信技术的信息。需要说明的是，在本申请实施例中，第一节点支持所述第二通信技术，也可以理解为，第一节点支持所述第二通信技术的业务的传输，第一节点支持对应于所述第二通信技术的业务传输，或者，第一节点支持基于所述第二通信技术实现的业务传输。

第三方面，本申请实施例提供了一种通信装置，该通信装置应用于第一节点，包括：通信单元，用于与第二节点通信；处理单元，用于获取第一信息；根据所述第一信息与第二节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点。示例地，所述第一业务为所述第一通信技术的业务或者所述第二通信技术的业务。

结合第三方面，在一种可能的实现方式中，所述第一信息包括用于与所述第二节点通

信认证的第一密钥，所述处理单元用于：根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。结合第三方面，在一种可能的实现方式中，所述第一信息包括用于与所述第二节点通信认证的第一密钥，所述通信单元用于：接收来自所述第二节点的第一消息，所述第一消息承载密钥类型指示信息或业务类型指示信息；所述处理单元用于：根据所述密钥类型指示信息或所述业务类型指示信息，获取所述第一密钥。

结合第三方面，在一种可能的实现方式中，所述通信单元用于：向所述第二节点发送与所述第一密钥关联的第二消息，所述第二消息用于所述第一节点的身份认证；接收响应于所述第二消息的第三消息，所述第三消息用于所述第二节点的身份认证；在所述第二节点的身份认证成功的情况下，向所述第二节点发送第四消息，所述第四消息用于与所述第二节点建立所述第一通信连接。

结合第三方面，在一种可能的实现方式中，所述第一密钥为用于所述第一通信技术的业务的密钥，或者，为用于所述第二通信技术的业务的密钥。

结合第三方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；和/或，在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

结合第三方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的密钥包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥，所述非可信密钥为未经过所述网络鉴权的密钥，所述可信密钥的优先级高于所述非可信密钥的优先级。

结合第三方面，在一种可能的实现方式中，在所述处理单元建立所述第一通信连接之前，所述通信单元还用于：接收来自所述网络的用于所述第二通信技术的业务的密钥。

结合第三方面，在一种可能的实现方式中，所述第一信息包括用于与所述第二节点通信的第一安全上下文，所述通信单元用于：接收来自所述第二节点的第五消息，所述第五消息承载与所述第一安全上下文关联的标识；所述处理单元用于：根据所述标识，获取所述第一安全上下文。

结合第三方面，在一种可能的实现方式中，所述第一安全上下文为用于第一通信技术的业务的安全上下文，或者，为用于所述第二通信技术的业务的安全上下文。

结合第三方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；和/或，在所述第一业务为第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

结合第三方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的安全上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文，所述可信安全上下文的优先级高于所述非可信安全上下文的优先级。结合第三方面，在一种可能的实现方式中，所述通信单元还用于：在所述处理单元获取第一信息之前向所述第二节点发送第六消息，所述第六消息承载用于指示所述第一节点支持对应于所述第二通信技术的信息。

第四方面，本申请实施例提供了一种通信装置，包括：通信单元，用于与第一节点通信；处理单元，用于获取第一信息；根据所述第一信息与第一节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点。示例地，所述第一业务可以为所述第一通信技术的业务或者所述第二通信技术的业务。

结合第四方面，在一种可能的实现方式中，所述第一信息包括用于与所述第一节点通信认证的第一密钥，所述处理单元用于：根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。结合第四方面，在一种可能的实现方式中，所述通信单元还用于：向所述第一节点发送第一消息，所述第一消息承载与所述第一密钥关联的信息。示例地，与所述第一密钥关联的信息例如可以包括密钥类型指示信息或业务类型指示信息。

结合第四方面，在一种可能的实现方式中，所述通信单元用于：接收来自所述第一节点的第二消息，所述第二消息关联于所述第一密钥，所述第二消息用于所述第一节点的身份认证；在所述第一节点的身份认证成功的情况下，向所述第二节点发送第三消息，所述第三消息用于所述第二节点的身份认证；接收响应于所述第三消息的第四消息，所述第四消息用于与所述第二节点建立所述第一通信连接。

结合第四方面，在一种可能的实现方式中，所述第一密钥为用于所述第一通信技术的业务的密钥，或者，为用于所述第二通信技术的业务的密钥。

结合第四方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；和/或，在所述第一业务为第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

结合第四方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的密钥包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥，所述非可信密钥为未经过所述网络鉴权的密钥，所述可信密钥的优先级高于所述非可信密钥的优先级。

结合第四方面，在一种可能的实现方式中，在所述处理单元建立所述第一通信连接之前，所述方法还包括：接收来自所述网络的用于所述第二通信技术的业务的密钥。

结合第四方面，在一种可能的实现方式中，所述第一信息包括第一安全上下文，所述第一安全上下文用于所述第二节点与所述第一节点建立所述第一通信连接，所述处理单元用于：根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一安全上下文。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。

结合第四方面，在一种可能的实现方式中，所述第一安全上下文为用于第一通信技术的业务的安全上下文，或者，为用于所述第二通信技术的业务的安全上下文。

结合第四方面，在一种可能的实现方式中，在所述第一业务为第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；和/或，在所述第一业务为第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

结合第四方面，在一种可能的实现方式中，所述用于所述第二通信技术的业务的安全

上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文，所述可信安全上下文的优先级高于所述非可信安全上下文的优先级。

结合第四方面，在一种可能的实现方式中，所述通信单元还用于：向所述第一节点发送第五消息，所述第五消息承载与所述第一安全上下文关联的标识。

结合第四方面，在一种可能的实现方式中，所述通信单元还用于：接收来自所述第一节点的第六消息，所述第六消息承载用于指示所述第一节点支持对应于所述第二通信技术的信息。

第五方面，本申请实施例提供了一种通信装置，包括：处理器和存储器；所述存储器用于存储程序；所述处理器用于执行所述存储器所存储的程序，以使所述装置实现如上第一方面以及第一方面的任一可能实现方式所述的方法，或者，实现如上第二方面以及第二方面的任一可能实现方式所述的方法。

第六方面，本申请实施例提供了一种通信装置，包括：至少一个处理器和接口电路，所述接口电路用于为所述至少一个处理器提供数据或者代码指令，所述至少一个处理器用于通过逻辑电路或执行代码指令实现如上第一方面以及第一方面的任一可能实现方式所述的方法，或者，实现如上第二方面以及第二方面的任一可能实现方式所述的方法。

第七方面，本申请实施例提供了一种通信系统，包括如上第三方面以及第三方面任一可能实现方式所述的通信装置，和，如上第四方面以及第四方面任一可能实现方式所述的通信装置。

第八方面，本申请实施例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存储有程序代码，当所述程序代码在所述计算机上运行时，使得计算机执行上述第一方面以及第一方面的任一可能实现方式所述的方法，或者，当所述程序代码在计算机上运行时，使得计算机执行上述第二方面以及第二方面的任一可能实现方式所述的方法。

第九方面，本申请实施例提供了一种计算机程序产品，当所述计算机程序产品在计算机上运行时，使得所述计算机执行上述第一方面以及第一方面的任一可能实现方式所述的方法，或执行上述第二方面以及第二方面的任一可能实现方式所述的方法。

第十方面，本申请实施例提供了一种芯片系统，该芯片系统包括处理器，用于调用存储器中存储的计算机程序或计算机指令，以使得该处理器执行上述第一方面以及第一方面的任一可能实现方式所述的方法，或执行上述第二方面以及第二方面任一可能实现方式所述的方法。

结合第十方面，在一种可能的实现方式中，该处理器通过接口与存储器耦合。

结合第十方面，在一种可能的实现方式中，该芯片系统还包括存储器，该存储器中存储有计算机程序或计算机指令。

第十一方面，本申请实施例提供了一种处理器，该处理器用于调用存储器中存储的计算机程序或计算机指令，以使得该处理器执行上述第一方面以及第一方面任一可能实现方式所述的方法，或执行上述第二方面以及第二方面任一可能实现方式所述的方法。

第十二方面，本申请实施例提供了一种终端设备，该终端设备可用于实现上述第一方面以及第一方面任一可能实现方式所述的方法，或者实现上述第二方面以及第二方面任一可能实现方式所述的方法。示例地，该终端设备包括但不限于：智能运输设备（诸如汽车、轮船、无人机、火车、货车等）、智能制造设备（诸如机器人、工业设备、智能物流、智

能工厂等）、智能终端（手机、计算机、平板电脑、掌上电脑、台式机、耳机、音响、穿戴设备、车载设备等）。

第十三方面，本申请实施例提供了一种车辆，该车辆可用于实现如上述第一方面以及第一方面任一可能实现方式所述的方法，和/或，实现如上述第二方面以及第二方面任一可能实现方式所述的方法。

第十四方面，本申请实施例提供了一种车辆，该车辆可以包括上述第三方面以及第三方面任一可能实现方式所述的通信装置，和/或实现上述第四方面以及第四方面任一可能实现方式所述的通信装置。

本申请实施例在上述各方面提供的实现的基础上，还可以进行进一步组合以提供更多实现。

上述第二方面至第十四方面中任一方面中的任一可能实现方式可以达到的技术效果，可以相应参照上述第一方面中任一方面中的任一可能实现方式可以达到的技术效果描述，重复之处不予论述。

附图说明

图 1 示出了本申请实施例适用的系统架构的示意图；
图 2 示出了本申请实施例适用的系统架构的示意图；
图 3 示出了本申请实施例的通信方法的流程示意图；
图 4a 示出了本申请实施例的通信方法的流程示意图；
图 4b 示出了本申请实施例的通信方法的流程示意图；
图 4c 示出了本申请实施例的通信方法的流程示意图；
图 4d 示出了本申请实施例的通信方法的流程示意图；
图 5 示出了本申请实施例的通信装置的示意图；
图 6 示出了本申请实施例的通信装置的示意图。

具体实施方式

本申请实施例提供了一种通信方法、装置及系统，有助于满足异构式通信技术在融合通信场景下的安全需求。其中，方法和装置是基于同一技术构思的，由于方法及装置解决问题的原理相似，因此装置与方法的实施可以相互参见，重复之处不再赘述。为了便于理解，下面结合附图及实施例进行介绍。

图 1 示出了本申请实施例适用的系统架构的示意图。

参阅图 1 所示，该系统架构中可以包括第一节点 110、第二节点 120、第三节点 130。其中，第一节点 110 和第二节点 120 可以组成第一通信系统，双方之间可以采用第一通信技术进行通信。第一节点 110 和第三节点 130 可以组成第二通信系统，双方之间可以采用第二通信技术进行通信，第一通信技术与第二通信技术不同。在该第一通信技术和第二通信技术的融合通信场景中，第一通信系统与第二通信系统之间可以建立通信连接，组成异构式通信系统，以便在该异构式通信系统中执行相应的通信业务和/或传输通信业务数据。示例地，该异构式通信系统还可以称为融合后的通信系统，或者紧耦合（tight interworking）的通信系统，或者互相配合（interworking）的通信系统。

本申请实施例中，第一节点 110、第二节点 120、或第三节点 130 中的任一个节点，可以是具有数据收发能力的电子设备。

示例地，该电子设备可以为终端设备，包括向用户提供语音和/或数据连通性的设备，具体地，包括向用户提供语音的设备，或包括向用户提供数据连通性的设备，或包括向用户提供语音和数据连通性的设备。例如，包括具有无线连接功能的手持式设备、或连接到无线调制解调器的处理设备。该终端设备比如可以经无线接入网（radio access network，RAN）与核心网进行通信，与 RAN 交换语音和/或数据。

在具体实施过程中，该终端设备可以包括但不限于车辆、用户设备（user equipment，UE）、无线终端设备、移动终端设备、设备到设备（device-to-device，D2D）终端设备、车到一切（vehicle to everything，V2X）终端设备、机器到机器/机器类通信（machine-to-machine/machine-type communications，M2M/MTC）终端设备、物联网（internet of things，IoT）终端设备或窄带物联网（narrow band internet of things，NB-IoT）终端设备、签约单元（subscriber unit）、签约站（subscriber station）、移动站（mobile station）、移动台（mobile）、远程站（remote station）、接入点（access point，AP）、远程终端设备（remote terminal）、接入终端设备（access terminal）、用户终端设备（user terminal）、用户代理（user agent）、或用户装备（user device）等。又例如，该终端设备具体可以实现为：移动电话（或称为“蜂窝”电话），或具有移动终端设备的计算机；IoT 中的专用终端设备、或工业控制(industrial control)设备、或远程医疗(remote medical)设备、或智能电网(smart grid)设备、或智慧城市(smart city)设备等；便携式、袖珍式、手持式、计算机内置的或者车载的移动装置等；个人通信业务（personal communication service，PCS）电话、无绳电话、会话发起协议（Session Initiation Protocol，SIP）话机、无线本地环路（Wireless Local Loop，WLL）站、个人数字助理（Personal Digital Assistant，PDA）等。在一种可选的设计中，该终端设备还可以实现为受限设备，例如功耗较低的设备，或存储能力有限的设备，或计算能力有限的设备等。在一种可选的设计中，该终端设备可以包括条码、射频识别（radio frequency identification，RFID）、传感器、全球定位系统（global positioning system，GPS）、激光扫描器等部件。

在一种可选的设计中，该终端设备还可以是可穿戴设备。可穿戴设备也可以称为穿戴式智能设备或智能穿戴式设备等，是应用穿戴式技术对日常穿戴进行智能化设计，以开发出可以穿戴的设备的总称，如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上，或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备，更可以通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能，例如：智能手表或智能眼镜等，以及只专注于某一类应用功能，需要和其它设备如智能手机配合使用，如各类进行体征监测的智能手环、智能头盔、智能首饰等。

在一种可选的设计中，该终端设备还可以是机器智能设备如无人驾驶(self-driving)设备、运输安全(transportation safety)设备、虚拟现实(virtual reality，VR)终端设备、增强现实(augmented reality，AR)终端设备等。

而如上介绍的各种终端设备，如果位于车辆上（例如放置在车辆内或安装在车辆内），都可以认为是车载终端设备，车载终端设备例如也可以称为车载单元（on-board unit，OBU）。

在一种可选的设计中，终端设备还可以包括中继（relay）。或者理解为，终端设备可

以包括能够与基站进行数据通信的任一设备。

示例地，该电子设备也可以为网络设备，例如包括接入网（access network，AN）设备，该接入网设备可以包括接入网中在空口通过一个或多个小区与无线终端设备通信的设备，比如基站或接入点。其中，基站可用于将收到的空中帧与互联网协议（Internet Protocol，IP）分组进行相互转换，作为终端设备与接入网的其余部分之间的路由器，其中接入网的其余部分可包括 IP 网络。在一种可选的设计中，网络设备可以包括第二代（2th generation，2G）通信系统中的基站，或者包括第三代（3th generation，3G）通信系统中的基站，或者包括第四代（4th generation，4G）通信系统中的基站，比如，长期演进（long term evolution，LTE）系统或高级长期演进（long term evolution-advanced，LTE-A）中的演进型基站（NodeB 或 eNB 或 e-NodeB，evolutional Node B），或者也可以包括第五代（the 5th generation，5G）新无线（new radio，NR）系统（也简称为 NR 系统）中的下一代节点 B（next generation node B，gNB），或者也可以包括云接入网（cloud radio access network，Cloud RAN）系统中的集中式单元（centralized unit，CU）和分布式单元（distributed unit，DU），以及未来的各种通信系统中的基站，例如第六代（6th generation，6G）通信系统中的基站，本申请实施例对此不做限定；又例如网络设备可以包括 V2X 中的网络设备即路侧单元（road side unit，RSU）。RSU 可以包括支持 V2X 应用的固定基础设施实体，可以与支持 V2X 应用的其他实体交换消息；再例如，网络设备还可以包括核心网设备，核心网设备例如包括 5G 系统中的如下一项或多项：接入和移动性管理功能（access and mobility management function，AMF）、会话管理功能（session management function，SMF）、用户面功能（user plane function，UPF），或者包括 4G 系统中的移动管理实体（mobility management entity，MME）等。

应理解，在某些技术场景中，具备相类似数据收发能力的电子设备的名称也可能不称为节点，但是为了方便描述，本申请实施例中将具有数据收发能力的电子设备统称为节点。

本申请实施例中，在图 1 所示的异构式通信系统中，该第一节点 110、第二节点 120、或第三节点 130 的设备类型可以相同或不同。例如，第一节点 110、第二节点 120、第二节点 130 均是终端设备或网络设备，或者，第一节点 110、第二节点 120 可以是终端设备、第三节点 130 可以是网络设备。以第一通信技术为短距离通信技术、第二通信技术为 5G 通信技术为例，如图 2 所示，该第一节点 110、第二节点 120 可以为具备短距通信功能的终端设备，第三节点 130 可以包括但不限于接入设备：可信的非第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）网关功能（Trusted Non-3GPP Gateway Function，TNGF）、以及核心网设备：SMF、AMF、UPF 以及数据网络（Data Network，DN）等功能实体中的至少一项。其中，该第一节点 110 可支持第一通信技术和第二通信技术，可以作为第二节点 120 的主控节点（或者称为授权节点），一方面与第二节点 120 进行短距离通信，另一方面与第三节点 130 进行 5G 通信。需要说明的是，第一节点 110 可支持第一通信技术，也可以理解为，第一节点可以支持基于第一通信技术实现的业务传输，或者第一节点可以支持第一通信技术的业务；第一节点 110 支持第二通信技术，也可以理解为，第二节点可以支持基于第二通信技术实现的业务传输，或者第二节点可以支持第二通信技术的业务。

各个节点或功能实体之间可以通过接口连接，接口的序列号或接口的名称本申请实施例中不作限定，可以按照 5G 系统的 3GPP 相关标准协议中定义的接口，也可以使用未来通信系统中的接口。例如，第二节点 120 可以通过 Yt 接口与第一节点 110 通信，第一节点

110 可以通过 Ta 接口与 TNGF 通信，第二节点 120 可以通过 NWt 接口与 TNGF 通信。第二节点 120、第一节点 110 可以通过下一代网络（next generation，N）1 接口（简称 N1）与 AMF 通信，网络设备（例如 TNGF）通过 N2 接口（简称 N2）与 AMF 通信，TNGF 通过 N3 接口（简称 N3）与本地 UPF 通信，UPF 通过 N6 接口（简称 N6）与 DN 通信。AMF 通过 N11 接口（简称 N11）与 SMF 通信，SMF 通过 N4 接口（简称 N4）与 UPF 通信。由此，使得 5G 网络能够透过该第一节点 110 来感知该第二节点 120 的设备状态、网络状态、业务状态等关键信息，达到远程对行业现场网络和业务的可达、可感、可管等。

需要说明的是，上述仅是示意性表示该异构式通信系统中可以包括第一节点 110、第二节点 120 和第三节点 130，以及各个节点及其功能模块之间的通信方式，并不限定各个节点的数量以及接口的序列号或名称。在具体实施时，第一节点 110、第二节点 120、第三节点 130 的数量可以不限于 1 个。

另外，需要说明的是，本申请实施例中，在一种可选的设计中，第一节点 110 可以和第三节点 130 进行无线资源控制（radio resource control，RRC）建立过程，当第一节点 110 和第三节点 130 建立了 RRC 连接后，该第一节点 110 的 RRC 状态即为 RRC 连接态。随后，第一节点 110 的 RRC 状态可以在以下状态中进行转换：RRC 空闲（RRC_IDLE）态、RRC 连接（RRC_CONNECTED）态和 RRC 非激活（RRC_INACTIVE）态，在本申请实施例的融合通信场景中，该第一节点 110 可以是处于上述的空闲态、连接态、非激活态中的任一状态，本申请实施例对此不做限定。并且，本申请实施例中，任意两个节点之间建立通信连接是指，该两个节点之间可以通过信号的传输交互，以在所述两个节点之间进行通信，包括但不限于物理连接或虚拟连接，下文中将不再逐一区分。

本申请实施例中，短距离通信技术可以包括支持无线短距通信的技术，无线短距通信包括通信双方通过无线电波传输信息并且传输距离在较短的范围内（例如百米以内），都可以称为短距离无线通信，包括但是不限于是蓝牙（bluetooth）技术、无线保真（wireless fidelity，Wi-Fi）技术、近场通讯（near field communication，NFC）技术、Wi-Fi Aware 技术、通用短距通信技术、星闪联盟规范的短距通信技术等。短距离通信可以在文件传输、远程控制、投屏、周围设备（例如智能汽车、智能终端设备、智能家居设备和智能制造设备等）的感知等各方面有大量应用。下面列举几种短距离通信技术的示例。

蓝牙：一种支持设备短距离通信的无线电技术，能在包括移动电话、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。利用“蓝牙”技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与因特网之间的通信，从而使得数据传输变得更加迅速高效，为无线通信拓宽道路。

无线保真技术（wireless fidelity，Wi-Fi）：又称为无线局域网（wireless local area networks，WLAN）直连或 Wi-Fi Direct，是 Wi-Fi 协议簇中的一个，使设备之间能够轻松连接彼此而不再需要中介性质的无线接入点。其使用范围从网页浏览到文件传输，以及同时与多个设备进行通信，能够充分发挥 Wi-Fi 的速度优势。符合此标准的设备即使来自不同的生产厂商，亦可实现轻松互联。

Wi-Fi Aware 技术：在 Wi-Fi 技术中负责感知和发现部分，能够帮助 Wi-Fi 设备感知周边的服务，比如，周边的设备，进而通过 Wi-Fi Aware 实现近距离的两个设备的点对点（Peer to Peer，P2P）消息交互。由于 WIFI-Aware 可以感知周围的设备，所以可实现多种功能，比如，感知的附近的人并建立连接，进而加好友、玩同一款游戏等等；或者，发现周围的

设备，实现照片分享或地点分享等等；或者，无需接入网络（比如蜂窝或无线），就可以向打印机安全地发送文件，等等。

需要说明的是，除了上面列举的短距离通信技术之外，现有的其它短距离通信技术，或者，随着通信技术的演进，未来可能出现的其他的短距离通信技术，也可以适用于本方案。

此外，需要说明的是，图 2 中各个功能实体或网元也可以采用服务化接口进行交互。比如，AMF 对外提供的服务化接口可以为网络接入和移动性管理功能（network access and mobility management function，Namf）接口；SMF 对外提供的服务化接口可以为网络会话管理功能（network session management function，Nsmf）接口。相关描述可以参考第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）-23501 标准中定义的 5G 系统架构（5G system architecture），在此不予赘述。

系统架构中包括的各个功能也可以称为功能实体、网元或其他名称。例如，SMF 可以称为 SMF 实体。在一种可选的设计中，本申请实施例中的各个功能可以由一个设备实现，也可以由多个设备共同实现，还可以是由一个设备内的一个或多个功能模块实现，本申请实施例对此不作具体限定。可以理解的是，本申请实施例涉及的各个功能既可以是硬件设备中的网络元件的功能，也可以是在专用硬件上运行的软件功能，或者是硬件与软件的结合，或者是平台(例如，云平台)上实例化的虚拟化功能。

需要说明的是，本申请实施例并不限定各个功能的分布形式，在一种可选的设计中，上述系统架构中包括的各个功能还可以对应上述任意多种功能之间、或与其他功能之间融合后形成的其他功能实体，例如，具有会话管理和策略控制两种功能的功能实体，或者具有会话管理、接入与移动性管理和策略控制三种功能的功能实体，或者具有网络开放和应用功能两种功能的功能实体。

需要说明的是，图 1~图 2 所示的系统架构并不构成本申请实施例能够适用的系统架构的限定。图 2 中的终端设备的数量只是举例，在实际应用中，网络设备可以为多个终端设备提供服务，网络设备，以及多个终端设备中的全部终端设备或者部分终端设备，都可以采用本申请实施例提供的通信方法。本申请实施例中涉及的各个功能或设备也可以称之为通信装置，其可以是一个通用设备或者是一个专用设备，本申请实施例对此不作具体限定。

需要说明的是，本申请实施例中“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 的情况，其中 A，B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a,b,或 c 中的至少一项（个），可以表示：a,b,c,a 和 b,a 和 c,b 和 c,或 a 和 b 和 c，其中 a,b,c 可以是单个，也可以是多个。

以及，除非有特别说明，本申请实施例提及“第一”、“第二”、“第三”等序数词是用于对多个对象进行区分，不用于限定多个对象的优先级或者重要程度。例如，第一节点、第二节点、第三节点，只是为了区分不同的节点，而不是表示这三个节点的优先级或者重要程度等的不同。

此外，需要说明的是，在本申请各个实施例中，第一通信技术的业务，可以理解为，通过第一通信技术实现的业务（例如通过非 5G 技术实现的业务，进一步地比如通过短距

离通信技术实现的业务），或者第一通信技术对应的业务（例如非 5G 业务，进一步地比如短距离通信业务）。第二通信技术的业务可以包括融合通信场景下的第二通信技术的业务，其中，第二通信技术的业务，可以理解为，通过第二通信技术实现的业务（例如通过 5G 实现的业务），或者第二通信技术对应的业务（例如 5G 业务）。在本申请各个实施例中，第一通信连接对应第一通信技术，可以理解为，第一通信连接是基于第一通信技术实现的连接。例如当第一通信技术为短距离通信技术时，第一通信连接是通过使用短距离通信技术实现的连接。进一步可选地，通过该通信连接，可以传输第一通信技术的业务，或者可以传输第二通信技术的业务。下文中将不再对此逐一进行说明。在本申请各个实施例中，对应第二通信技术的网络，可以理解为，至少支持第二通信技术的网络，或者至少支持基于第二通信技术实现的业务传输的网络，例如 5G 网络，或者 5G 核心网。

基于图 1 和图 2 所示的系统架构，在本申请实施例的融合通信场景中，在一种可选的设计中，对于第一节点 110 和第二节点 120 组成的第一通信系统，为保障第一通信系统的通信安全性，第二节点 120 可以在选择好可信的第一节点 110 后、在与该第一节点 110 进行初始建链时，采用一个预置密钥与该第一节点 110 相互进行身份认证，并在身份认证成功后，基于该密钥相应的安全上下文建立双方之间的通信连接。进一步地，为保障第一节点 110、第二节点 120 与第三节点 130 组成的异构式通信系统的通信安全性，第二节点 120 还可以通过第一节点 110 发起到第三节点 130 的新的身份认证和/或安全上下文协商流程，以协商确定三者之间的新的密钥和相应的安全上下文。

在第一节点 110 和第二节点 120 中存在至少两套密钥和/或相应的安全上下文的情况下，第一节点 110 和第二节点 120 之间还可以从所述至少两套密钥和/或相应的安全上下文中选择所需的密钥或安全上下文，以便基于所选择的密钥或安全上下文，来与对端节点建立安全的通信连接，从而保障双方之间执行相应的通信业务和/或传输通信业务数据的安全需求。

需要说明的是，本申请实施例中，密钥是一种参数，可以是在将明文转换为密文的算法中或将密文转换为明文的算法中输入的参数，第一节点 110、第二节点 120、第三节点 130 中的任意两方之间可以基于密钥发起身份认证流程和/或安全上下文（Security Context）协商流程，在双方之间身份认证成功后，双方之间能够获得协商一致的安全上下文，即访问控制属性。基于该安全上下文，双方之间可以发起连接建立流程，以在双方之间建立安全的通信连接。应理解，若第一节点 110、第二节点 120、第三节点 130 中的任意两方之间已经存在协商一致的安全上下文，双方之间无需进行上述身份认证流程和/或安全上下文协商流程，可直接使用协商一致的安全上下文发起连接建立流程，以在双方之间建立安全的通信连接。

应理解，本申请实施例中，第一节点 110、第二节点 120 或第三节点 130 均可以支持一种或多种密钥协商算法，第一节点 110、第二节点 120、第三节点 130 中的任意两方之间在发起上述身份认证流程和/或安全上下文协商流程之前，还可以通过信息交互，完成双方之间的密钥协商。示例地，该密钥协商算法可以包括但不限于：非对称加密算法：如公钥加密（Rivest-Shamir-Adleman，RSA）算法、椭圆曲线加密（Elliptic Curves Cryptography，ECC）算法等；专用密钥交互算法：如迪菲-赫尔曼密钥协商（Diffie-Hellman algorithm，DH）算法、椭圆曲线迪菲-赫尔曼秘钥交换（Elliptic Curve Diffie－Hellman key Exchange，ECDH）等；共享密钥算法：预共享密钥（Pre-shared key，PSK）算法等，本申请实施例对此不做限定。为了便于描述，下文中将以采用 PSK 算法为例，来对本申请实施例的通信

方法的具体实现过程进行介绍，在此暂不赘述。

其中，身份认证又称为“身份验证”、“身份鉴权”，是指通过一定的手段，完成对节点身份的确认。身份认证的方法有很多实现方式，例如，基于 PSK 的身份认证方法、基于生物学特征的身份认证方法和基于公开密钥加密算法的身份认证方法等。其中，基于预共享密钥的身份认证是指至少两个节点可共同拥有一个或一组密钥，例如第一节点 110 和第二节点 120 之间、或第一节点 110 与第三节点 130 之间、或第一节点 110、第二节点 120 与第三节点 130 之间。在需要进行身份认证时，第一节点 110 或第二节点 120 或第三节点 130 可向对端节点发送该 PSK（或与该 PSK 关联的相关参数，本申请实施例对该相关参数的具体实现方式不做限定），对端节点接收到该 PSK 后，检查该 PSK 是否与本地保存的密钥一致，如果一致，则可判定身份认证成功，如果不一致则可判定身份认证失败。任意两方节点之间在相互进行身份认证成功的情况下，方可获得协商一致的安全上下文，并基于该安全上下文，在双方之间建立安全的通信连接，以保障双方之间执行相应的通信业务和/或传输通信业务数据的安全需求。

在具体实施过程中，一种可能的实现方式是，第一节点 110 和第二节点 120 可以选择关联于第一业务的第一信息（例如包括第一密钥和/或第一安全上下文），并基于该第一信息进行信息交互，以在第一节点 110 和第二节点 120 之间建立第一通信连接，该第一通信连接可用于传输第一业务的数据，以在满足融合通信场景下的安全需求的同时，实现第三节点 130 透过该第一节点 110 感知第二节点 120 的相关信息，从而达到远程对第二节点 120 的网络和业务的可达、可感、可管等。在实施时，在不同的场景中，该通信方法的流程可由第一节点 110 或第二节点 120 触发，本申请实施例对此不做限定。

为便于理解，下面结合附图及实施例介绍该通信方法。其中，需要说明的是，本申请述及的各个方法实施例中所包括的步骤仅是对该通信方法的可选步骤的示例，并不限定该通信方法的具体实现过程，在一些可选的实现方式中，任一个方法实施例中的步骤还可以交换实施顺序。

如图 3 所示，在一个示例中，该方法流程可由第一节点 110 触发，可以包括以下步骤：

S310：第一节点 110 获取第一信息。

S320：第一节点 110 根据所述第一信息与第二节点 120 建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点 110 为接入对应第二通信技术的网络的节点。

可以理解的是，该第一信息与所述第一业务相关联。示例地，所述第一业务可以为所述第一通信技术的业务或者所述第二通信技术的业务。

应理解，本申请实施例中，第一节点和第二节点是为了区分不同节点而加以描述，在一些示例中，第一节点可以为第二节点，第二节点可以为第一节点，图 3 中示出的方法流程，可以是第二节点 120 触发的，即第二节点 120 可以获取第一信息，根据所述第一信息与第一节点 110 建立第一通信连接，本申请实施例对此不做限定。

其中，上述第一信息可以包括第一节点 110 和第二节点 120 之间建立安全的通信连接所需的相关信息，该第一信息可以预先存储在该第一节点 110 或第二节点 120 侧，或者，也可由该第一节点 110 或第二节点 120 从网络侧或其它设备侧获取的，本申请实施例对此不做限定。

本申请实施例中，该第一节点 110 和第二节点 120 可以处于无安全上下文场景，该第

一信息可以包括用于第一节点 110 与第二节点 120 通信认证的第一密钥，实施 S320 时，第一节点 110 可以根据该第一密钥与第二节点 120 进行身份认证和安全上下文协商流程，进而，基于协商获得的第一安全上下文，第一节点 110 与第二节点 120 之间可以建立所述第一通信连接。或者，该第一节点 110 和第二节点 120 可以处于有安全上下文场景，该第一信息可以包括用于第一节点 110 与第二节点 120 通信的第一安全上下文，实施 S320 时，第一节点 110 与第二节点 120 之间可以根据该第一安全上下文建立所述第一通信连接。

在一个可能的设计中，在所述第一信息为用于第一节点 110 与第二节点 120 通信认证的密钥的情况下，该密钥可以包括所述第一节点 110 或所述第二节点 120 侧的预置密钥，或者该密钥可以来自第二通信技术的网络（例如第三节点 130 侧的核心网），例如用于所述第二通信技术的业务的密钥。

本申请实施例中，在不同的情形下，S310-S320 的具体实现过程有所不同，为了便于理解，下面结合方法流程图进行介绍。

情形一：第一信息包括用于第一节点 110 与第二节点 120 通信认证的第一密钥。

在该情形中，第一节点 110 和第二节点 120 无关联于第一业务的第一安全上下文，第一节点 110 和第二节点 120 之间建立所述第一通信连接时，可以首先获取所述第一密钥，之后基于所获取的第一密钥，先相互进行身份认证和协商第一安全上下文。在双方之间身份认证成功并获得所述第一安全上下文的情况下，该第一节点 110 可以基于所获得的第一安全上下文向第二节点 120 发起用于建立通信连接的消息，以基于该第一安全上下文在该第一节点 110 和该第二节点 120 之间建立第一通信连接。

方法示例一：

在方法示例一中，可由第二节点 120 获取第一密钥，第二节点 120 获取第一密钥后，可向第一节点 110 上报密钥类型指示信息或业务类型指示信息，由第一节点 110 根据第二节点 120 上报的密钥类型指示信息或业务类型指示信息确定所述第一密钥，并与第二节点 120 进行身份认证和安全上下文协商流程，从而在第一节点 110 和第二节点 120 之间建立安全的第一通信连接。需要说明的是，方法示例一中所包括的步骤 S411-S419 仅为可选步骤的示例，在一些示例中，下述步骤还可以交换实施顺序，本申请实施例不做具体限定。如图 4a 所示，该通信方法例如可以包括以下步骤：

S411（可选）：第一节点 110 发送第六消息（例如系统消息）。相应地，第二节点 120 可以接收该第六消息。

示例地，该第六消息中可以携带（或者说承载）第一指示信息，该第一指示信息可以用于指示所述第一节点 110 支持的业务类型（包括支持对应于第二通信技术的业务）。

在一种可选的设计中，该第一指示信息还可以指示第一节点 110 支持的一种或多种密钥协商算法，以便第二节点 120 可以根据所述第一指示信息，从自身所支持的密钥协商算法中选择第一节点 110 同样支持的密钥协商算法，以完成双方之间的密钥协商，以便根据协商确定的密钥协商算法（例如前述的 PSK 算法），生成用于节点身份认证的相关认证参数。应理解，第一节点 110 和第二节点 120 节点之间进行密钥协商可以不限于是通过该第六消息实现的，本申请实施例对此不做限定。为便于理解和说明，本文中以 PSK 算法为例进行介绍。

进一步地，该第六消息中还可以携带所述第一节点 110 的身份标识（例如域标识（Domain ID）），该身份标识可用于唯一标识所述第一节点 110。

示例地，该第六消息可以是单播消息，S411 中，第一节点 110 可以向该第二节点 120 发送该第六消息。或者，该第六消息可以是广播消息，S411 中，第一节点 110 可以广播该第六消息，第二节点 120 可以处于广播信号覆盖的范围内，且可以接收到该第六消息。

第二节点 120 接收到所述第六消息后，通过解析该第六消息，可以获知第一节点 110 支持的业务类型。

S412：该第二节点 120（例如第二节点 120 的服务层）根据对应所述第二通信技术的类型，和/或，根据第一业务的业务类型，获取第一密钥或第一密钥的类型。

示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。

应理解，实施 S412 时，该第二节点 120 还可以是根据用户输入的相关指示信息获取所述第一密钥或第一密钥的类型，或者根据来自其它设备的相关指示信息获取所述第一密钥或第一密钥的类型，本申请实施例对此不做限定。

应理解，本申请实施例中，对于第二节点 120 获取第一密钥或第一密钥的类型还可以通过其他方式，本申请实施例对此不做限定。

本申请实施例中，在基于第一通信技术和第二通信技术的融合通信场景下，该第一密钥可以包括以下任一种实现方式：

示例 1：第一密钥为用于第一通信技术的业务的密钥。

该第一密钥可以是在第一节点 110 和第二节点 120 之间配置的密钥（例如对应前文中述及的预置密钥），该密钥对应于第一通信技术的业务，可用于在第一节点 110 和第二节点 120 之间完成身份认证和安全上下文协商后建立第一通信连接，并基于所建立的第一通信连接执行第一通信技术的业务，或者对基于第一通信技术的业务数据进行安全传输。相应地，该密钥对应的安全上下文为第一通信技术的业务的安全上下文。本申请实施例中，为便于区分，该用于第一通信技术的业务的密钥也可称为普通密钥，与普通密钥对应的安全上下文也可称为普通安全上下文。

其中，以该普通密钥为普通 PSK 为例，该普通 PSK 的配置方法可以包括以下方法中的任一种：

①配置密钥方法：通过预配置的方法，将该普通 PSK 预配置在第一节点 110 侧和第二节点 120 侧。预配置方法的详细实现在此不再赘述。

②配置口令方法：用户在第一节点 110 和第二节点 120 上输入相同的口令。该口令可以转换为该普通 PSK，例如可以通过节点内的算法实现（比如密钥协商算法实现）转换为普通 PSK。应理解，不同的第二节点 120 可以使用不同口令接入同一个第一节点 110，在此不再赘述。

③第三方服务器认证凭证配置方法：第三方服务器认证凭证配置方法的主要目的是识别第二节点 120 是否和第一节点 110 满足预设的绑定关系。第二节点 120 应可以获取第一节点 110 的身份标识，并利用第二节点 120 的身份标识和第一节点 110 的身份标识生成校验信息发送给第三方服务器，以获取认证口令。第一节点 110 和第二节点获取到第三方服务器发送的认证口令后，基于认证口令获得该普通 PSK。

通过以上任一种配置方法，第二节点 120 和第一节点 110 之间可以配置相同的普通 PSK。应理解，本申请实施例中，第二节点 120 和第一节点 110 之间也可以通过其他方法完成两节点之间的用于第一通信技术的业务的 PSK 的配置过程，在此不再赘述。

示例 2：第一密钥为用于第二通信技术的业务的密钥。

为便于区分，用于所述第二通信技术的密钥可称为融合密钥。其中，在具体实现时，该融合密钥可以包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥（例如前文中述及的在融合通信场景下，第二节点 120 通过第一节点 110 发起到第三节点 130 的新的身份认证和/或安全上下文协商流程确定的三者之间的新的密钥），所述非可信密钥为未经过所述网络鉴权的密钥（例如前述所述及的第二节点与第一节点进行初始建链时采用的预置密钥，该预置密钥可以用于第一节点和第二节点相互进行身份认证）。这里的网络可以理解为第三节点所对应的网络，例如可以为 5G 核心网。应理解，在本申请实施例中，未经过所述网络鉴权的密钥，可以理解为：没有经过网络或者无需经过网络确认的密钥（例如默认的密钥），或者虽然经过网络确认但是没有确认成功的密钥。第一密钥相应地可以为可信密钥或非可信密钥，该第一密钥对应于第二通信技术的业务，可用于在融合通信场景下，保障在第一节点 110、第二节点 120 以及第三节点 130 之间安全地实现第二通信技术的业务或安全地传输通过第二通信技术实现的业务数据。该第一密钥例如可以是第三节点 130，和第一节点 110 与第二节点 120 中的至少一个节点协商的密钥（例如对应前文中述及的新的密钥，或者对应可信密钥），比如该第一密钥可以是第三节点 130 和第一节点 110 协商的密钥，又比如该第一密钥可以是第三节点 130 和第二节点 120 协商的密钥，再比如，该第一密钥可以是第一节点 110、第二节点 120 和第三节点 130 之间协商的密钥；又例如，第一密钥可以是非可信密钥。

以该融合密钥为融合 PSK 为例，该融合 PSK 可以是第三节点 130 侧的核心网下发至第一节点 110 和/或第二节点 120 的，或者，该 PSK 也可以是在第一节点 110 或第二节点 120 配置的默认密钥参数，配置实现可以是示例 1 中的三种方式之一或其它实现方式，本申请实施例对此不做限定。第一节点或第二节点可以接收来自对应第二通信技术的网络的融合密钥。例如，第一节点和第二节点之间在建立第一通信连接之前，第一节点或第二节点可以接收来自网络的融合密钥，并将其保存在本地，以便于在后续第一通信连接建立过程中，第一节点或第二节点可以根据对应第二通信技术的类型，和/或根据第一业务的业务类型，确定在第一通信连接建立过程中所使用的第一密钥。第一节点在建立第一通信连接之前接收来自对应第二通信技术的网络的融合密钥，还便于第一节点在第一通信连接建立过程中，根据接收到的第一信息，获取第一密钥。

其中，若该 PSK 未经过第三节点 130 侧的核心网（例如 5G 核心网）的鉴权和密钥协商过程或未协商达成一致，该融合 PSK 为非可信融合 PSK。若该融合 PSK 经过第三节点 130 侧的核心网的鉴权和/或密钥协商过程且达成一致，该融合 PSK 为可信融合 PSK。相应地，与可信融合 PSK 对应的安全上下文，为在融合通信场景下，用于第二通信技术的业务的可信安全上下文，与非可信融合 PSK 对应的安全上下文，为在融合通信场景下，用于第二通信技术的业务的非可信安全上下文。应理解，在本申请实施例中，对应第二通信技术的网络，可以理解为，至少支持第二通信技术的网络，或者至少支持基于第二通信技术实现的业务传输的网络。

实施例 S412 时，该第二节点 120 根据对应所述第二通信技术的类型，和/或，根据第一业务的业务类型等，在上述示例 1 或示例 2 中述及的至少两个密钥中选择一个密钥作为该第一密钥。

需要说明的是，本申请实施例中，在存在多个密钥的情况下，该多个密钥可以具有优

先级和使用原则，其中，第一密钥与第一业务相关联，在所述多个密钥中选择第一密钥至少需要遵循以下原则：在所述第一业务为第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；和/或，在所述第一业务为对应于所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

以上述的普通 PSK、可信融合 PSK 和非可信融合 PSK 为例，该多个密钥的使用原则具体可以是：1）在融合通信场景下，针对第二通信技术的业务，存在可信融合 PSK，则不使用非可信融合 PSK，而是使用可信融合 PSK，即可信融合 PSK 的优先级高于非可信融合 PSK 的优先级；2）在融合通信场景下，针对第二通信技术的业务，当不存在可信融合 PSK 时，使用非可信融合 PSK，而不使用普通 PSK；3）针对第一通信技术的业务，即使存在融合 PSK，也要使用普通 PSK，以确保第一节点 110 和第二节点 120 之间的私有业务的安全性。

基于上述密钥使用原则，第二节点 120 可以根据第一业务的业务类型获取相应的第一密钥或第一密钥的类型。比如，如果第一业务为融合通信场景下第二通信技术的业务，那么存在可信融合 PSK 则使用可信融合 PSK（进一步地，如果基于可信融合 PSK 建立连接失败，则再使用非可信融合 PSK），没有可信融合 PSK 时则使用非可信融合 PSK。一般地，非可信融合 PSK 可以为默认值，示例地，当第一节点 110 和第二节点 120 为支持第二通信技术的设备时，该第一节点 110 和第二节点 120 中可以配置有该非可信融合 PSK。又比如，如果第一业务为第一通信技术的业务，那么第一节点 110 和第二节点 120 可以通过普通 PSK 来建立第一通信连接。

S413a：第二节点 120（例如第二节点 120 的服务层）向第一节点 110 发送第一消息。相应地，第一节点 110 可以接收来自所述第二节点 120 的第一消息。

本申请实施例中，该第一消息也可称为密钥指示消息，该第一消息可以承载与所述第一密钥关联的信息，例如密钥类型指示信息或业务类型指示信息或其他信息。

在本申请实施例中，该密钥类型指示信息可用于指示密钥类型为以下任一种：非可信融合密钥（例如前述的非可信融合 PSK）、可信融合密钥（例如前述的可信融合 PSK）、或者普通密钥（例如前述的普通 PSK）。该业务类型指示信息可用于指示业务类型为以下任一种：第一通信技术的业务，或者，融合通信场景下，第二通信技术的业务。

在一些设计中，该第一消息中还可以携带该第二节点 120 的身份标识（例如媒体接入层标识），示例地，该第一消息可以表示为如下多元组：

(ID, 密钥类型指示信息或业务类型指示信息)。

S414：第一节点 110 根据所述密钥类型指示信息或所述业务类型指示信息，获取所述第一密钥。

本申请实施例中，第一节点 110 可以存储有多个密钥，实施 S414 时，第一节点 110 可以根据所述密钥类型指示信息或所述业务类型指示信息，从本地的多个密钥中获取所述第一密钥。或者，实施 S414 时，第一节点 110 可以根据所述密钥类型指示信息或所述业务类型指示信息，从其它设备获取该第一密钥，本申请实施例对此不做限定。示例地，该第一密钥可以为如前所述的普通 PSK、非可信融合 PSK 或可信融合 PSK 中的任一个，该普通 PSK、非可信融合 PSK 或可信融合 PSK 的配置过程可以参考 S412 中的相关描述，不做具体赘述。

由此，第一节点 110 和第二节点 120 之间可以通过协商，对所选择的第一密钥达成一

致，进一步地，第一节点 110 和第二节点 120 之间即可基于所获得的第一密钥进行身份认证和安全上下文协商流程。

示例地，如图 4a 所示，该身份认证和安全上下文协商流程可以包括以下步骤：

S415a（可选）：第二节点 120 向第一节点 110 发送关联请求消息。相应地，第一节点 110 接收该关联请求消息。

示例地，该关联请求消息中可以承载所述第二节点 120 的身份标识（例如域标识）、以及用于第二节点 120 的身份认证的相关认证参数，包括但不限于第二节点 120 选择的密钥协商算法（例如用 KE alg 表示）、密钥协商参数（例如用 KEt 表示）、第二节点 120 的安全能力（sec capabilities）和随机数（例如用 NONCEt 表示）等。安全能力可以包括第二节点 120 支持的密钥派生函数（key derivation function，KDF）、加密算法、完整性保护算法和认证加密算法中的一项或多项，在此不再赘述。

第一节点 110 可基于该关联请求消息中携带的相关信息，处理该关联请求消息。

比如，对于使用配置密钥方式接入的第二节点 120，若第一节点 110 配置了白名单，第一节点 110 可以根据第二节点 120 的身份标识，判断第二节点 120 的固定身份是否在该白名单中，如果不在，则丢弃该关联请求消息。

又比如，第一节点 110 可以判断第二节点 120 选择的密钥协商算法是否在前述的第六消息承载的信息（例如第一指示信息）中，如果不在则丢弃该关联请求消息；如果在，第一节点 110 可根据第二节点 120 的安全能力、第一节点 110 预配置的算法优选策略和业务类型选择优先级最高的算法，包括优先级最高的密钥派生函数以及信令面的认证加密算法和完整性保护算法，以及优先级最高的用户面的认证加密算法和完整性保护算法，或者，优先级最高的用户面的认证加密算法。其中，算法优选策略可以通过按照优先级排序的算法列表来实现，如第一节点 110 预配置的密钥派生函数优先级列表、信令面认证加密算法优先级列表、信令面完整性保护算法优先级列表、用户面认证加密算法优先级列表、用户面完整性保护算法优先级列表等。信令面和用户面选择的算法可以不同。在一种可选的设计中，当选择的完整性算法或认证加密算法支持多个消息完整性代码（Message Integrity Code, MIC）长度时，第一节点 110 还可以根据选择的信令面完整性保护算法支持的 MIC 长度，选择信令面完整性保护的 MIC 长度，该过程例如可以通过星闪联盟规范的相应操作实现，或者也可以通过其他方式，本申请实施例不做具体限定。

在一种可选的设计中，该第一节点 110 还可根据所述第一消息中携带的相关信息和/或第一节点 110 自身选择的相关算法生成用于第一节点 110 的身份认证的相关认证参数。

示例地，第一节点 110 可产生私钥，并根据所选择的密钥协商算法（具体的密钥协商算法例如可以参照 S411 中的相关描述），生成相应的公钥，该公钥可作为第一节点 110 的密钥协商参数（例如用 KEg 表示）。或者，第一节点 110 可生成随机数（例如用 NONCEg 表示）。或者，第一节点 110 可根据第一消息中携带的 KEt 和密钥协商算法，计算出共享密钥（例如用 K_{KE} 表示）。或者，第一节点 110 可根据 K_{KE}、NONCEt 和 NONCEg，使用选择的密钥派生函数计算出共享密钥（例如用 Kgt 表示），计算方式如下：

$$Kgt=KDF(K_{KE}, NONCEt, NONCEg)。$$

或者，第一节点 110 可生成 Kgt 的标识（例如用 Kgt ID 表示）。或者，第一节点 110 可计算认证参数（例如用 AUTHg 表示），计算方式如下：

$$AUTHg = AUF(PSK，K_{KE}，NONCEg，关联请求消息)|_{高 32 位比特}。$$

其中，AUF()|高32位比特，表示通过密钥派生函数 AUF 对括号内包括的参数进行运算，然后取高 32 位比特信息作为 AUTHg。AUF 与前述的 KDF 使用相同的认证加密算法。

第一节点 110 可以基于所获取的第一密钥、上述相关认证参数中的一种或多项，生成安全上下文请求消息（第二消息的一个示例）。

示例地，该安全上下文请求消息中可以包括用于第一节点 110 的身份认证的相关认证参数，包括但不限于第一节点 110 的密钥协商参数 KEg、随机数 NONCEg、第一密钥对应的第一安全上下文关联的标识 Kgt ID、选择的算法（algorithm）、MIC 长度（MIC length）和认证参数 AUTHg。选择的算法（algorithm）可以包括密钥派生算法、信令面的加密算法和完整性保护算法、用户面的加密算法和完整性保护算法、用户面的认证加密算法中的一项或多项。

在一种可选的设计中，第一节点 110 还可以使用选择的信令面的完整性保护算法和完整性保护密钥 Ks.int 对安全上下文请求消息做完整性保护，即计算 MIC，并将 MIC 包含在安全上下文请求消息中。

示例地，该安全上下文请求消息可以表示为如下多元组:

$$(KEg, NONCEg, Kgt\ ID, algorithm, MIC\ length, AUTHg)_{MIC}。$$

其中，该（）$_{MIC}$ 表示该安全上下文请求消息为经过完整性保护处理的消息。

S416: 第一节点 110 向所述第二节点发送与所述第一密钥关联的安全上下文请求消息（第二消息的一个示例）。相应地，第二节点 120 接收来自所述第一节点 110 的安全上下文请求消息。

本申请实施例中，该第二消息可用于第一节点 110 的身份认证。应理解，在本申请实施例中，该第二消息可用于第一节点 110 的身份认证，可以理解为，该第二消息包含的或者携带的信息可用于第一节点 110 的身份认证。

本申请实施例中，第二消息与第一密钥相关联，在一种可选的设计中，第二消息承载的信息中包括根据第一密钥生成的信息。

在一种可选的设计中，第二节点 120 可根据第一节点 110 选择的密钥派生函数，使用和第一节点 110 相同的方式计算出共享密钥 Kgt、信令面的安全密钥，用户面的安全密钥等。

在一种可选的设计中，第二节点 120 可检查第二消息的完整性，即校验 MIC 是否正确。如果完整性验证不通过，第二节点 120 丢弃该消息，并可重新发送关联请求消息。

在一种可选的设计中，第二节点 120 还可基于协商一致的第一密钥，验证 AUTHg 是否正确。如果 AUTHg 验证不通过，第二节点 120 丢弃该第二消息，并可重新发送关联请求消息。应理解，在本申请实施例中，检查消息的完整性，可以包括检查消息包括或者承载的信息的完整性。

进一步地，该第二节点 120 还可根据安全上下文请求消息中携带的相关信息和/或自身的相关算法生成用于第二节点 120 的身份认证的相关认证参数。

示例地，第二节点 120 可计算认证参数 AUTHt，计算方法符合以下表达式:

AUTHt = AUF (PSK，K_{KE}，安全上下文请求消息, NONCEt，第一节点 110 的密钥协商算法能力，第一指示信息)|高32位比特;

其中，AUF()|高32位比特，表示通过密钥派生函数 AUF 对括号内包括的参数进行运算，然后取高 32 位比特信息作为 AUTHt。AUF 和前述的 KDF 使用相同的认证加密算法。

在一种可选的设计中，第二节点 120 可以在对第一节点 110 的身份认证成功后，基于上述生成的相关认证参数生成安全上下文响应消息（第三消息的一个示例）。

S417: 第二节点 120 向第一节点 110 发送安全上下文响应消息(第三消息的一个示例)。相应地，第一节点 110 接收来自所述第二节点 120 的安全上下文响应消息。

本申请实施例中，该第三消息可用于所述第二节点的身份认证、且该第三消息可以是在所述第一节点 110 的身份认证成功的情况下发送的。

应理解，在本申请实施例中，第三消息可用于指示所述第一节点 110 的身份认证成功、以及用于所述第二节点 120 的身份认证，第三消息包含或者携带用于指示所述第一节点身份认证成功的信息和用于所述第二节点的身份认证的信息。此外，作为一种可选的设计，在本申请实施例中，用于指示所述第一节点 110 身份认证成功的信息和用于所述第二节点 120 的身份认证的信息，可以通过相同的消息发送，或者通过不同的消息发送，相应地，第三消息可以对应一个消息，也可以对应多个消息，本申请实施例对此不做限定。示例地，该第三消息中可以包含 AUTHt。

示例地，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对安全上下文响应消息做完整性保护。

应理解，在本申请实施例中，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对安全上下文响应消息做完整性保护，可以理解为，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对安全上下文响应消息包含的或携带的信息做完整性保护。完整性保护生成的 MIC 可以携带在安全上下文响应消息中。当信令面加密保护启动时，第二节点 120 可以使用信令面的加密算法和加密密钥 Ks.enc 对安全上下文响应消息做加密保护。

示例地，该安全上下文响应消息可以表示如下:

$$(\mathrm{AUTHt})_{\mathrm{MIC}}。$$

其中，AUTHt 为该安全上下文响应消息中携带的相关认证参数的示例，$()_{\mathrm{MIC}}$ 表示该安全上下文响应消息为经过完整性保护处理的消息。

此外，如果第二节点 120 对安全上下文响应消息进行了加密（或者，对安全上下文响应消息中包含的或携带的信息进行了加密），则第一节点 110 接收到该安全上下文响应消息后，可解密该安全上下文响应消息（或者，解密该安全上下文响应消息中包含的或携带的信息）。

第一节点 110 可以检查该安全上下文响应消息的完整性（或检查安全上下文响应消息包含的或携带的消息的完整性），并验证该安全上下文响应消息中携带的 AUTHt 是否正确。如果完整性或 AUTHt 验证不通过，即第二节点 120 的身份认证不成功，第一节点 110 可向第二节点 120 发送关联建立失败消息。如果完整性和 AUTHt 验证通过，第一节点 110 可为第二节点 120 生成用于标识该第二节点 120 的身份的临时 ID（例如为物理层标识）。

第一节点 110 可以根据所述安全上下文响应消息中携带的相关信息，对第二节点 120 进行身份认证，该过程例如可以通过星闪联盟规范的相应操作实现，或者也可以通过其他方式实现，本申请实施例不做具体限定。

S418: 第一节点 110 可在所述第二节点 120 的身份认证成功的情况下，向所述第二节点发送关联建立消息（第四消息的一个示例）。相应地，第二节点 120 接收来自第一节点 110 的关联建立消息。

本申请实施例中，该第四消息可用于与所述第二节点建立所述第一通信连接，所述第四请求消息可以是在所述第二节点 120 的身份认证成功的情况下发送的。

应理解，在本申请实施例中，第四消息可用于指示所述第二节点的身份认证成功、以及用于请求与所述第二节点建立第一通信连接，第三消息包含或者携带用于指示所述第二节点的身份认证成功的信息和用于请求与所述第二节点建立第一通信连接的信息。此外，作为一种可选的设计，在本申请实施例中，用于指示所述第二节点的身份认证成功的信息和用于请求与所述第二节点建立第一通信连接的信息，可以通过相同的消息发送，或者通过不同的消息发送，相应地，第四消息可以对应一个消息，也可以对应多个消息，本申请实施例对此不做限定。

示例地，该第四消息中可以包括第一节点 110 为第二节点 120 生成的以下一项或多项参数：临时 ID（T-ID）（例如为物理层标识）、共享密钥 Kgt 的有效期（Kgt expiration）、[GKc/GK]，[GK ID]，[Galgorithm]，[GK 的有效期（GK expiration）]。

其中，[GKc/GK]表示当单播信令面的加密保护开启时携带第二节点 120 所在组的组密钥（例如用 GK 表示），当单播信令面的加密保护未开启时携带 GKc，GKc 由 GK 和保护组密钥 GK 机密性的密钥（例如用 Kg 表示）进行异或处理得到：

$$Kg=KDF(Kgt, COUNTERg, "group key");$$

$$GKc=GK \oplus Kg。$$

其中，[GK ID]为 GK 的标识，Galgorithm 为第二节点 120 所在组的组算法。

在一种可选的设计中，第一节点 110 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联建立消息做完整性保护。

应理解，在本申请实施例中，第一节点 110 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联建立消息做完整性保护，可以理解为，第一节点 110 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联建立消息包含的或者携带的信息做完整性保护。完整性保护生成的 MIC 可携带在关联建立消息中。当信令面加密保护启动时，第一节点 110 可使用信令面的加密算法和加密密钥 Ks.enc 对关联建立消息做加密保护。

应理解，在本申请实施例中，第一节点 110 可使用信令面的加密算法和加密密钥 Ks.enc 对关联建立消息做加密保护，可以理解为，第一节点 110 可使用信令面的加密算法和加密密钥 Ks.enc 对关联建立消息包含的信息或携带的信息做加密保护。

示例地，该关联建立消息可以表示为如下多元组：

(临时 ID, Kgt expiration, [GKc/GK], [GK ID], [Galgorithm], [GK expiration])$_{MIC}$。

其中，()$_{MIC}$ 表示该关联建立消息为经过完整性保护处理的消息。

在一种可选的设计中，第二节点 120 在接收到关联建立失败消息的情况下，可以重新发起关联请求消息。

在一种可选的设计中，第二节点 120 在接收到关联建立消息时，如果关联建立消息进行了加密（或者，关联建立消息包含的或者携带的信息进行了加密），则第二节点 120 可以解密该关联建立消息（或者，解密关联建立消息包含的或携带的信息）。第二节点 120 还可检查关联建立消息的完整性（或者，检查关联建立消息包含的或携带的信息的完整性）。

如果完整性验证不通过，则第二节点 120 丢弃该消息。

如果完整性验证通过，S419：第二节点 120 可向第一节点 110 发送关联完成消息。相应地，第一节点 110 可接收来自第二节点 120 的关联完成消息，所述关联完成消息可用于

表示所述第一通信连接建立完成。

在一种可选的设计中，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联完成消息做完整性保护。

应理解，在本申请实施例中，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联完成消息做完整性保护，可以理解为，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联完成消息包含的或者携带的信息做完整性保护。当信令面加密保护启动时，第二节点 120 可使用信令面的加密算法和加密密钥 Ks.enc 对关联完成消息做加密保护。应理解，在本申请实施例中，第二节点 120 可使用信令面的加密算法和加密密钥 Ks.enc 对关联完成消息做加密保护，可以理解为，第二节点 120 可使用信令面的加密算法和加密密钥 Ks.enc 对关联完成消息包含的或者携带的信息做加密保护。

示例地，该关联完成消息可以表示如下：

（关联完成消息）$_{MIC}$。

其中，（）$_{MIC}$ 表示该关联完成消息为经过完整性保护处理的消息。

第一节点 110 可以对接收到的关联完成消息进行处理。

例如，如果关联完成消息进行了加密（或者，关联完成消息包含的或者携带的信息进行了加密），则第一节点 110 可解密关联完成消息（或者，解密关联完成消息包含的或者携带的信息）。或者，第一节点 110 可以检查关联完成消息的完整性（或者，检查关联完成消息包含的或者携带的信息的完整性）。如果完整性验证不通过，则丢弃该消息。如果完整性验证通过，则执行后续流程，在此不再赘述。

上述安全上下文协商和关联完成之后，第一节点 110 和第二节点 120 可保存协商的第一安全上下文。

示例地，该第一安全上下文可以包括但不限于前述的身份 ID、临时 ID、Kgt、Kgt 有效期、Kgt ID、密钥协商算法、信令面的加密算法和完整性保护算法、信令面的加密密钥和完整性保护密钥、用户面的加密算法和完整性保护算法或用户面的认证加密算法、用户面的加密密钥和完整性保护密钥或用户面的认证加密密钥、[GK]、[GK ID]、[组算法]、[GK 有效期]等。

在一种可选的设计中，本申请实施例中，第一节点 110 和第二节点 120 还可支持安全上下文过期删除机制，需要保存安全上下文的节点可以配置一个时钟，以支持该机制，在此不再赘述。或者，第一节点 110 还可保存第二节点 120 的身份标识与第一密钥的对应关系，第二节点 120 还可保存第一节点 110 的身份标识与第一密钥的对应关系。

在第一通信连接建立完成之后，第一节点 110 和第二节点 120 之间进行业务时，可以根据密钥类型或业务类型确定该第一通信连接的业务范围，并传输该业务范围对应的业务。

例如，基于可信融合 PSK 建立的通信连接（包括安全上下文）只能用于融合通信场景下第二通信技术的业务。基于普通 PSK 建立的通信连接（包括安全上下文）用于第一通信技术的业务（如，可以是除融合通信场景下第二通信技术的业务外的其他业务）。

方法示例二：

在该方法示例二中，可由第二节点 120 获取第一密钥，第二节点 120 获取第一密钥后，可以同步获取用于第二节点 120 的身份认证的相关参数，并在同一消息（例如关联请求消息）中携带密钥类型指示信息或业务类型指示信息、以及用于第二节点 120 的身份认证的

相关参数，以便第一节点 110 可以根据第二节点 120 上报的密钥类型指示信息或业务类型指示信息确定所述第一密钥，并基于第二节点 120 上报的相关参数与第二节点 120 进行身份认证和安全上下文协商流程，从而在第一节点 110 和第二节点 120 之间建立安全的第一通信连接。需要说明的是，方法示例二中所包括的步骤 S411-S419 仅为可选步骤的示例，在一些示例中，下述步骤还可以交换实施顺序，本申请实施例不做具体限定。

如图 4b 所示，在方法示例二中，该通信方法可以包括以下步骤:

S411（可选）: 第一节点 110 发送第六消息（例如系统消息）。相应地，第二节点 120 可以接收该第六消息。详细实现可参见上文中结合图 4a 介绍的 S411 的相关描述，在此不再赘述。

S412: 该第二节点 120（例如第二节点 120 的服务层）根据对应所述第二通信技术的类型，和/或，根据第一业务的业务类型，获取第一密钥或第一密钥的类型。详细实现可参见上文中结合图 4a 介绍的 S412 的相关描述，在此不再赘述。

S413b: 第二节点 120 向第一节点 110 发送关联请求消息。相应地，第一节点 110 可以接收来自所述第二节点 120 的关联请求消息。

与图 4a 介绍的方法示例一相比，在该方法示例二中是在第二节点 120 发送的关联请求消息中携带密钥类型指示信息或业务类型指示信息，即方法示例二中的关联请求消息对应方法示例一中的第一消息和关联请求消息的合并，该关联请求消息中可以承载所述第一节点 110 的 ID、密钥类型指示信息或业务类型指示信息、以及用于第二节点 120 的身份认证的相关认证参数，包括但不限于第二节点 120 选择的 KE alg、KEt、第二节点 120 的安全能力和 NONCEt 等。安全能力可以包括第二节点 120 支持的 KDF、加密算法、完整性保护算法和认证加密算法中的一项或多项。详细实现可参见上文中结合图 4a 介绍的 S413a、S415a 的相关描述，在此不再赘述。

S414: 第一节点 110 根据所述密钥类型指示信息或所述业务类型指示信息，获取所述第一密钥。详细实现可参见上文中结合图 4a 介绍的 S414，在此不再赘述。

S416: 第一节点 110 向所述第二节点发送与所述第一密钥关联的安全上下文请求消息（第二消息的一个示例）。相应地，第二节点 120 接收来自所述第一节点 110 的安全上下文请求消息。详细实现可参见上文中结合图 4a 介绍的 S416 的相关描述，在此不再赘述。

S417: 第二节点 120 向第一节点 110 发送安全上下文响应消息(第三消息的一个示例)。相应地，第一节点 110 接收来自所述第二节点 120 的安全上下文响应消息。详细实现可参见上文中结合图 4a 介绍的 S417 的相关描述，在此不再赘述。

S418: 第一节点 110 可在所述第二节点 120 的身份认证成功的情况下，向所述第二节点发送关联建立消息（第四消息的一个示例）。相应地，第二节点 120 接收来自第一节点 110 的关联建立消息。详细实现可参见上文中结合图 4a 介绍的 S418 的相关描述，在此不再赘述。

S419: 第二节点 120 可向第一节点 110 发送关联完成消息。相应地，第一节点 110 可接收来自第二节点 120 的关联完成消息。详细实现可参见上文中结合图 4a 介绍的 S419 的相关描述，在此不再赘述。

方法示例三:

在方法示例三中，可由第一节点 110 获取第一密钥，第一节点 110 可以根据所述第一密钥，与第二节点 120 进行身份认证和安全上下文协商流程，从而在第一节点 110 和第二

节点 120 之间建立安全的第一通信连接。需要说明的是，方法示例三中所包括的步骤 S421-S427 仅为可选步骤的示例，在一些示例中，下述步骤还可以交换实施顺序，本申请实施例不做具体限定。

如图 4c 所示，该通信方法例如可以包括以下步骤：

S421（可选）：第一节点 110 发送第六消息（例如系统消息）。相应地，第二节点 120 可以接收该第六消息。详细实现可参见上文中结合图 4a 介绍的 S411，在此不再赘述。

S422：第二节点 120 向第一节点 110 发送关联请求消息。相应地，第一节点 110 可以接收来自所述第二节点 120 的关联请求消息。

本申请实施例中，该关联请求消息中可以携带该第二节点 120 的身份 ID（例如媒体接入层标识）、以及用于指示第二节点 120 的能力的相关参数，包括但不限于第二节点 120 选择的密钥协商算法（例如用 KE alg 表示）、密钥协商参数（例如用 KEt 表示）、第二节点 120 的安全能力（sec capabilities）和随机数 NONCEt 等。安全能力可以包括第二节点 120 支持的密钥派生函数 KDF、加密算法，完整性保护算法和认证加密算法等中的一项或多项，在此不再赘述。

示例地，该关联请求消息可以表示为如下多元组：

(ID, KE alg, KEt,sec capabilities, NONCEt)。

S423：第一节点 110 根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。

应理解，实施 S423 时，该第一节点 110 还可以是根据用户输入的相关指示信息获取所述第一密钥或者根据来自其它设备的相关指示信息获取所述第一密钥，本申请实施例对此不做限定。S423 的详细实现可参见上文中结合图 4a 介绍的 S412，在此不再赘述。

S424：第一节点 110 根据所述第一密钥向所述第二节点发送安全上下文请求消息（第二消息的一个示例）。相应地，第二节点 120 接收来自所述第一节点 110 的安全上下文请求消息，该安全上下文请求消息关联于第一密钥。详细实施细节可参见图 4a 中 S416 的相关描述，在此不再赘述。

S425：第二节点 120 向第一节点 110 发送安全上下文响应消息（第三消息的一个示例）。相应地，第一节点 110 接收来自所述第二节点 120 的安全上下文响应消息。详细实施细节可参见图 4a 中 S417 的相关描述，在此不再赘述。

S426：第一节点 110 在所述第二节点 120 的身份认证成功的情况下，向所述第二节点发送关联建立消息（第四消息的一个示例）。相应地，第二节点 120 接收来自第一节点 110 的关联建立消息。详细实施细节可参见图 4a 中 S418 的相关描述，在此不再赘述。

S427：第二节点 120 可向第一节点 110 发送关联完成消息。相应地，第一节点 110 可接收来自第二节点的关联完成消息。详细实施细节可参见图 4a 中 S419 的相关描述，在此不再赘述。

由此，在图 4a、图 4b、图 4c 所示的通信方法中，在存在多个密钥的场景中，第一节点 110 和第二节点 120 之间可以选择与第一业务关联的第一密钥，并根据所述第一密钥完成双方之间的身份认证和安全上下文协商流程，以在双方之间建立安全的第一通信连接，进而使得第一节点 110 和第二节点 120 之间进行业务时，可以根据使用不同密钥建立的安全通信连接传输对应业务的数据，以满足融合通信场景下的安全需求，并保障相应业务数据的安全性。

其中，与图 4a、图 4b 所示的通信方法相比，图 4c 所示的通信方法中，可由第一节点 110 根据第二节点 120 的相关能力，例如在注册时上报的业务类型、业务特征、通信能力等，主动为该第二节点 120 选择密钥作为第一密钥，由此，第二节点 120 与第一节点 110 之间无需交互第一消息（即密钥指示消息），可以减少信令开销。

情形二：该第一信息包括用于第一节点 110 与第二节点 120 通信的第一安全上下文。

在该情形中，第一节点 110 和第二节点 120 均存在至少两套安全上下文，例如前述普通安全上下文、可信安全上下文和非可信安全上下文，第一节点 110 和第二节点 120 之间可以在所述至少两套安全上下文中协商确定所需的第一安全上下文，并基于该第一安全上下文建立安全的第一通信连接。需要说明的是，情形二中所包括的步骤 S431-S435 仅为可选步骤的示例，在一些示例中，下述步骤还可以交换实施顺序，本申请实施例不做具体限定。

如图 4d 所示，该通信方法例如可以包括以下步骤：

S431（可选）：第一节点 110 发送第六消息（例如系统消息）。相应地，第二节点 120 可以接收该第六消息。详细实现可参见上文中结合图 4a 介绍的 S411，在此不再赘述。

S432：第二节点 120 根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一安全上下文或所述第一安全上下文的类型。

应理解，实施 S432 时，该第二节点 120 还可以是根据用户输入的相关指示信息获取所述第一安全上下文或所述第一安全上下文的类型，或者根据来自其它设备的相关指示信息获取所述第一安全上下文或所述第一安全上下文的类型，本申请实施例对此不做限定。应理解，本申请实施例中，对于第二节点 120 获取第一安全上下文或第一安全上下文的类型还可以通过其他方式，本申请实施例对此不做限定。

本申请实施例中，在融合通信场景下，该第一安全上下文可以包括以下任一种实现方式：

示例 3：所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

其中，用于所述第二通信技术的业务的安全上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文。这里的网络可以理解为第三节点所对应的网络，例如可以为 5G 核心网。应理解，在本申请实施例中，未经过所述网络鉴权的安全上下文，可以理解为：没有经过网络或者无需经过网络确认的安全上下文（例如默认的密钥对应的安全上下文），或者虽然经过网络确认但是没有确认成功的安全上下文（例如对应于前述未经过所述网络鉴权的密钥的安全上下文）。

以前述的与 PSK 对应的安全上下文为例，若该安全上下文未经过第三节点 130 侧的核心网（例如 5G 核心网）的鉴权和密钥协商过程或未协商达成一致，该安全上下文为非可信安全上下文，对应前述的非可信融合 PSK。若该安全上下文经过第三节点 130 侧的核心网的鉴权和密钥协商过程且达成一致获得的，该安全上下文为可信安全上下文，对应前述的可信融合 PSK。

示例 4：所述第一安全上下文为用于第一通信技术的业务的安全上下文。

其中，与前述多个密钥的优先级和使用原则相似，本申请实施例中，所述至少两套安全上下文也可以有安全上下文的优先级和使用原则，其中，第一安全上下文与第一业务相关联，在所述至少两套安全上下文中选择第一安全上下文至少需要遵循以下原则：在所述

第一业务为第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；和/或，在所述第一业务为所述第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

比如，1）针对融合通信场景下第二通信技术的业务，存在用于融合通信场景下第二通信技术的业务的可信安全上下文，则不使用用于融合通信场景下第二通信技术的业务的非可信安全上下文，而是使用可信安全上下文，即可信安全上下文的优先级高于非可信安全上下文的优先级；2）针对融合通信场景下第二通信技术的业务，使用用于融合通信场景下第二通信技术的业务的安全上下文，而不使用用于第一通信技术的业务的安全上下文，即用于融合通信场景下第二通信技术的业务的非可信安全上下文的优先级高于用于第一通信技术的业务的安全上下文的优先级；3）针对第一通信技术的业务，即使存在用于融合通信场景下第二通信技术的业务的安全上下文，也要使用用于第一通信技术的业务的安全上下文，以确保第一节点 110 和第二节点 120 之间的私有业务的安全性。

实施 S432 时，第二节点 120 可以根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，基于上述使用原则，获取所述第一安全上下文，例如用于第一通信技术的业务的安全上下文、或融合通信场景下的非可信安全上下文、或融合通信场景下的可信安全上下文。示例地，对应所述第二通信技术的类型可以是指所述第二通信技术采用的通信制式的类型，例如 5G 技术。

S433：第二节点 120 向第一节点 110 发送关联请求消息（第五消息的一个示例）。相应地，第一节点 110 接收所述关联请求消息。

示例地，该关联请求消息中可包含该第二节点 120 的临时 ID（例如物理层标识）、和/或，与所述第一安全上下文关联的标识，例如表示为 Kgt ID。

在一种可选的设计中，第二节点 120 还可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联请求消息做完整性保护，计算得到的 MIC 可携带在该关联请求消息中。

示例地，该关联请求消息可表示为如下多元组：

$$(\text{临时 ID, Kgt ID})_{\text{MIC}}。$$

其中，$()_{\text{MIC}}$ 表示该关联请求消息为经过完整性保护处理的消息。

S434：第一节点 110 根据临时 ID 和/或所述 Kgt ID，获取所述第一安全上下文。

在一种可选的设计中，第一节点 110 可以根据所述第一安全上下文检查所述关联请求消息的完整性。

如果第一节点 110 无第二节点 120 的临时 ID，或无相应的第一安全上下文，或第一节点 110 校验 MIC 失败，则第一节点 110 可向第二节点 120 发送失败消息并携带原因值（图中未示出）。第二节点 120 收到该失败消息后，可发起无安全上下文情况下的身份认证流程和安全上下文协商流程，例如可参见图 4a 或图 4b 的方法步骤，在此不再赘述。

如果第一节点 110 检查关联请求消息的完整性成功，则第一节点 110 可为第二节点 120 生成新的临时 ID（T-ID）。

S435：第一节点 110 向第二节点 120 发送关联建立消息（即第七消息）。相应地，第二节点 120 可接收来自所述第一节点的第七消息。

在一种可选的设计中，该关联建立消息中可包括第一节点 110 为第二节点 120 生成新的临时 ID（T-ID）。

在一种可选的设计中，第一节点 110 还可使用信令面的完整性保护算法和完整性保护

密钥 Ks.int 对关联建立消息做完整性保护。当信令面加密保护启动时，第一节点 110 可使用信令面的加密算法和加密密钥 Ks.enc 对关联建立消息做加密保护。

示例地，该关联建立消息可以表示为如下多元组：

(新临时 ID)$_{MIC}$。

其中，( )$_{MIC}$ 表示该关联建立消息为经过完整性保护处理的消息。

其中，如果第一节点 110 对该关联建立消息进行了加密，则第二节点 120 可解密该关联建立消息。第二节点 120 还可检查关联建立消息的完整性。如果完整性验证不通过，则丢弃该消息。如果完整性验证通过，则 S436：第二节点 120 可第一节点 110 发送关联完成消息（即第八消息）。

其中，第二节点 120 可使用信令面的完整性保护算法和完整性保护密钥 Ks.int 对关联完成消息做完整性保护。当信令面加密保护启动时，第二节点 120 可使用信令面的加密算法和加密密钥 Ks.enc 对关联完成消息做加密保护。

示例地，该关联完成消息可以表示如下：

（关联完成消息）$_{MIC}$。

其中，( )$_{MIC}$ 表示该关联完成消息为经过完整性保护处理的消息。

由此，在图 4d 所示的通信方法中，在存在多套安全上下文的场景中，第一节点 110 和第二节点 120 之间可以选择与第一业务关联的第一安全上下文，并根据所述第一安全上下文在双方之间建立第一通信连接，进而使得第一节点 110 和第二节点 120 之间进行业务时，可以根据使用基于不同的安全上下文建立的第一通信连接传输对应业务的数据，以满足融合通信场景下的安全需求，并保障相应业务数据的安全性。

需要说明的是，本申请实施例中，若第二节点 120 多次无法使用保存的安全上下文和第一节点 110 建立关联时，第二节点 120 可尝试删除保存的安全上下文，并采用前述图 4a 或图 4b 所示的方法，在第二节点 120 和第一节点 110 之间发起无安全上下文的关联流程，在此不再赘述。

本申请实施例还提供了一种通信装置，用于执行上述方法实施例中第一节点所执行的方法，相关特征可参见上述方法实施例，在此不再赘述。

如图 5 所示，该装置 500 可以包括：通信单元 501，用于与第二节点通信；处理单元 502，用于获取第一信息；根据所述第一信息与第二节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点。示例地，所述第一业务可以为所述第一通信技术的业务或者所述第二通信技术的业务。具体实现方式，请参考图 1 至图 4d 所示实施例中的详细描述，这里不再赘述。

在一种可选的设计中，图 5 所示的通信装置 500，还可用于执行上述方法实施例中第二节点所执行的方法，例如，通信单元 501，用于与第一节点通信；处理单元 502，用于获取第一信息；根据所述第一信息与第一节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点。示例地，所述第一业务可以为所述第一通信技术的业务或者所述第二通信技术的业务。相关特征可参见上述方法实施例，在此不再赘述。

需要说明的是，本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。在本申请的实施例中的各功能单元可以集成在一个处

理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

在一种可能的实现方式中，本申请实施例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存储有程序代码，当所述程序代码在所述计算机上运行时，使得计算机执行上述方法实施例。

在一种可能的实现方式中，本申请实施例提供了一种计算机程序产品，当所述计算机程序产品在计算机上运行时，使得所述计算机执行上述方法实施例。

在一个简单的实施例中，本领域的技术人员可以想到上述实施例中的通信装置均可采用图 6 所示的形式。

如图 6 所示的装置 600，包括至少一个处理器 610 和通信接口 630。在一种可选的设计中，还可以包括存储器 620。

本申请实施例中不限定上述处理器 610 以及存储器 620 之间的具体连接介质。

在如图 6 的装置中，处理器 610 在与其他设备进行通信时，可以通过通信接口 630 进行数据传输。

当通信装置采用图 6 所示的形式时，图 6 中的处理器 610 可以通过调用存储器 620 中存储的计算机执行指令，使得装置 600 可以执行上述任一方法实施例中通信装置执行的方法。

本申请实施例还涉及一种芯片系统，该芯片系统包括处理器，用于调用存储器中存储的计算机程序或计算机指令，以使得该处理器执行上述任一实施例的方法。

在一种可能的实现方式中，该处理器可以通过接口与存储器耦合。

在一种可能的实现方式中，该芯片系统还可以直接包括存储器，该存储器中存储有计算机程序或计算机指令。

示例地，存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。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），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如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，DDR SDRAM）、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（synchlink DRAM，SLDRAM）和直接内存总线随机存取存

储器（direct rambus RAM，DR RAM）。

本申请实施例还涉及一种处理器，该处理器用于调用存储器中存储的计算机程序或计算机指令，以使得该处理器执行上述任一实施例所述的方法。

示例地，在本申请实施例中，处理器是一种集成电路芯片，具有信号的处理能力。例如，该处理器可以是现场可编程门阵列（field programmable gate array，FPGA），可以是通用处理器、数字信号处理器（digital signal processor，DSP）、专用集成电路（application specific integrated circuit，ASIC）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件，还可以是系统芯片（system on chip，SoC），还可以是中央处理器（central processor unit，CPU），还可以是网络处理器（network processor，NP），还可以是微控制器（micro controller unit，MCU），还可以是可编程控制器（programmable logic device，PLD）或其他集成芯片，可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请实施例范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1.一种通信方法，其特征在于，应用于第一节点，所述方法包括:

获取第一信息;

根据所述第一信息与第二节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术;

其中，所述第一节点为接入对应第二通信技术的网络的节点，所述第一业务为所述第一通信技术的业务或者所述第二通信技术的业务。

2.根据权利要求 1 所述的方法，其特征在于，所述第一信息包括用于与所述第二节点通信认证的第一密钥，所述获取第一信息，包括:

根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。

3.根据权利要求 1 所述的方法，其特征在于，所述第一信息包括用于与所述第二节点通信认证的第一密钥，所述方法还包括:

接收来自所述第二节点的第一消息，所述第一消息承载密钥类型指示信息或业务类型指示信息;

所述获取第一信息，包括:

根据所述密钥类型指示信息或所述业务类型指示信息，获取所述第一密钥。

4.根据权利要求 2 或 3 所述的方法，其特征在于，所述根据所述第一信息与第二节点建立第一通信连接，包括:

向所述第二节点发送与所述第一密钥关联的第二消息，所述第二消息用于所述第一节点的身份认证;

接收响应于所述第二消息的第三消息，所述第三消息用于所述第二节点的身份认证;

在所述第二节点的身份认证成功的情况下，向所述第二节点发送第四消息，所述第四消息用于与所述第二节点建立所述第一通信连接。

5.根据权利要求 2-4 中任一项所述的方法，其特征在于 ，

在所述第一业务为所述第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥; 或者，

在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

6.根据权利要求 5 所述的方法，其特征在于，所述用于所述第二通信技术的业务的密钥包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥，所述非可信密钥为未经过所述网络鉴权的密钥，所述可信密钥的优先级高于所述非可信密钥的优先级。

7.根据权利要求 1-6 中任一项所述的方法，其特征在于，在建立所述第一通信连接之前，所述方法还包括:

接收来自所述网络的用于所述第二通信技术的业务的密钥。

8.根据权利要求 1 所述的方法，其特征在于，所述第一信息包括用于与所述第二节点通信的第一安全上下文，所述获取第一信息，包括:

接收来自所述第二节点的第五消息，所述第五消息承载与所述第一安全上下文关联的

标识;

所述获取第一信息，包括:

根据所述标识，获取所述第一安全上下文。

9.根据权利要求 8 所述的方法，其特征在于，

在所述第一业务为所述第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；或者，

在所述第一业务为所述第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

10.根据权利要求 9 所述的方法，其特征在于，所述用于所述第二通信技术的业务的安全上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文，所述可信安全上下文的优先级高于所述非可信安全上下文的优先级。

11.根据权利要求 1-10 中任一项所述的方法，其特征在于，所述获取第一信息之前，所述方法还包括:

向所述第二节点发送第六消息，所述第六消息承载用于指示所述第一节点支持所述第二通信技术的信息。

12.一种通信方法，其特征在于，应用于第二节点，所述方法包括:

获取第一信息;

根据所述第一信息与第一节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术;

其中，所述第一节点为接入对应第二通信技术的网络的节点，所述第一业务为所述第一通信技术的业务或者所述第二通信技术的业务。

13.根据权利要求 12 所述的方法，其特征在于，所述第一信息包括用于与所述第一节点通信认证的第一密钥，所述获取第一信息，包括:

根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一密钥。

14.根据权利要求 13 所述的方法，其特征在于，所述方法还包括:

向所述第一节点发送第一消息，所述第一消息承载与所述第一密钥相关联的信息。

15.根据权利要求 13 或 14 所述的方法，其特征在于，所述根据第一信息与所述第一节点建立所述第一通信连接，包括:

接收来自所述第一节点的第二消息，所述第二消息关联于所述第一密钥，所述第二消息用于所述第一节点的身份认证;

在所述第一节点的身份认证成功的情况下，向所述第一节点发送第三消息，所述第三消息用于所述第二节点的身份认证;

接收响应于所述第三消息的第四消息，所述第四消息用于与所述第二节点建立所述第一通信连接。

16.根据权利要求 13-15 中任一项所述的方法，其特征在于，

在所述第一业务为所述第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；或者，

在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二

通信技术的业务的密钥。

17.根据权利要求 16 所述的方法，其特征在于，所述用于所述第二通信技术的业务的密钥包括可信密钥或非可信密钥，其中，所述可信密钥为经过所述网络鉴权成功的密钥，所述非可信密钥为未经过所述网络鉴权的密钥，所述可信密钥的优先级高于所述非可信密钥的优先级。

18.根据权利要求 12-17 中任一项所述的方法，其特征在于，在建立所述第一通信连接之前，所述方法还包括:

接收来自所述网络的用于所述第二通信技术的业务的密钥。

19.根据权利要求 12 所述的方法，其特征在于，所述第一信息包括第一安全上下文，所述第一安全上下文用于所述第二节点与所述第一节点建立所述第一通信连接，所述获取第一信息，包括:

根据对应所述第二通信技术的类型，和/或，根据所述第一业务的业务类型，获取所述第一安全上下文。

20.根据权利要求 19 所述的方法，其特征在于，

在所述第一业务为所述第一通信技术的业务的情况下，所述第一安全上下文为用于所述第一通信技术的业务的安全上下文；或者，

在所述第一业务为所述第二通信技术的业务的情况下，所述第一安全上下文为用于所述第二通信技术的业务的安全上下文。

21.根据权利要求 20 所述的方法，其特征在于，所述用于所述第二通信技术的业务的安全上下文包括可信安全上下文或非可信安全上下文，其中，所述可信安全上下文为经过所述网络鉴权成功的安全上下文，所述非可信安全上下文为未经过所述网络鉴权的安全上下文，所述可信安全上下文的优先级高于所述非可信安全上下文的优先级。

22.根据权利要求 19-21 中任一项所述的方法，其特征在于，所述方法还包括:

向所述第一节点发送第五消息，所述第五消息承载与所述第一安全上下文关联的标识。

23.根据权利要求 12-22 中任一项所述的方法，其特征在于，所述方法还包括:

接收来自所述第一节点的第六消息，所述第六消息承载用于指示所述第一节点支持所述第二通信技术的信息。

24.一种通信装置，其特征在于，应用于第一节点，包括:

通信单元，用于与第二节点通信;

处理单元，用于获取第一信息；根据所述第一信息与所述第二节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点，所述第一业务为所述第一通信技术的业务或者所述第二通信技术的业务。

25.根据权利要求 24 所述的装置，其特征在于，

所述第一信息包括用于与所述第二节点通信认证的第一密钥，在所述第一业务为所述第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；或者，在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

26.一种通信装置，其特征在于，包括:

通信单元，用于与第一节点通信;

处理单元，用于获取第一信息；根据所述第一信息与所述第一节点建立第一通信连接，所述第一通信连接用于传输第一业务的数据，所述第一通信连接对应第一通信技术；其中，所述第一节点为接入对应第二通信技术的网络的节点，所述第一业务为所述第一通信技术的业务或者所述第二通信技术的业务。

27.根据权利要求 26 所述的装置，其特征在于，所述第一信息包括用于与所述第一节点通信认证的第一密钥，在所述第一业务为所述第一通信技术的业务的情况下，所述第一密钥为用于所述第一通信技术的业务的密钥；或者，在所述第一业务为所述第二通信技术的业务的情况下，所述第一密钥为用于所述第二通信技术的业务的密钥。

28.一种通信装置，其特征在于，包括至少一个处理器和接口电路，所述接口电路用于为所述至少一个处理器提供数据或者代码指令，所述至少一个处理器用于通过逻辑电路或执行代码指令实现如所述权利要求 1-11 或 12-23 中任一项所述的方法。

29.一种通信系统，其特征在于，包括用于实现如权利要求 1-11 中任一项所述方法的通信装置，和，实现如权利要求 12-23 中任一项所述方法的通信装置。

30.一种计算机可读存储介质，其特征在于，所述计算机可读介质存储有程序代码，当所述程序代码在计算机上运行时，使得计算机执行如权利要求 1 至 11 中任一项所述的方法；或者，当所述程序代码在计算机上运行时，使得计算机执行如权利要求 12 至 23 中任一项所述的方法。

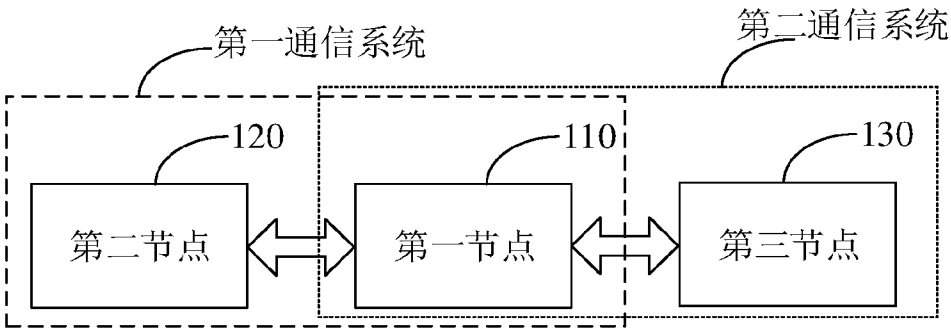
第一通信系统
第二通信系统
120
110
130
第二节点
第一节点
第三节点

图 1

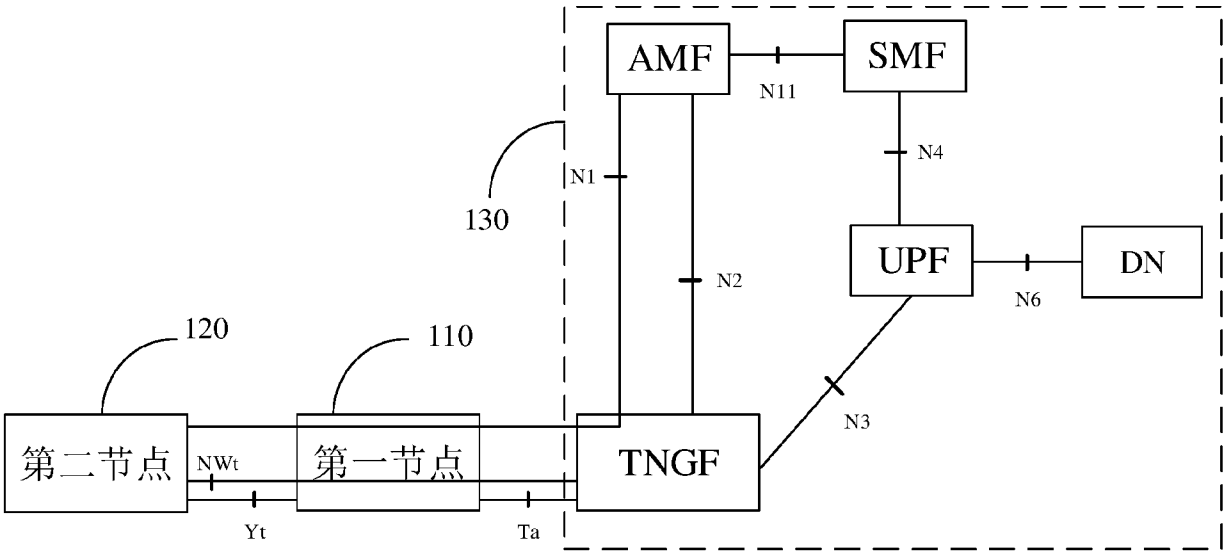
AMF
SMF
N11
N4
N1
130
UPF
DN
N2
N6
120
110
N3
第二节点
NWt
第一节点
TNGF
Yt
Ta

图 2

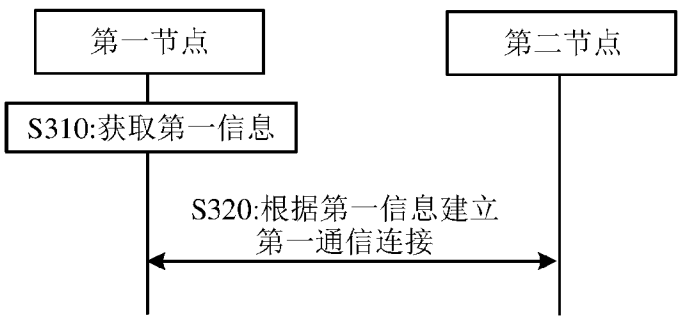
第一节点
第二节点
S310:获取第一信息
S320:根据第一信息建立
第一通信连接

图 3

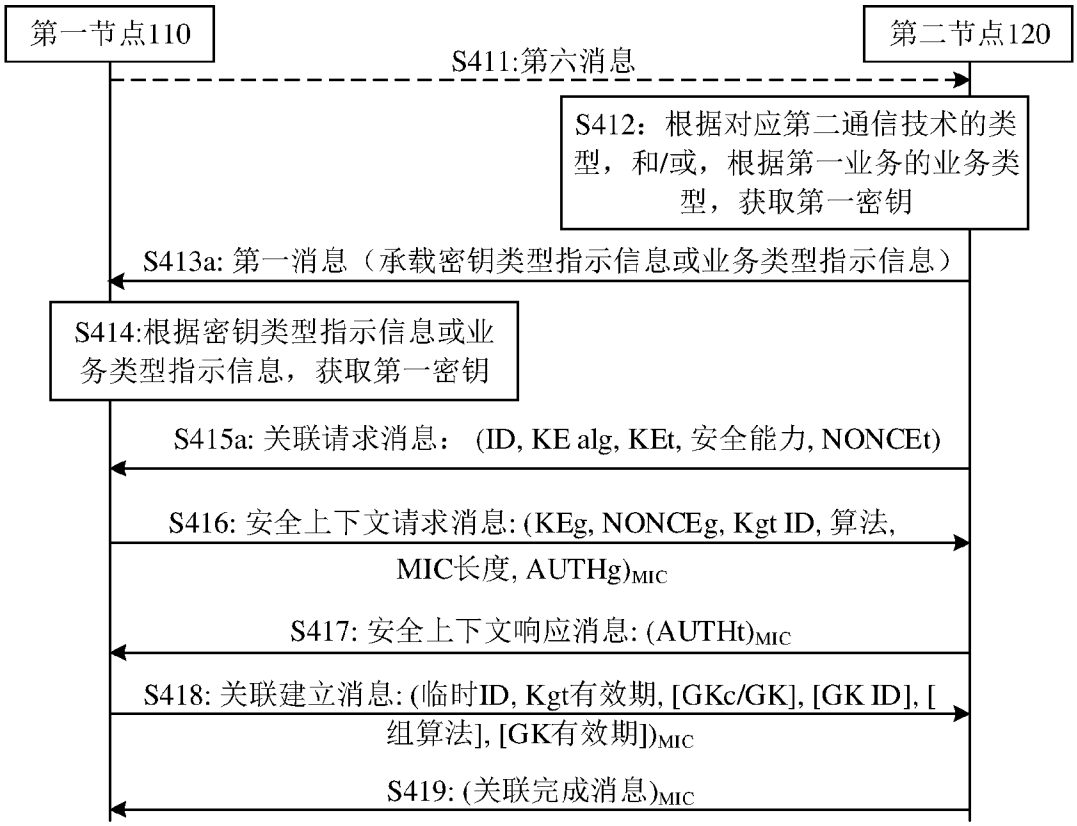
第一节点110
第二节点120
S411:第六消息
S412：根据对应第二通信技术的类型，和/或，根据第一业务的业务类型，获取第一密钥
S413a: 第一消息（承载密钥类型指示信息或业务类型指示信息）
S414:根据密钥类型指示信息或业务类型指示信息，获取第一密钥
S415a: 关联请求消息： (ID, KE alg, KEt, 安全能力, NONCEt)
S416: 安全上下文请求消息: (KEg, NONCEg, Kgt ID, 算法, MIC长度, AUTHg)MIC
S417: 安全上下文响应消息: (AUTHt)MIC
S418: 关联建立消息: (临时ID, Kgt有效期, [GKc/GK], [GK ID], [组算法], [GK有效期])MIC
S419: (关联完成消息)MIC

图 4a

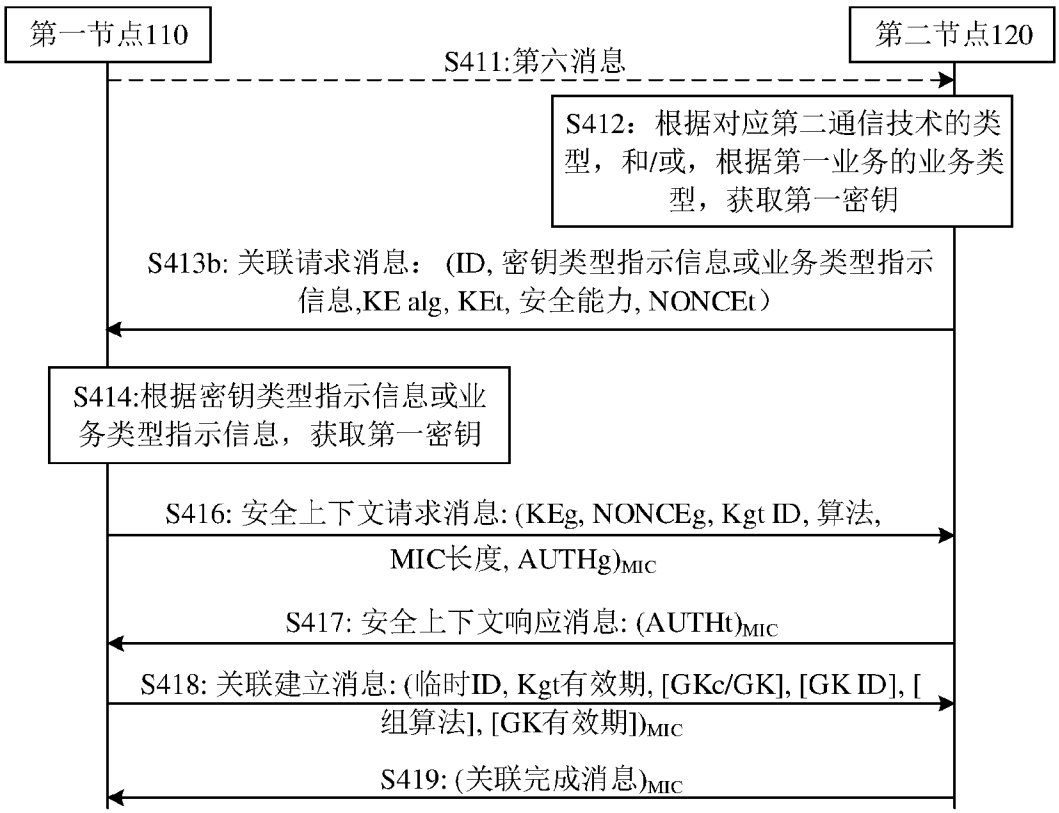
第一节点110
第二节点120
S411:第六消息
S412：根据对应第二通信技术的类型，和/或，根据第一业务的业务类型，获取第一密钥
S413b: 关联请求消息： (ID, 密钥类型指示信息或业务类型指示信息,KE alg, KEt, 安全能力, NONCEt）
S414:根据密钥类型指示信息或业务类型指示信息，获取第一密钥
S416: 安全上下文请求消息: (KEg, NONCEg, Kgt ID, 算法, MIC长度, AUTHg)MIC
S417: 安全上下文响应消息: (AUTHt)MIC
S418: 关联建立消息: (临时ID, Kgt有效期, [GKc/GK], [GK ID], [组算法], [GK有效期])MIC
S419: (关联完成消息)MIC

图 4b

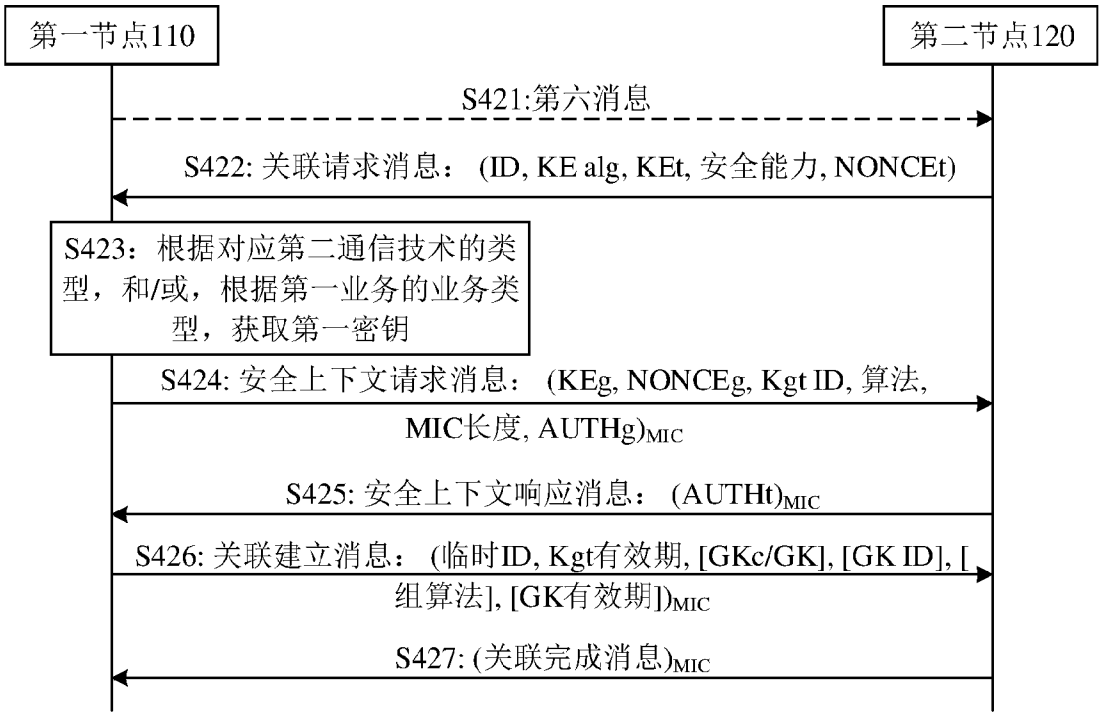
第一节点110
第二节点120
S421:第六消息
S422: 关联请求消息： (ID, KE alg, KEt, 安全能力, NONCEt)
S423：根据对应第二通信技术的类型，和/或，根据第一业务的业务类型，获取第一密钥
S424: 安全上下文请求消息： (KEg, NONCEg, Kgt ID, 算法, MIC长度, AUTHg)MIC
S425: 安全上下文响应消息： (AUTHt)MIC
S426: 关联建立消息： (临时ID, Kgt有效期, [GKc/GK], [GK ID], [组算法], [GK有效期])MIC
S427: (关联完成消息)MIC

图 4c

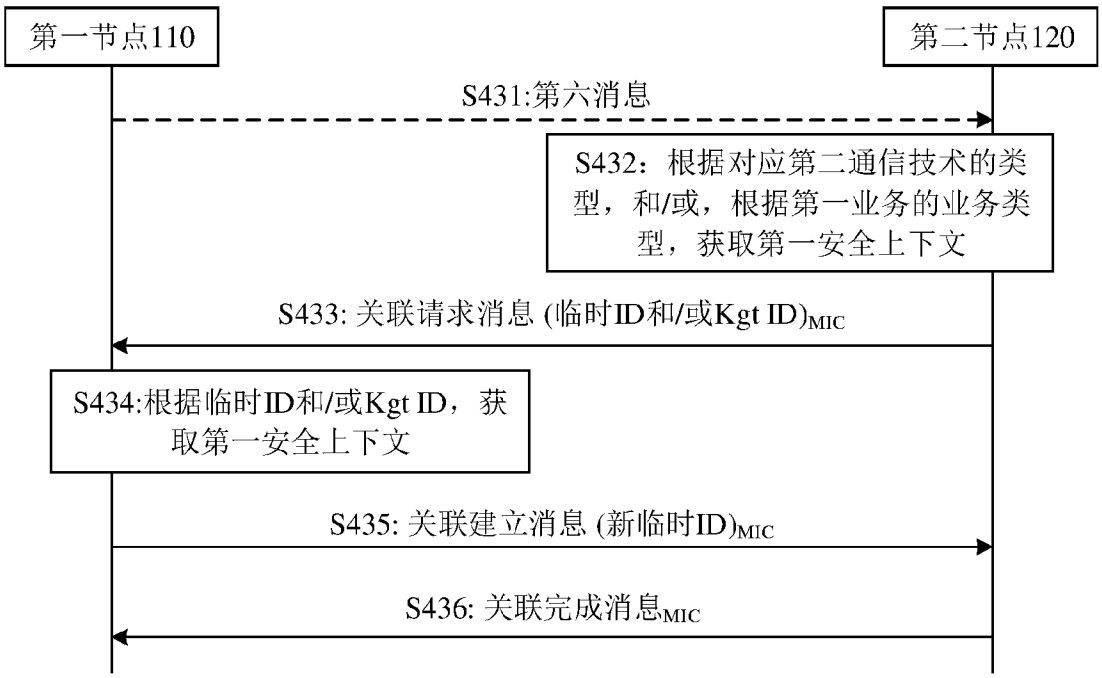
第一节点110
第二节点120
S431:第六消息
S432：根据对应第二通信技术的类型，和/或，根据第一业务的业务类型，获取第一安全上下文
S433: 关联请求消息 (临时ID和/或Kgt ID)MIC
S434:根据临时ID和/或Kgt ID，获取第一安全上下文
S435: 关联建立消息 (新临时ID)MIC
S436: 关联完成消息MIC

图 4d

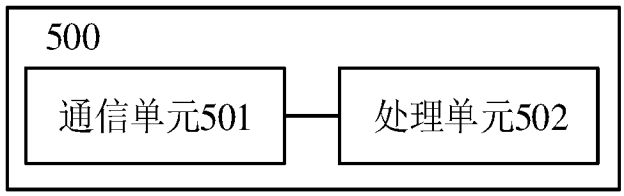

图 5

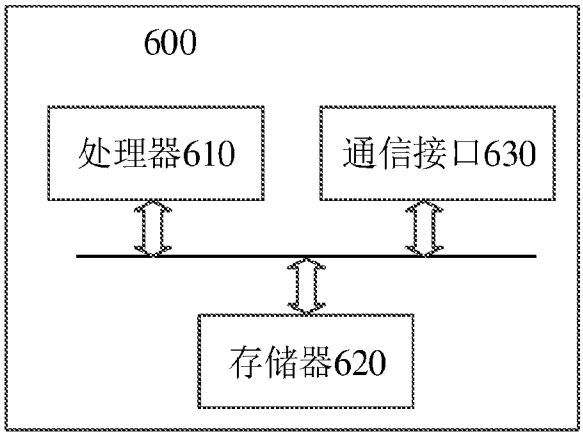

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/122352

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2021.01)i; H04W 12/04(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)

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)

CNTXT; VEN; ENTXTC; ENTXT; VCN: 第二通信技术, 短距离, 近距离, 短程, 远程, 5G, 密钥, 秘钥, 认证, 令牌, 密码, 业务类型, 异构, 上下文, 优先, NFC, wifi, key, authenti+, certif+, context, token?, priority

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2020314841 A1 (CISCO TECHNOLOGY, INC.) 01 October 2020 (2020-10-01) description, paragraphs [0022]-[0077]	1-30
Y	CN 112491533 A (HUAWEI TECHNOLOGIES CO., LTD.) 12 March 2021 (2021-03-12) description, paragraphs [0082]-[0304]	1-30
Y	CN 112740733 A (HUAWEI TECHNOLOGIES CO., LTD.) 30 April 2021 (2021-04-30) description, paragraphs [0167]-[0359]	4-11, 15-23, 28-30
A	CN 107820247 A (LEGIC IDENTSYSTEMS AG) 20 March 2018 (2018-03-20) entire document	1-30
A	CN 109906624 A (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 18 June 2019 (2019-06-18) entire document	1-30

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 May 2022	**29 June 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/122352

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2020314841	A1	01 October 2020	EP	3949598	A1	09 February 2022
				WO	2020198123	A1	01 October 2020
				US	10904882	B2	26 January 2021
CN	112491533	A	12 March 2021	WO	2021047276	A1	18 March 2021
CN	112740733	A	30 April 2021		None		
CN	107820247	A	20 March 2018	CA	2975517	A1	06 March 2018
				KR	20180027378	A	14 March 2018
				US	2018070199	A1	08 March 2018
				KR	101947917	B1	13 February 2019
				US	10555154	B2	04 February 2020
CN	109906624	A	18 June 2019	US	2020059783	A1	20 February 2020
				WO	2018077607	A1	03 May 2018
				EP	3533245	A1	04 September 2019

国际检索报告

国际申请号
PCT/CN2021/122352

A. 主题的分类

H04W 12/06(2021.01)i; H04W 12/04(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)

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））

CNTXT;VEN;ENTXTC;ENTXT;VCN：第二通信技术，短距离，近距离，短程，远程，5G，密钥，秘钥，认证，令牌，密码，业务类型，异构，上下文，优先，NFC，wifi，key，authenti+，certif+，context，token?，priority

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
Y	US 2020314841 A1 (CISCO TECH INC) 2020年10月1日 (2020-10-01) 说明书第[0022]-[0077]段	1-30
Y	CN 112491533 A (华为技术有限公司) 2021年3月12日 (2021-03-12) 说明书第[0082]-[0304]段	1-30
Y	CN 112740733 A (华为技术有限公司) 2021年4月30日 (2021-04-30) 说明书第[0167]-[0359]段	4-11、15-23、28-30
A	CN 107820247 A (励智识别技术有限公司) 2018年3月20日 (2018-03-20) 全文	1-30
A	CN 109906624 A (瑞典爱立信有限公司) 2019年6月18日 (2019-06-18) 全文	1-30

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2022年5月30日	2022年6月29日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 巫吟荷 电话号码 (86-512)88996227

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/122352

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)
US	2020314841	A1	2020年10月1日	EP	3949598	A1	2022年2月9日
				WO	2020198123	A1	2020年10月1日
				US	10904882	B2	2021年1月26日
CN	112491533	A	2021年3月12日	WO	2021047276	A1	2021年3月18日
CN	112740733	A	2021年4月30日		无		
CN	107820247	A	2018年3月20日	CA	2975517	A1	2018年3月6日
				KR	20180027378	A	2018年3月14日
				US	2018070199	A1	2018年3月8日
				KR	101947917	B1	2019年2月13日
				US	10555154	B2	2020年2月4日
CN	109906624	A	2019年6月18日	US	2020059783	A1	2020年2月20日
				WO	2018077607	A1	2018年5月3日
				EP	3533245	A1	2019年9月4日